Oesterreichs Energie Companion Standard
Smart Meter 2.0

OE_CS_Hauptdokument

Version 1.0

31.3.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Einleitung 5

A.1 Ziel und Zweck des Dokuments 5

A.2 Nutzen 5

A.3 Geltungsbereich und Stückzahlen in Österreich 6

A.4 Zielgruppen 7

A.5 Referenzierte Gesetze Normen und Standards 7

A.6 Dokumentenstruktur des Companion Standards OE 7

B. Big Picture 7

B.1 Architektur des Zählersystems 7

B.2 Schnittstellentabelle 12

B.3 Schnittstellen im Detail 13

B.4 Übersicht Zählerregister 14

C. Use Cases 15

C.1 Übersicht 15

D. Implementierungsstandards 16

D.1 Objektmodel 16

D.2 Implementation Guide G3-PLC und G3-Hybrid 16

D.3 Implementation Guide Mobilfunk 16

D.4 Implementation Guide Ethernet 17

E. Lastenhefte 17

E.1 Lastenheft für Smart Meter 1ph und 3ph direkte Messung der 2. Generation 17

E.2 Lastenheft für Smart Meter Messwandler der 2. Generation 17

E.3 Lastenheft Displayguide 17

E.4 Lastenheft über die funktionale Beschreibung Dualmode-Gateway 17

F. Security Anforderungen 17

F.1 Anforderungskatalog Ende-zu-Ende-Sicherheit 17

G. Standard-Liefer-Konfiguration 18

G.1 Standard-Liefer-Konfiguration 18

G.2 Shipment File 18

H. Anhang 18

H.1 Glossar und Begriffsdefinitionen 18

H.2 Beispielkonfigurationen 19

H.3 Zählerstifte und Steckleisten 19

H.4 Spezifizierung des Direktzähler mit Hardwareerweiterung 19

A. Einleitung

Dieses Hauptdokument definiert den Rahmen des OE Companion Standard für Smart Meter 2.0 in Österreich. Für Detaillierungen und Abweichungen von etwaigen Standards verweist das Hauptdokument gezielt auf ergänzende Dokumente. Eine Übersicht der Kapitel und der ergänzenden Dokumente ist in Abbildung 1 dargestellt.

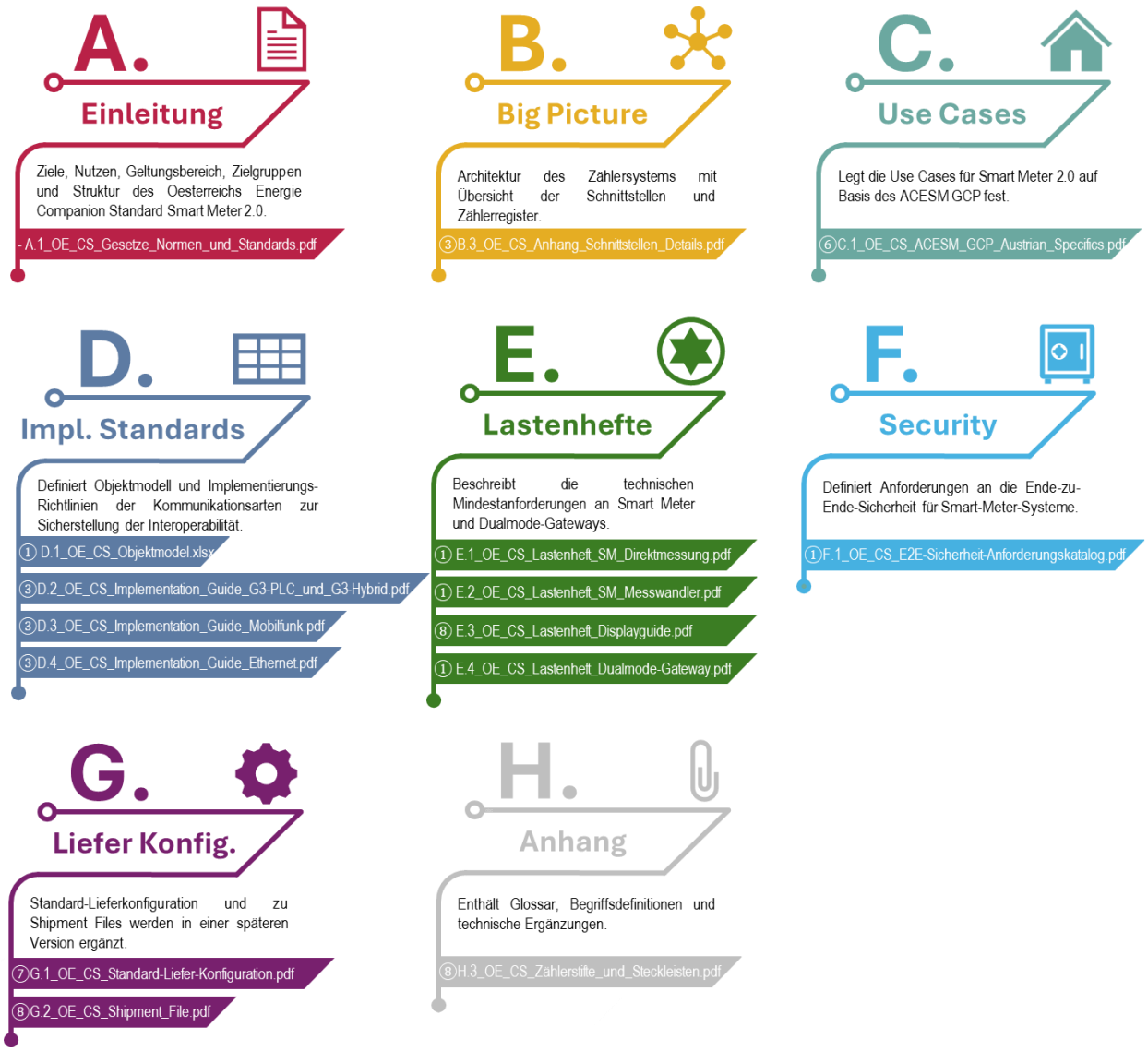


Abbildung 1: Kapitelübersicht des OE Companion Standards für Smart Meter 2.0 in Österreich. Bei widersprüchlichen Informationen gilt die vor dem Dokumentennamen angegebene Priorität. (1=hoch, 8=niedrig)

A.1 Ziel und Zweck des Dokuments

Der OE Companion Standard definiert die nächste Generation Smart Meter Strom für Österreich und dient den österreichischen Netzbetreibern als Grundlage für zukünftige Beschaffungen von Smart Metern. Der Companion Standard orientiert sich dabei konsequent an den neuen europäischen und nationalen Rahmenbedingungen, den Bedürfnissen von Netzbetreibern sowie den Anforderungen des Marktes. Der Companion Standard basiert daher auf internationalen, offenen Standards. Nach dem Prinzip - so detailliert wie notwendig und so offen wie möglich - wurden die Anforderungen vertieft spezifiziert, um Interpretationsspielraum zu vermeiden und Interoperabilität sowie Interchangeability sicherzustellen.

Dabei soll mit dem Companion Standard ein modularer Ansatz sichergestellt werden, der einen Austausch des Kommunikationsmoduls ermöglicht und somit neue Kommunikationstechnologien auch künftig genutzt werden können. Welche Kommunikationstechnologien für das jeweilige Versorgungsgebiet optimal sind, obliegt den Netzbetreibern selbst.

Dadurch soll ein nachhaltiger und effizienter Einsatz von Smart Metern 2.0 in Österreich gewährleistet werden.

Ziele:

- Ein österreichweiter Companion Standard für alle Smart Meter Typen der Sparte Strom (gültig für alle Spannungsebenen)
- Interoperabilität und Interchangeability von Smart Metern
- Einheitliche Funktionalitäten von Smart Metern in Österreich
- Umsetzung einheitlicher Use Cases basierend auf dem AC Electricity Smart Meter Generic Companion Profile (ACESM GCP) der DLMS UA
- Nutzung unterschiedlicher Kommunikationstechnologien mit einem Smart Meter
- Reduktion der Komplexität von Smart Meter Prozessen und zugehörigen Komponenten
- Erhöhte Transparenz gegenüber Kunden und dem Markt
- Steigerung der Attraktivität des österreichischen Marktes für Smart Meter Hersteller durch größere Mengen
- Reduktion der Kosten für individuelle Entwicklungen, Anpassungen, Integration und Testing
- Sicherstellung einer fortwährenden Weiterentwicklung gemäß den anerkannten Regeln der Technik
- Funktionale Beschreibung eines Dualmode-Gateways

Nichtziele:

- Produktentwicklung bzw. Auswahl eines Zählerherstellers
- Standardisierung der zentralen Softwarekomponenten (HES / MDM)
- Direkter Zugriff durch Dritte auf die Smart Meter Infrastruktur
- Österreichischer Companion Standard für Dualmode-Gateways
- Zertifizierung der Dualmode-Gateways
- Interoperabilität und Interchangeability der Dualmode-Gateways

A.2 Nutzen

Der Nutzen eines österreichweiten Companion Standard ist, im Schulterschluss mit der Branche effiziente Marktprozesse mit einer erhöhten Transparenz den Kund*innen gegenüber zu ermöglichen. Durch den österreichweiten und herstellerunabhängigen Standard soll eine Kostenreduktion und Investitionssicherheit erzielt werden. Darüber hinaus soll eine hohe Datenverfügbarkeiten sichergestellt werden, um die neuen gesetzlichen, regulatorischen oder kundenseitigen Anforderungen bestmöglich zu erfüllen.

A.3 Geltungsbereich und Stückzahlen in Österreich

Der Österreichs Energie Companion Standard wurde von den 13 größten Netzbetreiben in Österreich entwickelt:

- Wiener Netze GmbH
- Netz Niederösterreich GmbH
- Netz Oberösterreich GmbH

- Energienetze Steiermark GmbH
- Salzburg Netz GmbH
- Kärnten Netz GmbH (KNG)
- TINETZ – Tiroler Netze GmbH
- Vorarlberger Energienetze GmbH
- Netz Burgenland GmbH
- LINZ NETZ GmbH
- Stromnetz Graz GmbH & Co KG
- Innsbrucker Kommunalbetriebe AG (IKB Netze)
- Stadtwerke Klagenfurt AG

Alle weiteren Netzbetreiber wurden durch einen Vertreter der Vereinigung Österreichischer Elektrizitätswerke (VÖEW) repräsentiert.

Der Geltungsbereich des Companion Standards OE bezieht sich demnach auf alle Smart Meter in Österreich. Gemäß ElWG 2025 sind alle Kundenverrechnungszähler unabhängig der Spannungsebene als Smart Meter auszuführen. Die genauen Stückzahlen werden von der E-Control in einem jährlichen Smart Meter Monitoring Bericht veröffentlicht. Im „Bericht zur Einführung von intelligenten Messgeräten in Österreich 2025 – Berichtsjahr 2024“ sind 6.737.329 Smart Meter in Österreich angeführt.

Es wird von einem jährlichen Zählerzuwachs von rund 1% ausgegangen, respektive der Möglichkeit auf Kundenwunsch zusätzliche Messeinrichtungen (ehem. Submeter) in Kundenanlagen zu installieren.

Hinweis: Zusätzlich zu dem hier beschriebenen Companion Standard, wird ein Subset der österreichischen Netzbetreiber (ca. 8%) Direktzähler mit einer Hardwareerweiterung ausschreiben (nicht vor 2029). Diese Erweiterung wird von den anderen österreichischen Netzbetreibern nicht benötigt. Die Erweiterung umfasst eine zusätzliche Schnittstelle für einen externen Taster, zur Bedienung des Displays. gemäß Kapitel H.4.

A.4 Zielgruppen

Zielgruppen für das Dokument sind sämtliche Stakeholder eines Smart Meters in Österreich, Zählerhersteller, Netzbetreiber, als auch Behörden und Ministerien.

A.5 Referenzierte Gesetze Normen und Standards

Siehe Dokument „A.1_OE_CS_Gesetze_Normen_und_Standards.pdf“.

B. Big Picture

B.1 Architektur des Zählersystems

Basis für die Systemarchitektur von Smart Metering 2.0 stellt die im Rahmen des EU-Mandats M/441 erarbeitete Smart Metering Referenzarchitektur dar, welche im technischen Report TR 50572 der CENELEC veröffentlicht wurde. Nachstehend ist die aus der Referenzarchitektur abgeleitete Systemarchitektur für Smart Metering 2.0 für Österreich sowie Beschreibung der funktionalen Komponenten und Kommunikationsschnittstellen dargestellt.

Das Architekturbild gilt für direkte als auch (halb-)indirekte Smart Meter 2.0. Wobei ein Breaker ausschließlich bei direkten Zählern vorgesehen ist.

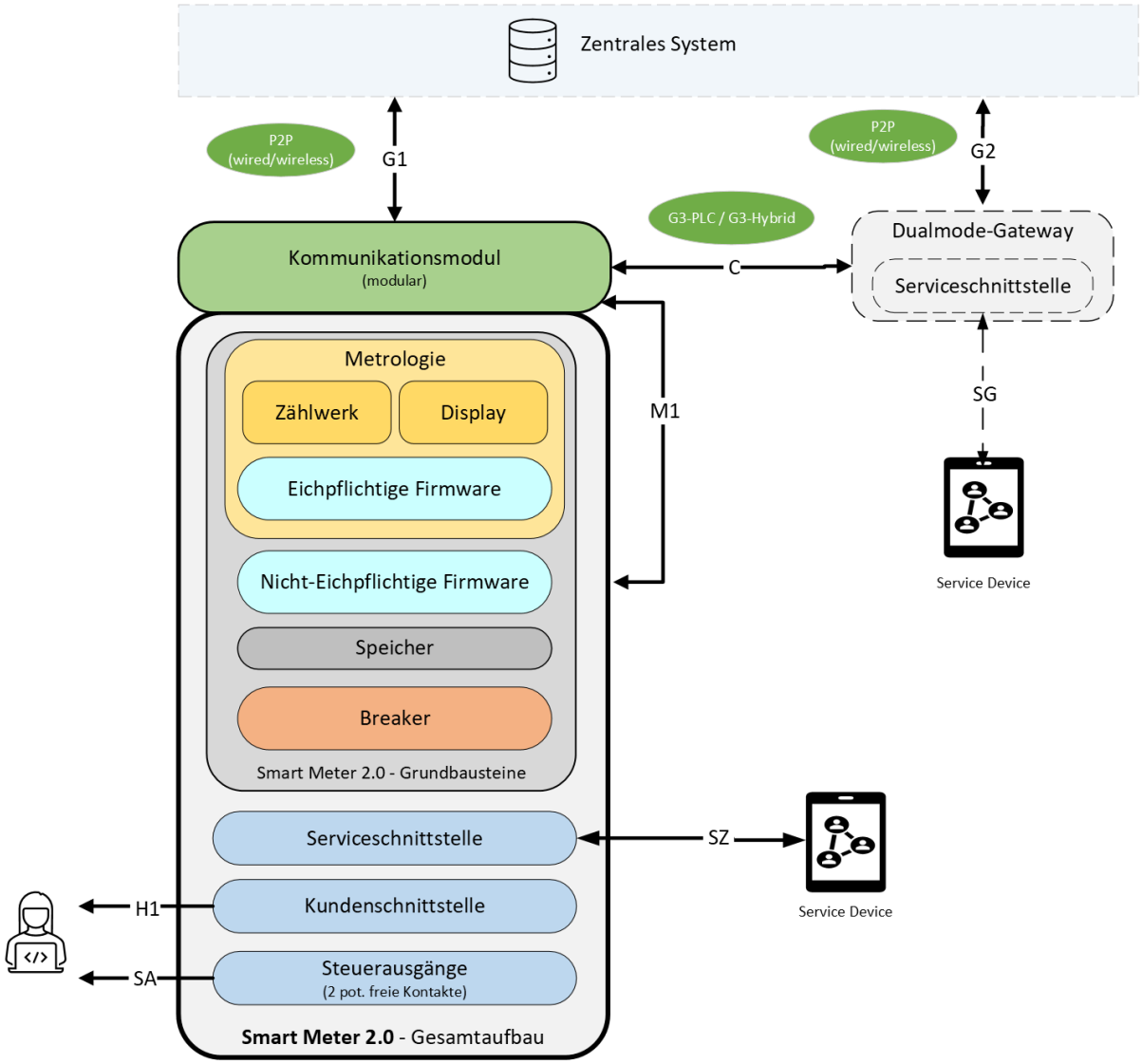


Abbildung 3: Gesamtaufbau des Smart Meters 2.0

B.1.1 Grundbausteine des Smart Meters

- **Zählwerk**
  zum Messen und Erfassen der Verbrauchs- und Betriebsdaten
- **Display:**
  zum Anzeigen von Messdaten, Zählerständen, und Konfigurationen am Smart Meter
- **Breaker (Abschalteinrichtung):**
  zum Ein- und Ausschalten der Kundenanlage
- **Firmware**
  - **Eichpflichtiger** Bestandteil der Firmware
  - **Nicht-Eichpflichtiger** Bestandteil der Firmware
- **Speicher**
  Für Firmware, Messdaten und Protokolle der auch einen sicheren Bereich für kryptografisches Material vorsieht.

B.1.2 Schnittstellen der Komponenten

- **Schnittstelle G1** (Smart Meter – Zentrales System)
  Über diese bidirektionale Schnittstelle wird der Smart Meter über eine Punkt-zu-Punkt Verbindung (P2P) an das zentrale System angebunden.
- **Schnittstelle G2** (Dualmode-Gateway – Zentrales System)
  Über diese bidirektionale Schnittstelle wird das Dualmode-Gateway über eine Punkt-zu-Punkt Verbindung (P2P) an das zentrale System angebunden.
- **Schnittstelle C** (Smart Meter – Dualmode-Gateway)
  Über diese bidirektionale Schnittstelle wird der Smart Meter über eine G3-PLC bzw. G3-Hybrid Verbindung an das Dualmode-Gateway angebunden.
- **Schnittstelle M1** (Modulschnittstelle)
  Diese Schnittstelle verbindet den Smart Meter mit dem Kommunikationsmodul.
- **Schnittstelle SZ** (Serviceschnittstelle Smart Meter)
  Die bidirektionale Schnittstelle SZ dient zur lokalen Anbindung von Wartungsgeräten (z.B. Handheld-Geräten) für die Parametrierung, Updates oder für das Auslesen von Daten aus den Smart Metern. Diese Schnittstelle muss so performant sein, dass die Use Cases vor Ort in vertretbarer Zeit abgewickelt werden können.
- **Schnittstelle H1** (Kundenschnittstelle)
  Die unidirektionale Schnittstelle H1 dient zur Bereitstellung von Daten in nahezu Echtzeit, für das Monitoren von Verbrauchsdaten oder zum Einbinden in kundenseitige Energiemanagementsysteme.
- **Schnittstelle SG** (Serviceschnittstelle Dualmode-Gateway)
  Die bidirektionale Schnittstelle SG dient zur lokalen Anbindung von Wartungsgeräten für die Parametrierung, Updates oder für das Auslesen von Betriebsdaten aus dem Dualmode-Gateway.
- **Schnittstelle SA** (Steuerausgänge)
  Der Smart Meter stellt zwei potentialfreie Kontakte für externe (Last-)Schaltung zur Verfügung.

B.1.3 Angebundene Komponenten

- **Dualmode-Gateway (DGW)**
  Das Dualmode-Gateway bildet die Übertragungskomponente zwischen G3-PLC bzw. G3-Hybrid Kommunikationsmodulen, der angebundenen Smart Meter und dem zentralen System. Die Kommunikation zwischen dem Kommunikationsmodul der Smart Meter und dem zentralen System erfolgt über die Schnittstellen **C** und **G2** am Dualmode-Gateway.

  Die sicherheitsrelevanten Funktionen sind im „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ definiert, die technischen Anforderungen im Dokument „E.4_OE_CS_Lastenheft_Dualmode-Gateway.pdf“.

  a. <u>Betrieb als reines Gateway (Gateway-Mode)</u>

     In diesem Mode wird eine transparente Ende-zu-Ende-Kommunikationsverbindung zwischen dem zentralen System und den Zählern hergestellt.

  b. <u>Dualer Betrieb als Gateway und Datenkonzentrator (Dualmode)</u>

     In diesem Modus wird die Verarbeitung der Nachricht nach der Quelle unterschieden.

     Nachrichten zwischen zentralem System und Smart Meter (Gateway-Mode)

     Werden Nachrichten zwischen zentralem System und den angebundenen Smart Metern ausgetauscht, werden diese vom Dualmode-Gateway weitergeleitet. Die Verarbeitung folgt den Regeln des reinen Gateway-Betriebs. (siehe Gateway-Mode).

     Nachrichten zwischen DGW und Smart Meter (Datenkonzentrator-Mode)

     Werden Nachrichten zwischen DGW und den angebundenen Smart Metern ausgetauscht, wird eine DLMS COSEM Verbindung direkt zwischen DGW und den Smart Metern aufgebaut, um die Operationen des Datenkonzentrators durchzuführen.

Zentrales System

Das zentrale System ist die Gegenstelle der Smart Meter oder der Dualmode-Gateways. Dieses umfasst folgende Systeme:

- Head-End-System (HES)
- Gateway Managementsystem
- Hardware Security Module (HSM)
- Public-Key-Infrastructure (PKI)
- Key-Management-System (KMS)

Ferner stellt das zentrale System die Gegenstelle des Kommunikationskanals und des Applikationsprotokolls der Smart Meter und Dualmode-Gateways dar. Diese Strecke ist gemäß „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ abzusichern. Das zentrale System bietet definierte Schnittstellen für die Ankopplung an die IT-Backendsysteme.

- **Service Device**

Das Service Device ist ein mobiles Servicegerät zur Installation, Wartung und Konfiguration von Smart Metern und Dualmode-Gateways im Feld. Es ermöglicht eine sichere Kommunikation über die Schnittstellen SZ (für Smart Meter) und SG (für Dualmode-Gateways). Die Bedienung erfolgt über eine intuitive Benutzeroberfläche mit Logging- und Diagnosetools. Das Gerät ist robust, energieeffizient und für den Außeneinsatz optimiert.

B.2 Schnittstellentabelle Smart Meter

Tabelle 1: Beschreibung der WAN-, LAN-, Service-, Kunden- und Steuerschnittstellen (G1, G2, C, M1, SZ, H1, SA)

Schnittstelle	Bezeichnung	Anwendungsbereich	Richtung	Zusatzinformation
G1	G1	Remote Verbindung Zentrales System und Smart Meter ohne Gateway; DLMS-Client im Zentralen System	bidirektional	Kabellos: • NB-IoT1/2 • LTE-M1/2 (inkl. 450 MHz) • LTE CAT-1/1bis (inkl. 450 MHz) Kabelgebunden: • Ethernet
G2	G2	Remote Verbindung Zentrales System und Smart Meter.	bidirektional	Zentrales System und GW (G2): NB-spezifisch, z.B.: Ethernet / LWL / Mobilfunk
C	LAN C	Remote Verbindung Dualmode-GW und SM (Netzzugangsschicht G3-PLC bzw. G3-Hybrid)	bidirektional	G3-PLC bzw. G3-Hybrid auf Netzzugangsschicht
M1	Modulschnittstelle (Module Interface)	Lokale Verbindung zwischen Kommunikationsmodul und Smart Meter	bidirektional	Herstellerspezifisch. Nicht durch OE CS spezifiziert.
SZ	Serviceschnittstelle (Service Interface)	Lokale Verbindung zwischen Service Device und Smart Meter	bidirektional	Infrarot nach IEC62056-21 Standard Baudrate ab 19200
H1	Kundenschnittstelle (Customer Interface)	Bereitstellung von Daten (Push) in nahezu Echtzeit gemäß gesetzlicher Anforderung.	unidirektional	DSMR P1; spannungsversorgt, 115k baud rate
SA	Steuerausgang (Control Output)	Steuersignale (Ein/Aus) je Steuerausgang	unidirektional	2 potentialfreie Schaltrelais (kein Kommunikationsprotokoll)

B.3 Schnittstellen im Detail

Die Details zu den Schnittstellen, Protokollen und IT Basisservices sind im Dokument „B.3_OE_CS_Anhang_Schnittstellen_Details.pdf“ definiert.

B.4 Übersicht Zählerregister

Tabelle 2: Übersicht der wichtigsten Messgrößen sowie deren zugehörige Ausgabe- und Speicherintervalle am Smart Meter.

	Ausgabeintervall Kundenschnittstelle H1	1 Sekunde	-	-	-	-
	Speicherintervall	-	15 Minuten	24 Stunden	1 Monat	10 oder 15 Minuten
	Speichertiefe	-	>=60 Tage	>=60 Tage	15 Werte	>=10 Tage
	OBIS Code der Profile		1-0:99.1.0.255	1-0:99.2.0.255	1-0:99.1.4.255	1-0:99.14.0.255
OBIS Code	**Beschreibung des Momentanregisters (Gemessen im Abtastintervall des Zählers)**	**Momentanwert /Sekundenwert**	**15-Minuten Lastprofil**	**24 Stunden Lastprofil**	**Monatliches Verrechnungsprofil**	**Betriebsdatenprofil**
0:96.1.1.255	Zählernummer	x				
0:96.10.x.255	Status		x	x		x
0-0:1.0.0.255	Clock	x	x	x	x	x
1-0:1.6.0.255	Höchster 15-Minuten-Wirkleistungswert des Monats - Bezug +P	x			x	
1-0:2.6.0.255	Höchster 15-Minuten-Wirkleistungswert des Monats - Lieferung -P	x			x	
1-0:3.6.0.255	Höchster 15-Minuten-Blindleistungswert des Monats - Bezug +Q				x	
1-0:4.6.0.255	Höchster 15-Minuten-Blindleistungswert des Monats - Lieferung -Q				x	
1-0:1.7.0.255	Wirkleistung Bezug +P	x				
1-0:2.7.0.255	Wirkleistung Lieferung -P	x				
1-0:3.7.0.255	Blindleistung Bezug +Q	x				
1-0:4.7.0.255	Blindleistung Lieferung -Q	x				
1-0:5.7.0.255	Blindleistung +Qi	x				
1-0:6.7.0.255	Blindleistung +Qc	x				
1-0:7.7.0.255	Blindleistung -Qi	x				
1-0:8.7.0.255	Blindleistung -Qc	x				
1-0:1.8.0.255	Wirkenergie Bezug +A	x	x	x	x	
1-0:2.8.0.255	Wirkenergie Lieferung -A	x	x	x	x	
1-0:3.8.0.255	Blindenergie Bezug +R	x	x	x	x	
1-0:4.8.0.255	Blindenergie Lieferung -R	x	x	x	x	
1-0:5.8.0.255	Blindenergie +Ri	x	x	x	x	
1-0:6.8.0.255	Blindenergie +Rc	x	x	x	x	
1-0:7.8.0.255	Blindenergie -Ri	x	x	x	x	
1-0:8.8.0.255	Blindenergie -Rc	x	x	x	x	
1-0:32.7.0.255	Spannung L1	x				

1-0:52.7.0.255	Spannung L2	x				
1-0:72.7.0.255	Spannung L3	x				
1-0:31.7.0.255	Strom L1	x				
1-0:51.7.0.255	Strom L2	x				
1-0:71.7.0.255	Strom L3	x				
0-1:96.3.10.255	Kontaktstatus Relay 1 (0 oder 1)	x				
0-2:96.3.10.255	Kontaktstatus Relay 2 (0 oder 1)	x				
1-0:32.23.0.255	Min Spannung L1					x
1-0:32.24.0.255	Average Spannung L1					x
1-0:32.26.0.255	Max Spannung L1					x
1-0:52.23.0.255	Min Spannung L2					x
1-0:52.24.0.255	Average Spannung L2					x
1-0:52.26.0.255	Max Spannung L2					x
1-0:72.23.0.255	Min Spannung L3					x
1-0:72.24.0.255	Average Spannung L3					x
1-0:72.26.0.255	Max Spannung L3					x
1-0:31.24.0.255	Average Strom L1					x
1-0:51.24.0.255	Average Strom L2					x
1-0:71.24.0.255	Average Strom L3					x

C. Use Cases

Die Use Cases für Smart Meter 2.0 basieren auf dem AC Electricity Smart Meter Generic Companion Profile (ACESM GCP) 1.0.1 der DLMS User Association. Österreich spezifische Anforderungen, Ergänzungen und Abweichungen zum ACESM GCP werden im Dokument „H.2_OE_CS_Annex.pdf“ spezifiziert. Weiters wurden drei spezifische Use Cases für den österreichischen Markt definiert. Die Österreich spezifische Anforderungen inklusive der drei spezifische Use Cases sind im Dokument „C.1_OE_CS_ACESM_GCP_ Austrian Specifics.pdf“. Alle Use Cases sind in der nachfolgenden Tabelle aufgelistet.

C.1 Übersicht

Tabelle 3: Übersicht der ACESM GCP Use Cases und der Österreich spezifische Anforderungen.

ID	Use Case	Description
UC01	Meter Registration	Process of incorporating devices (ACESMs, submeters, ...) into the system.
UC02	Remote Tariff Programming	Process of remotely programming the parameters necessary to support a time of use (TOU) based tariff contract
UC03	On Demand Meter Register reading for multi-utility meters	Process of collecting meter register readings upon a specific request.
UC04	On Demand Meter Load Profile reading for multi-utility meters	Process of collecting load profile register readings upon a specific request.
UC05	Periodic Meter reading for multi-utility meters	Process of periodically collecting meter readings for billing purposes (periodic reading)
UC06	Remote or local Disconnection and Reconnection (E, G)	Process of disconnecting or reconnecting the electricity I or gas (G) supply of a customer
UC07	Clock Synchronization	Process of adjusting the internal clock of the metering equipment
UC08	Quality of Supply	Process of supervising Power Outages, Sags and Swells,
UC09	Load Management by relay (E only)	Process of controlling specific local loads by means of relays.
UC10	Firmware update	Process of downloading new firmware to a device
UC11	Meter supervision	Process of supervising any events which could comprise the meter and the system.
UC12	Consumer Information	Process of periodically transmitting meter reads and consumer information via a local digital interface
UC13	Communication Supervision	Process of supervising events affecting the meter to HES communication.
UC14	Enabling / disabling functionalities	Process of enabling or disabling a functionality.
UC15	Power Control	Process of activating or deactivating the demanded power control mode in meters
UC16	Alarm and event Management	Process of management of events and equipment alarms
UC17	Meter Availability Control	Process to ping a meter to check that communication works

UC18	Display messages on meter display	Process of displaying pre-defined or on-the-fly messages such as supply of energy or tariffs
UC19	Configuration of meter locally	Process of initial installation or in-service control
UC20	Manage security settings	Process of setting and updating security credential scan be done locally or remotely and cover setting new security keys or certificates in the meter
UC21	Prepayment	Prepayment is not supported
Oe01	Communications Configuration	Configuration of communications parameters needed for PLC and P2P technologies.
Oe02	Test and Calibration	Change of meter operational mode to permit testing and return to service.
Oe03	Exchange of communications module	Replacement of a communications module to adopt a new communications technology

D. Implementierungsstandards

Die Basis für die Implementierung stellt der ACESM GCP 1.0.1 der DLMS User Association dar. Ergänzungen und Abweichungen sind im Dokument „H.2_OE_CS_Annex.pdf“ und in den folgenden Unterkapiteln (siehe OE Use Cases in Tabelle Oben) beschrieben.

D.1 Objektmodel

Um die Austauschbarkeit von Smart Metern verschiedener Hersteller in einem System zu gewährleisten, wurde das Objektmodel auf Basis der Use Cases definiert. In diesem Modell sind alle Obis Codes, Interface Klassen, Attribute, Instanzen, Clients und Berechtigungen definiert und festgelegt. Nur Smart Meter, welche dieses Objektmodell ohne Abweichungen implementiert haben, entsprechen diesem Companion Standard.

D.2 Implementation Guide G3-PLC und G3-Hybrid

Ziel dieses Dokuments ist eine einheitliche Definition der für die PLC-Kommunikationsinfrastruktur benötigten Funktionen und Parameter, um die Interoperabilität aller PLC-Geräte (Smart Meter, Dualmode- Gateway, etc.) und den Head-End-Systemen sicherzustellen. Es ergänzt die Standards ITU-T G.9901 und G.9903 und beschreibt die Bitübertragungs- und Datenverbindungsschicht (data link layer). Zusätzlich dient die „Implementierungsrichtlinie“ als Begleitdokument zur Definition von der Transportschicht (transport layer) bis hinunter zur Bitübertragungsschicht (pysical layer).

Dafür werden hier definiert:

- zu unterstützende Netzwerktechnologien
- Spezifische Zählerfunktionen
- Erläuterungen zum OE- Objektmodell *„D.1_OE_CS_Objektmodel.xlsx“*
- Zusätzliche Beschreibung von spezifischen Events, Alarmen und Fehlerbehebungsprozeduren

Für bereits dokumentierte Funktionen wird nur auf die entsprechenden Dokumente referenziert. Zum Beispiel: ACESM GCP der DLMS UA; AT commands; etc. Das Dokument ist in „D.2_OE_CS_Implementation_Guide_G3-PLC_und G3-Hybrid.pdf“ angeführt.

D.3 Implementation Guide Mobilfunk

Ziel des Dokuments ist eine einheitliche Definition der für die Mobilfunk Kommunikationsinfrastruktur benötigten Funktionen und Parameter, um die Interoperabilität aller Zähler und den Head-End-Systemen sicherzustellen.

Dazu werden in diesem Dokument folgende Aspekte definiert

- Zu unterstützende Mobilfunktechnologien
- Spezielle Anforderungen an die Mobilfunktechnologien
- Anforderungen an die technischen Eigenschaften des Funkmoduls
- Notwendige Zählerfunktionen
- Erläuterungen zum Objektmodell
- Zu überwachende Events und Alarme

Das Dokument ist in „D.3_OE_CS_Implementation_Guide_Mobilfunk.pdf“ angeführt.

D.4 Implementation Guide Ethernet

Das Dokument ist in „D.4_OE_CS_Implementation_Guide_Ethernet.pdf“ angeführt.

E. Lastenhefte

Die Zähler und das Dualmode-Gateway müssen zukunftssicher ausgeführt sein. Dies bedeutet die Geräte müssen über genügend Speicher (flüchtig und nichtflüchtig) und Rechenleistungsreserven verfügen, um Aktualisierungen (z.B.: Sicherheitsfunktionen) zu ermöglichen. Die Aktualisierbarkeit muss während des gesamten Produktlebenszyklus gewährleistet sein. Die Geräte dürfen nach Implementierung sämtlicher Anforderungen aus dem Österreichs Energie Companion Standard Smart Metering 2.0 inklusive V44 Kompression sowohl die Speicher als auch die Rechner nur maximal zu 50 % auslasten. Dies ist durch den Hersteller so detailliert nachzuweisen, dass eine einfache Überprüfung möglich ist.

E.1 Lastenheft für Smart Meter 1ph und 3ph direkte Messung der 2. Generation

Das Basisdokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“ beschreibt die wesentlichen technischen Anforderungen an die intelligenten Messgeräte.

E.2 Lastenheft für Smart Meter Messwandler der 2. Generation

In dem Dokument „E.2_OE_CS_Lastenheft_SM_Messwandler.pdf“ sind die Abweichungen bzw. Ergänzungen von Messwandlerzähler zu den Anforderungen zum Lastenheft E.1 direkte Messung definiert.

E.3 Lastenheft Displayguide

In dem Dokument „E.3_OE_CS_Lastenheft_Displayguide.pdf“ sind die wesentlichen Funktionen an die Menüführung der Anzeige am Display festgelegt.

E.4 Lastenheft über die funktionale Beschreibung Dualmode-Gateway

In dem Dokument „E.4_OE_CS_Lastenheft_Dualmode-Gateway.pdf“ gibt eine Übersicht über die wesentlichen funktionalen Anforderungen an ein Dualmode-Gateway für die G3-PLC bzw. G3-Hybrid Kommunikation. Es werden jedoch nicht alle Anforderungen im Detail beschrieben

F. Security Anforderungen

F.1 Anforderungskatalog Ende-zu-Ende-Sicherheit

Der Anforderungskatalog „Ende-zu-Ende-Sicherheit für Smart Metering“ von Österreichs Energie definiert die verbindlichen technischen und organisatorischen Mindestanforderungen an eine durchgängige Sicherheitsarchitektur für Smart-Meter-Systeme in Österreich, einschließlich Zähler, Dualmode-Gateways, zentrale Systeme und deren Kommunikation. Der Anforderungskatalog ist im Verzeichnis „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ aufzufinden.

G. Standard-Liefer-Konfiguration

G.1 Standard-Liefer-Konfiguration

Dieses Kapitel ist in der aktuellen Fassung des Österreichs Energie Companion Standards noch nicht finalisiert und wird in einer späteren Version ergänzt.

G.2 Shipment File

Dieses Kapitel ist in der aktuellen Fassung des Österreichs Energie Companion Standards noch nicht finalisiert und wird in einer späteren Version ergänzt.

H. Anhang

H.1 Glossar und Begriffsdefinitionen

Tabelle 4: Verzeichnis relevanter Abkürzungen, welche im OE CS verwendet werden.

Begriff	Erklärung
ACESM GCP	AC Electricity Smart Meter Generic Companion Profile
DGW	Dualmode-Gateway
DLMS	Device Language Message Specification
DLMS UA	DLMS User Association
DSMR	Dutch Smart Meter Requirements
DSO	Distribution System Operator
E2E	Ende-zu-Ende
ECA	E-Control Austria
ElWG	Elektrizitätswirtschaftsgesetz
G3-PLC	G3 Power Line Communication
GW	Gateway
HES	Head-End-System
HLS	High Level Security
HSM	Hardware Security Module
IEC	International Electrotechnical Commission
IKB	Innsbrucker Kommunalbetriebe
LAN	Local Area Network
MDM	Meter Data Management
OBIS	Object Identification System
OE / OE CS	Österreichs Energie / Österreichs Energie Companion Standard
P2P	Point-to-Point

PKI	Public Key Infrastructure
PLC	Power Line Communication
PQ	Power Quality
SA	Steuerausgang (Control Output)
Service Device	Mobiles Gerät zur Wartung- und Instandhaltung. (ehem. HHU)
SG	Serviceschnittstelle (Gateway)
SZ	Serviceschnittstelle (Smart Meter)
VÖEW	Vereinigung Österreichischer Elektrizitätswerke

H.2 Beispielkonfigurationen

Dieses Kapitel ist in der aktuellen Fassung des Österreichs Energie Companion Standards noch nicht finalisiert und wird in einer späteren Version ergänzt.

H.3 Zählerstifte und Steckleisten

Siehe Dokument “H.3_OE_CS_Zählerstifte_und_Steckleisten.pdf”.

H.4 Spezifizierung des Direktzähler mit Hardwareerweiterung

Die Erweiterung ist ein Eingang für einen externen Taster. Mit diesem muss es möglich sein sowohl den Breaker als auch die Displaysteuerung zu bedienen. Dieser Eingang muss die Spannungsversorgung für den externen Taster sicherstellen und entsprechend kurzschlussfest ausgeführt sein. Ein solcher Anschluss muss 2-polig als Schließer (z.B. 24V/250mA) mit Federzugklemmen oder Schraubklemmen ausgeführt werden und muss der technischen Betriebssicherheit des Zählers entsprechen.

Oesterreichs Energie Companion Standard
Smart Meter 2.0

A.1_OE_CS_Gesetze_Normen_und_Standards

Version 1.0

31.03.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Gesetzliche Rahmenbedingungen und Normen 3

A.1 Europäische Vorgaben 4

A.2 Nationale gesetzliche Vorgaben 4

A.3 Nationale Rahmenbedingungen 4

A.4 OE Anforderungskataloge und Dokumente 4

B. Standards und Normen 4

B.1 Nationale Berichte 5

B.2 Normen 5

A. Gesetzliche Rahmenbedingungen und Normen

A.1 Europäische Vorgaben

- Elektrizitätsbinnenmarkt-Richtlinie (RL 2009/72/EG)
- Clean Energy Packages (CEP) (RL [EU] 2019/944)
- Mandate M441 for smart meters
- MID-Richtlinie – europäisches MEG für Smart Meter
- Network Code: Requirements for Generators (RFG)
- Network Code: Demand Response
- Network Code: Cyber Security

A.2 Nationale gesetzliche Vorgaben

- Elektrizitätswirtschaftsgesetz (ElWG)
- Intelligente Messgeräte-Einführungsverordnung (IME-VO)
- Intelligente Messgeräte-Anforderungsverordnung (IMA-V 2026) *(Derzeit in Konsultation, Inkrafttreten im Juli 2026 geplant.)*
- Datenformat- und Verbrauchsinformationsdarstellungsverordnung (DAVID-VO)
- Datenschutzgesetz (DSG)
- Maß- und Eichgesetz (MEG)
- Erneuerbaren-Ausbau-Gesetz
- Netz- und Informationssystemsicherheitsgesetz (NISG)
- ÖNORM A-7700

A.3 Nationale Rahmenbedingungen

- Technische und Organisatorische Regeln für Betreiber und Benutzer von Netzen (TOR)
- Sonstige Marktregeln Strom (SoMa)

A.4 OE Anforderungskataloge und Dokumente

- OE Anforderungskatalog Ende-zu-Ende Sicherheit Smart Metering
- Data Protection Impact Assessment /Datenschutz-Folgenabschätzung für den Smart Meter Einsatz (aktuelle Version)

B. Standards und Technische Richtlinien

ETSI	Bezeichnung
TS 102 221	Smart Cards; UICC-Terminal interface; Physical and logical characteristics
TS 124 301	Universal Mobile Telecommunications System (UMTS); LTE; 5G; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3
TS 136 101	LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception
TS 136 133	LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management
TS 136 306	Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities

TS 136 321	Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification
TS 136 331	Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification
CEN/CLC/ETSI/TR	Bezeichnung
TR 50572	Functional reference architecture for communications in smart metering systems
GSMA	Bezeichnung
SGP.31	eSIM IoT Architecture and Requirements
SGP.32	eSIM IoT Technical Specification
TS.3	IoT Device Connetion Efficiency Guidelines
BSI	Bezeichnung
TR-03109-1	Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems
TR-03116, part 3	Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3 - Intelligente Messsysteme
TR-02102-1	Kryptographische Verfahren: Empfehlungen und Schlüssellängen
RFC	Bezeichnung
RFC 2119	Key words for use in RFCs to Indicate Requirement Levels
NIST	Bezeichnung
SP 800-57 Part 1 Rev. 5	Recommendation for Key Management: Part 1 – General
FIPS 186-4	Digital Signature Standard (DSS)
FIPS 186-5	Digital Signature Standard (DSS)
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS-140-2 Annex C	Approved Random Number Generators for FIPS PUB140-2

B.1 Nationale Berichte

- Rechnungshofbericht 2023 über „Intelligente Messegeräte (Smart Meter) – Einführungsstand 2022"
- E-Control Austria Monitoring Bericht 2024: „Bericht zur Einführung von intelligenten Messgeräten in Österreich 2024 – Berichtsjahr 2023".
- E-Control Austria Monitoring Bericht 2025: „Bericht zur Einführung von intelligenten Messgeräten in Österreich 2025 – Berichtsjahr 2024".

B.2 Normen

Es gelten die jeweils aktuellen Fassungen zum Zeitpunkt der Erstellung dieses Dokuments. Bezüglich Security müssen jedenfalls alle Normen des Dokumentes „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ eingehalten werden. Diese sind hier nicht extra angeführt.

Welmec	
Welmec Guide 7.2	Software Guide
Welmec Guide 11.1	Common application for utility meters
Welmec Guide 11.3	Guide for Sealing of Active Electrical Energy Meters and Gas Meters and Conversion Devices
Welmec Guide 11.5	Gas meters or Active electrical energy meters equipped with additional functionalities and ancillary devices
Welmec Guide 11.7	Modular evaluation of Active electrical energy meters
IEC/ISO	**Bezeichnung**
IEC Publ. 60529	Schutzarten durch Gehäuse (IP-Code)
ISO 75-1	Kunststoffe - Bestimmung der Wärmeformbeständigkeitstemperatur - Teil 1: Allgemeines Prüfverfahren
ISO 75-2	Kunststoffe - Bestimmung der Wärmeformbeständigkeitstemperatur - Teil 2: Kunststoffe und Hartgummi
ISO 75-3	Kunststoffe - Bestimmung der Wärmeformbeständigkeitstemperatur - Teil 3: Hochfeste duroplastische Laminate und langfaserverstärkte Kunststoffe
ISO 27001	*Information technology – Security techniques – Information security management systems – Requirements*
Europanormen	**Bezeichnung**
EN 50065-1	Signalübertragung auf elektrischen Niederspannungsnetzen im Frequenzbereich 3 kHz bis 526,5 kHz - Teil 1: Allgemeine Anforderungen, Frequenzbänder und elektromagnetische Störungen
EN 50065-2-3	Signalübertragung auf elektrischen Niederspannungsnetzen im Frequenzbereich 3 kHz bis 148,5 kHz - Teil 2-3: Störfestigkeitsanforderungen an Netz-Datenübertragungsgeräte und -systeme, die im Frequenzbereich 3 kHz bis 95 kHz betrieben werden und für den Gebrauch durch Stromversorgungs- und -verteilungsunternehmen bestimmt sind
EN 50470-1	Allgemeine Anforderungen, Prüfungen und Prüfbedingungen – Messeinrichtungen (Genauigkeitsklassen A, B und C)

EN 50470-3	Besondere Anforderungen – Elektronische Wirkverbrauchszähler der Genauigkeitsklassen A, B und C
EN 55011	Industrielle, wissenschaftliche und medizinische Geräte - Funkstörungen - Grenzwerte und Messverfahren (Basisdokument CISPR 11)
EN 55014-1	Elektromagnetische Verträglichkeit - Anforderungen an Haushaltgeräte, Elektrowerkzeuge und ähnliche Elektrogeräte - Teil 1: Störaussendung (Basisdokument CISPR 14-1)
EN 55014-2	Elektromagnetische Verträglichkeit - Anforderungen an Haushaltgeräte, Elektrowerkzeuge und ähnliche Elektrogeräte - Teil 2: Störfestigkeit - Produktfamiliennorm (Basisdokument CISPR 14-2)
EN 55022-CHRISPR22	Einrichtungen der Informationstechnik - Funkstöreigenschaften - Grenzwerte und Messverfahren (Basisdokument CISPR 22)
EN 55032	Elektromagnetische Verträglichkeit von Multimediageräten und Einrichtungen - Anforderungen an die Störaussendung (Basisdokument CISPR 32)
EN 60060-1	Hochspannungs-Prüftechnik - Teil 1: Allgemeine Begriffe und Prüfbedingungen
EN 61000-3-2 + A2	Elektromagnetische Verträglichkeit (EMV) - Teil 3-2: Grenzwerte - Grenzwerte für Oberschwingungsströme (Geräte-Eingangsstrom 16 A je Leiter)
EN 61000-4-2	Elektromagnetische Verträglichkeit (EMV) - Teil 4-2: Prüf- und Messverfahren - Prüfung der Störfestigkeit gegen die Entladung statischer Elektrizität
EN 61000-4-3	Elektromagnetische Verträglichkeit (EMV) – Teil 4-3: Prüf- und Messverfahren - Prüfung der Störfestigkeit gegen hochfrequente elektromagnetische Felder
EN 61000-4-4	Elektromagnetische Verträglichkeit (EMV) - Teil 4-4: Prüf- und Messverfahren - Prüfung der Störfestigkeit gegen schnelle transiente elektrische Störgrößen/Burst
EN 61000-4-5	Elektromagnetische Verträglichkeit (EMV) - Teil 4-5: Prüf- und Messverfahren - Prüfung der Störfestigkeit gegen Stoßspannungen
EN 61000-4-6	Elektromagnetische Verträglichkeit (EMV) - Teil 4-6: Prüf- und Messverfahren - Störfestigkeit gegen leitungsgeführte Störgrößen, induziert durch hochfrequente Felder
EN 61000-4-8	Elektromagnetische Verträglichkeit (EMV) - Teil 4-8: Prüf- und Messverfahren - Prüfung der Störfestigkeit gegen Magnetfelder mit energietechnischen Frequenzen
EN 62052-11	Elektrizitätszähler – Allgemeine Anforderungen, Prüfungen und Prüfbedingungen – Teil 11: Messeinrichtungen

EN 62052-21	Wechselstrom-Elektrizitätszähler - Allgemeine Anforderungen, Prüfungen und Prüfbedingungen -- Teil 21: Einrichtungen für Tarif- und Laststeuerung
EN 62053-21	Elektrizitätszähler - Besondere Anforderungen - Teil 21: Elektronische Wirkverbrauchszähler für Wechselstrom der Genauigkeitsklassen 0,5, 1 und 2
EN 62053-23	Elektrizitätszähler - Besondere Anforderungen - Teil 23: Elektronische Blindverbrauchszähler der Genauigkeitsklassen 2 und 3
EN 62053-24	Elektrizitätszähler - Besondere Anforderungen - Teil 24: Elektronische Grundschwingungs-Blindverbrauchszähler der Genauigkeitsklassen 0,5 S, 1 S, 1, 2 und 3
EN 62053-31	Einrichtungen zur Messung der elektrischen Energie (AC) - Besondere Anforderungen - Teil 31: Impulseinrichtungen für Induktionszähler und elektronische Zähler
EN 62053-52	Wechselstrom-Elektrizitätszähler - Besondere Anforderungen - Teil 52: Symbole
EN 62054-11, -21	Elektrizitätszähler Zusatzeinrichtungen Teil 11: Anforderungen an Impulsgeber Elektrizitätszähler Zusatzeinrichtungen Teil 21: Impulsgeber für Wechselstromzähler
EN 62054-21	Wechselstrom-Elektrizitätszähler - Tarif- und Laststeuerung - Teil 21: Besondere Anforderungen an Schaltuhren
EN 62056-21	Messung der elektrischen Energie - Zählerstandsübertragung, Tarif- und Laststeuerung - Teil 21: Datenübertragung für festen und mobilen Anschluss
EN 62056-46	Messung der elektrischen Energie - Zählerstandsübertragung, Tarif- und Laststeuerung - Teil 46: Anwendung des HDLC-Protokolls in der Verbindungsschicht
EN 62056-4-7	Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM -- Teil 4-7: DLMS/COSEM Transportschicht für IP-Netzwerke
EN 62056-5-3	Datenkommunikation der elektrischen Energiemessung - DLMS®/COSEM - Teil 5-3: DLMS®/COSEM-Anwendungsschicht
EN 62056-6-1	Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM - Teil 6-1: COSEM Object Identification System (OBIS)
EN 62056-6-2	Datenkommunikation der elektrischen Energiemessung - DLMS®/COSEM - Teil 6-2: COSEM Interface-Klassen

EN 62056-8-5	Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM - Teil 8-5: Schmalband-OFDM-G3-PLC-Kommunikationsprofil für Nachbarschaftsnetzwerke
EN 62056-8-6	Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM -- Teil 8-6: Schnelles PLC-ISO/IEC-12139-1-Profil für Areal-Netze
DIN/DIN-VDE Normen	**Bezeichnung**
DIN 43856	Elektrizitätszähler, Tarifschaltuhren und Rundsteuerempfänger; Schaltungsnummern, Klemmenbezeichnungen, Schaltpläne
DIN 43857-1	Elektrizitätszähler in Isolierstoffgehäusen, für unmittelbaren Anschluß, bis 60 A Grenzstrom; Hauptmaße für Wechselstromzähler
DIN 43857-2	Elektrizitätszähler in Isolierstoffgehäusen, für unmittelbaren Anschluß, bis 60 A Grenzstrom; Hauptmaße für Drehstromzähler
DIN 43857-3	Elektrizitätszähler in Isolierstoffgehäusen, für unmittelbaren Anschluß, bis 60 A Grenzstrom; Hauptmaße des Klemmendeckels für Wechselstromzähler
DIN 43859	Elektrizitätszähler für Wandleranschluss; Hauptmaße für Drehstromzähler
DIN VDE 0160 05.88	Ausrüstung von Starkstromanlagen mit elektronischen Betriebsmitteln (mit Änderung A1/04.89 und A2/10.88)
Allgemeines	**Bezeichnung**
IEC 13 (SEC) 1022	Zuverlässigkeitsanforderungen an elektronische Zähler
OVE-Richtlinie R 21	Zähleranschlussklemmen
ÖVE-Richtlinie R-23-1	Elektrische, magnetische und elektromagnetische Felder im Frequenzbereich von 0 Hz bis 300 GHz -- Teil 1: Begrenzung der Exposition von Personen der Allgemeinbevölkerung
FNN-Leitfaden	Leitfaden zur Bewertung der Zuverlässigkeit und Messbeständigkeit von Elektrizitätszählern und Zusatzeinrichtungen
DSMR P1	Dutch Smart Meter Requirements P1 Companion Standard - Version 5.0.2 Final, 2016
OIML 11	Allgemeine Anforderungen an elektronische Messgeräte
OIML 12	Anforderungen an geeichte Messgeräte
ÖNORM A-7700	Sicherer Betrieb von Webapplikationen
Use Cases	
Blue Book Part 1	DLMS UA 1000-1 Ed. 18 Part 1 - IEC 62056-6-1, Comprehensive Semantic Model for Energy

	Management, OBIS CODES
Blue Book Part 2	DLMS UA 1000-1 Ed. 18 Part 2 - IEC 62056-6-2, Comprehensive Semantic Model for Energy Management, COSEM Interface Classes
Green Book	DLMS UA 1000-2 Ed.12 V1.0 - - IEC 62056-5-3, DLMS/COSEM Architecture and Protocols
White Book	DLMS UA 1002:2003, First Edition reflects most important terms
Yellow Book	DLMS/COSEM Conformance Testing Process
IDIS Package 3, Smart Metering Objects	IDIS Interoperability Specification, Package 3 Smart Metering Objects
GCP	AC Electricity Smart Meter Generic Companion Profile (GCP) DLMS UA 1015-1 Ed. 1
ITU-T G.9901	Narrowband Orthogonal Frequency Division Multiplexing Power Line Communication Transceivers – Power Spectral Density Specification ITU-T G.9901 (06/17) ITU-T G.9901 (2017) Corrigendum 1 (11/22) ITU-T G.9901 (2017) Amendment 1 (04/23)
ITU-T G.9903	Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC network ITU-T G.9903 2017-08-13 ITU-T G.9903 (2017) Amd. 1 (05/21) ITU-T G.9903 (2017) Cor. 1 (03/23) ITU-T G.9903 (2017) Amd. 2 (03/23)
G3 Specification	Narrowband OFDM Power Line Communication and Radio Frequency Transceivers for G3 networks G3-Alliance G3 Specifications (07/2025)
G3 Certification	Performance test suite for G3 device certification
3GPP	3GPP Alliance Technical Specifications
RFC 5905	NTPv4 Specification from June 2010
RFC 6918	ICMP Specification
RFC 8200	ICMPv6 Specification
IETF_SSH	A. Spaghetti, "SSH File Transfer Protocol," Internet-Draft, Internet Engineering Task Force (IETF), Jul. 2025

Oesterreichs Energie Companion Standard
Smart Meter 2.0

B.3_OE_CS_Anhang_Schnittstellen_Details

Version 1.0

31.03.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Architektur des Zählersystems 3

B. Einführung und Umfang 4

B.1 Allgemeine Anforderungen zu den remote Schnittstellen G1 und G2 5

B.2 Übersicht der DLMS/COSEM-Clients 6

C. Schnittstellen im Detail 9

C.1 Schnittstelle G1 10

C.2 Schnittstelle G2 15

C.3 Schnittstelle C 21

C.4 Modulschnittstelle M1 23

C.5 Serviceschnittstelle SZ 24

C.6 Kundenschnittstelle H1 28

C.7 Steuerausgänge SA 29

A. Architektur des Zählersystems

Das Architekturbild gilt für direkte als auch (halb-)indirekte Smart Meter 2.0. Ein Breaker ist ausschließlich bei direkten Smart Meter 2.0 vorgesehen.

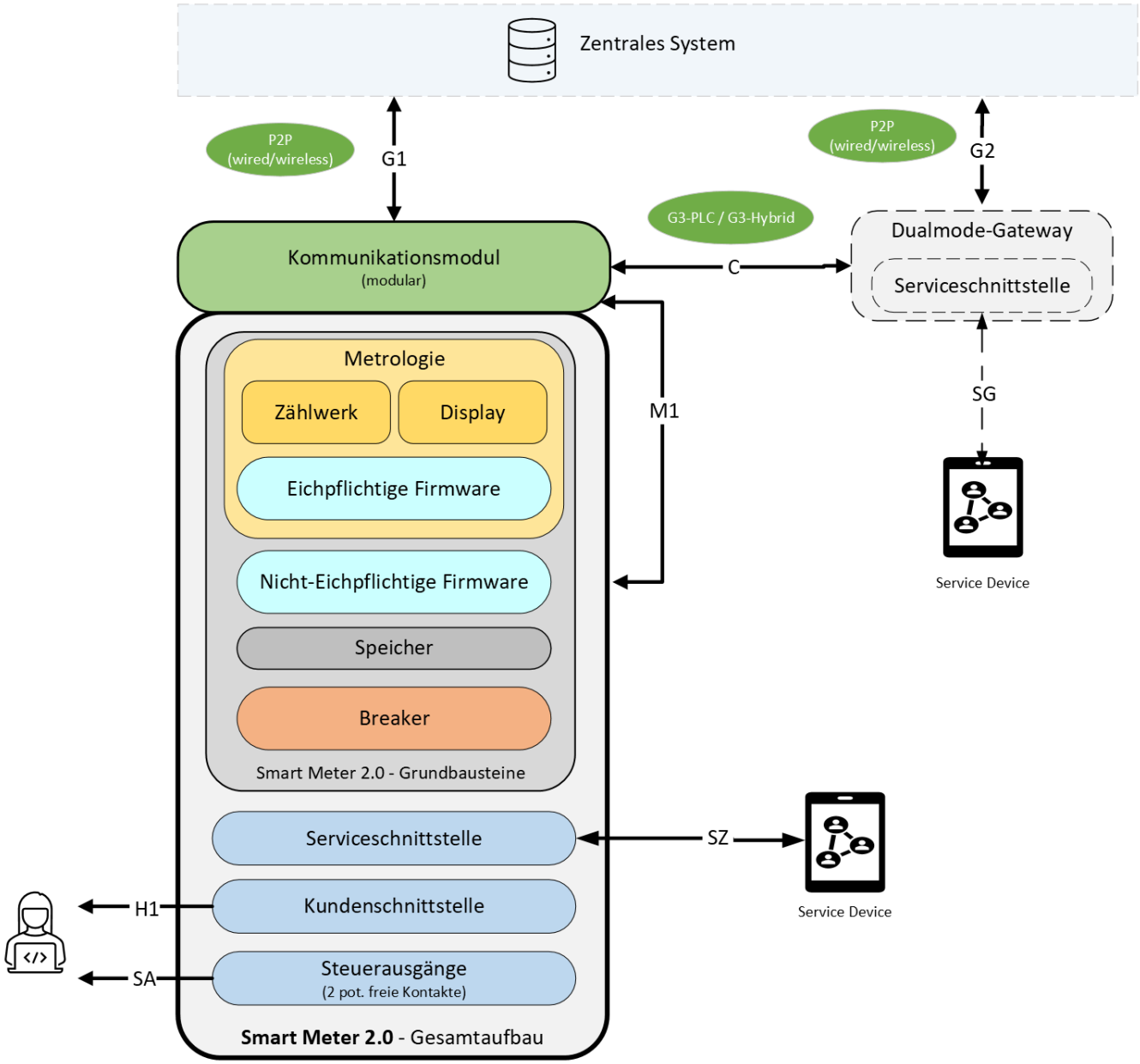


Abbildung 1: Gesamtaufbau des Smart Meters 2.0. Der Breaker ist nur für die Direktmessung vorgesehen.

B. Einführung und Umfang

Dieses Dokument legt die verbindlichen Anforderungen an die Schnittstellen des Smart Meter 2.0 fest. Es dient als technische Grundlage für Hersteller, die sowohl Hardware als auch Software entwickeln, um die geforderten Kommunikations- und Integrationsfunktionen bereitzustellen.

Ziel ist es, eine einheitliche und standardkonforme Umsetzung der Schnittstellen sicherzustellen, sodass eine reibungslose Integration in zentrale Plattformen gewährleistet ist. Die Beschreibung orientiert sich an einem vierstufigen Schichtenmodell (Anwendung, Transport, Vermittlung, Netzzugang), um die Protokolle und deren Einsatzbereiche klar zu definieren.

Jede Schnittstelle wird zunächst in ihrer Funktion und ihrem Zweck beschrieben und anschließend detailliert nach den vier Schichten spezifiziert. Die technischen Details verweisen auf die jeweils relevanten Normen und Standards, um sowohl Interchangeability, Interoperabilität, als auch regulatorische Konformität sicherzustellen.

B.1 Allgemeine Anforderungen zu den remote Schnittstellen G1 und G2

Die Anbindung an diese Schnittstellen wird via Kommunikationsmodul umgesetzt.

Der Einbau oder Tausch eines Kommunikationsmoduls muss ohne Verletzung der Werksplombe möglich sein. Weiters müssen die Module im Gehäuse so ausgeführt werden, dass ein Tausch auch von elektrotechnischen Laien durchgeführt werden darf. Die Spannungsversorgung des Moduls erfolgt auf der ungezählten Seite direkt aus dem Smart Meter 2.0.

Der Tausch des Moduls muss im laufenden Betrieb des Smart Meters möglich sein und ist im Dokument „Oe_UC-03 Communication Module Management.pdf“ definiert.

Es müssen unterschiedlichste Kommunikationsmodule (P2P; PLC, Ethernet, …) beliebig austauschbar sein.

B.1.1 Sicherer DLMS-Verbindungsaufbau

Die Schnittstellen müssen mindestens DLMS/COSEM Security Suite 2 nach Green Book unterstützen. Höhere und Security Standards sind zulässig.

Folgende Ausprägung ist dabei vorzusehen:

- High Level Security 5 **(HLS5)** gemäß DLMS/COSEM.
- High Level Security 7 **(HLS7)** gemäß DLMS/COSEM.

Der Verbindungsaufbau ist in folgendem Diagramm dargestellt. Weitere Informationen und Details zum Aufbau sind in Green Book beschrieben.

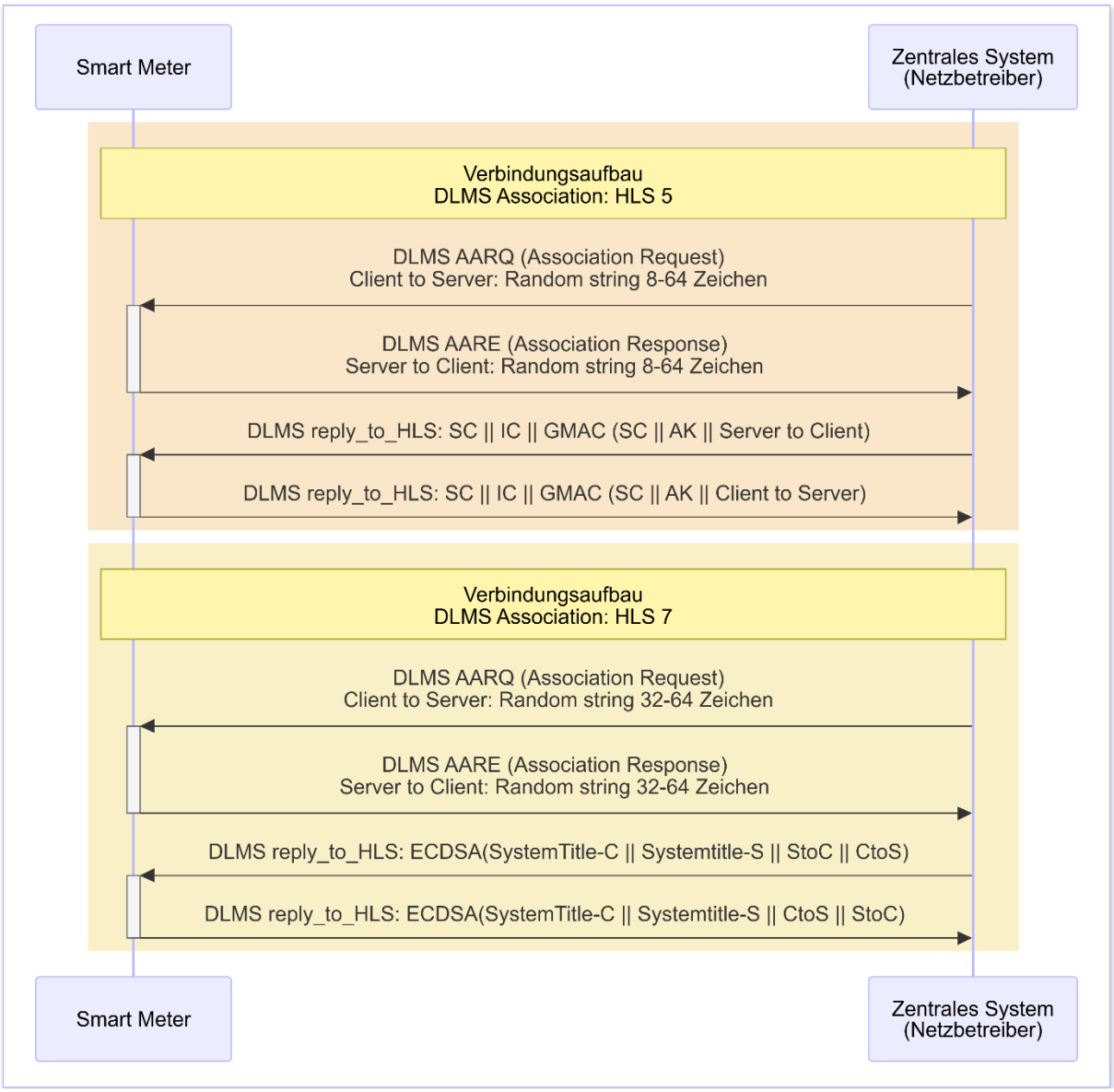


Abbildung 2: DLMS-Verbindungsaufbau mit HLS5 und HLS7

B.2 Übersicht der DLMS/COSEM-Clients

Der folgende Sicherheitsaspekt muss von den DLMS/COSEM-Clients erfüllt werden:

- Kein DLMS/COSEM-Client, dessen Verwendung kryptographisches Material erfordert, darf sowohl Remote als auch Lokal verwendet werden

Folgende DLMS/COSEM-Clients müssen vom Smart Meter 2.0 unterstützt werden:

Tabelle 1 Übersicht der DLMS/COSEM-Clients

Client-ID	Client-Titel	Service	Verwendung
1	management	Remote	Der management Client wird ausschließlich vom zentralen System für die WAN-Kommunikation über die Schnittstellen WAN G1 und WAN G2 genutzt. Er verfügt über sämtliche Berechtigungen, die für die Installation, Wartung und den Betrieb des Smart Meters 2.0 erforderlich sind. Bsp.: remote Admin Rolle für Firmware Updates, Konfigurationsänderungen, Schaltungen
2	data readout	Remote	Der data readout Client wird vom zentralen System zur Auslesung von Bewegungsdaten und zum Monitoring verwendet. Bsp.: automatische periodische und ad hoc Datenauslesetasks
3	fw upload	Remote	Der fw upload Client wird ausschließlich vom Dualmode-Gateway zum Upload der Firmware des Smart Meters 2.0 verwendet. Bsp.: Broadcasting für Firmware Upload ohne Aktivierung
4	comms mgmt	Remote	Der comms mgmt Client wird für spezifische Parametrierungen der Kommunikationstechnologie eingesetzt. Bsp.: Änderung spezifischer Kommunikations-parameter über ein separates System, zB. PLC Management System
5	readout_gw	Remote	Der readout_gw Client wird ausschließlich vom Dualmode-Gateway verwendet, um Bewegungsdaten und Monitoring-Daten vom Smart Meter 2.0 abzufragen. Bsp.: automatische periodische Datenauslesungen, zB. Lastprofile

6	maintenance	Lokal	Der maintenance Client wird lokal für Wartungszwecke eingesetzt. Bsp.: remote Admin Rolle für Firmware Updates, Konfigurationsänderungen, Schaltungen
7	certification	Lokal	Der certification Client wird lokal für die Prüfung/Eichung von Smart Metern in Österreich verwendet. Bsp.: für externe Eich- oder Zertifizierungsstellen ohne kritische Befehle.
16	public	Remote & Lokal	Mit dem public Client wird die Verfügbarkeit des Smart Meters und die Abfrage des Framecounters ermöglicht. Bsp.: im Bedarfsfall Auslesen des Framecounters einer spezifischen Rolle
20	security officer	Remote	Der security officer Client wird zum Tausch von Schlüsselmaterial eingesetzt.
102	pre-established	Remote	Der pre-established Client erlaubt es dem Smart Meter 2.0, Alarme oder Events an das zentrale System zu senden. Bsp.: Push Kommunikation
103	CII	Lokal	Der lokale CII Client dient der Ausgabe der Messwerte über die Kundenschnittstelle. Bsp.: für Kund*innen

Im Folgenden wird eine Übersicht über die DLMS/COSEM-Clients, die Usecases sowie die Schnittstellen gegeben, die für die Ausführung der jeweiligen Usecases mit dem zugehörigen Client verantwortlich sind.

Usecase	Remote Schnitstellen			Lokale Schnittstellen	
	G1	G2	C	SZ	H1
UC1 Meter Registration	management			maintenance	
UC2 Remote (& local) Tariff Programming	management			maintenance certification	
UC3 On Demand Meter Register reading for multi-utility meters	data readout management			maintenance certification	
UC4 On Demand Meter Load Profile reading for multi-utility meters	data readout management			maintenance certification	
UC5 Periodic Meter reading for multi-utility meters	data readout management		readout_gw		
UC6 Remote or local Disconnection and Reconnection (E, G)	management			maintenance	
UC7 Clock Synchronization	management			maintenance certification	
UC8 Quality of Supply	data readout management		readout_gw	maintenance	
UC9 Load Management by relay (E only)	management			maintenance	
UC10 Firmware update	management		fw upload	maintenance	
UC11 Meter supervision	management			maintenance	
UC12 Consumer Information	management			maintenance	CII
UC13 Communication Supervision	data readout management comms mgmt			maintenance	
UC14 Enabling / disabling functionalities	management			maintenance certification	
UC15 Power Control	management			maintenance	
UC16 Alarm and event Management	data readout management pre-established			maintenance	
UC17 Meter Availability Control	public				
UC18 Display messages on meter display	management			maintenance certification	
UC19 Configuration of meter locally				maintenance	
UC20 Manage security settings	public security officer		public	public	
UC21 Prepayment					
UC Oe-01 Communications configuration	management comms mgmt			maintenance	
UC Oe-02 Calibration & maintenance				maintenance certification	
UC Oe-03 Communications Module exchange	management comms mgmt			maintenance	

Abbildung 3: Übersicht Usecases zu Schnittstellen zu DLMS Clients

C. Schnittstellen im Detail

C.1 Schnittstelle G1

Die G1 Schnittstelle ist eine **bidirektionale** Punkt-zu-Punkt (P2P) Verbindung über die Ferne zwischen einem Smart Meter 2.0 und dem Zentralem System.

C.1.1 Allgemeine Informationen zur Schnittstelle G1

Die Umsetzung der G1 Schnittstelle basiert auf der in GCP-Kapitel 4 definierten Schnittstelle I3.2. Präzisierungen der GCP zur Schnittstelle I3.2 sind im Dokument „H.2_OE_CS_Annex.pdf“ festgelegt.

Die Schnittstelle unterstützt die nachfolgenden Kommunikationstechnologien. Weiterführende Details zu den Kommunikationstechnologien sind in „D.3_OE_CS_Implementation_Guide_Mobilfunk.pdf“ und „D.4_OE_CS_Implementation_Guide_Ethernet.pdf“ definiert.

Wireless:

- LTE-M (UE Cat.M1)
- LTE-M (UE Cat.M2) wenn verfügbar
- LTE NB-IoT (UE Cat.NB2)
- LTE (UE Cat.1bis)
- LTE (UE CAT.1)

Wired:

- Ethernet

Hinweis: In den Kommunikationstechnologien LTE-M1 und LTE CAT-1 muss auch die Frequenz 450Mhz nutzbar sein.

C.1.2 Kommunikationsprofil & Services der Schnittstelle G1

Die DLMS/COSEM Kommunikation basiert auf TCP/UDP via IPv4 und IPv6 Stack in Kombination mit der 3GPP folgendem GSM/LTE Netzzugangsschicht.

Die Kommunikation folgt dem im GCP Kapitel 6 definierten Client und Server Modell. Die unterstützten Clients über die G1 Schnittstelle sind in C.1.3.1 Anwendungsschicht festgelegt. Präzisierungen der GCP zum Client und Server Model sind im Dokument „H.2_OE_CS_Annex.pdf“ festgelegt.

C.1.3 Schichtmodell der Schnittstelle G1

Die folgende Grafik stellt das Schichtmodell der Schnittstelle dar. Weitere Informationen zu den einzelnen Schichten befinden sich in den jeweiligen Unterkapiteln.

Der Verbindungsaufbau, Profile und Services zur Kommunikation via DLMS/COSEM folgen dem DLMS-Standard in Green Book Kapitel 10.3, wobei die Schnittstelle G1 für die Kommunikation über das „Wide Area Network“ verwendet wird.

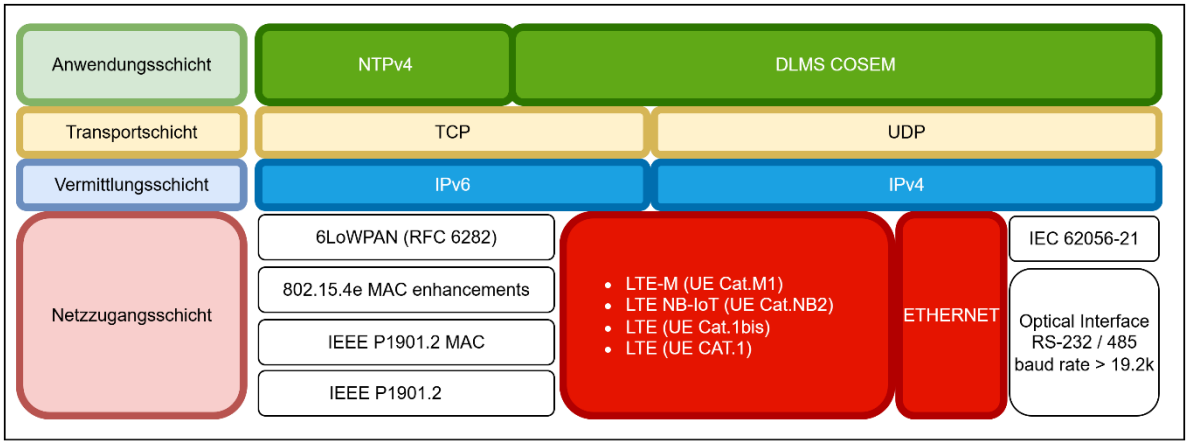


Abbildung 4: OSI Schichtmodell der Schnittstelle G1

C.1.3.1 Anwendungsschicht

Die Anwendungsschicht erlaubt zusätzlich zur DLMS/COSEM Kommunikation auch die Zeitsynchronisation, woraus sich zwei Protokolle der Anwendungsschicht ergeben.

(1) DLMS / COSEM

Die Anwendungsschicht umfasst den DLMS/COSEM Standard nach Blue Book Part 2. Das umzusetzende Objektmodell ist in „D.1_OE_CS_Objektmodel.pdf“ definiert.

Die von der G1 Schnittstelle verwendeten DLMS-Clients und die unterstützten OE Use-Cases sind in B.2 Übersicht der DLMS COSEM Clients zu finden.

(2) NTPv4

Die Zeitsynchronisation mithilfe von NTPv4 (NTP setup (class_id = 100)) ist zulässig und kann als alternative Lösung genutzt werden, falls die korrekte Zeit über DLMS nicht verfügbar ist. Siehe GCP Kapitel 8.8.

Die Umsetzung der NTP-Kommunikation erfolgt nach RFC 5905.

C.1.3.2 Transportschicht

Die Transportschicht folgt der Implementierung im Green Book Kapitel 7.2.4.2

- UDP nach Green Book Kapitel 7.2.3
- TCP nach Green Book Kapitel 7.2.4

Die Verwendung von TCP oder UDP wird via COSEM Objekt konfiguriert. Die Umsetzung folgt GCP Kapitel 6.8.

C.1.3.3 Vermittlungsschicht

Dem DLMS Green Book folgend werden sowohl

- IPv4 nach RFC 791 als auch
- IPv6 nach RFC 8200 unterstützt.

Die Verwendung von IPv4 oder IPv6 wird via COSEM Objekt konfiguriert. Nähere Details dazu in GCP Kapitel 6.8 oder Blue Book Part 2 Kapitel 4.9.2 (IPv4 setup Class ID 42)) bzw. Blue Book Part 2 Kapitel 4.9.3. (IPv6 setup (Class ID 48).

Als initiale Variante der Lieferkonfiguration ist IPv4 vorzusehen.

C.1.3.4 Netzzugangsschicht

Folgende Kapitel beschreiben die unterschiedlichen Optionen der Kommunikation. Details sind in „D.3. Implementation_Guide_Mobilunk.pdf“ erläutert.

Neben Ethernet werden folgende Varianten nach 3GPP unterstützt, welche gemäß 3GPP zumindest Release 14 compliant umgesetzt werden müssen.

(1) Wireless

Folgende Technologien sind zu unterstützen:

- LTE-M (UE Cat.M1)
- LTE NB-IoT (UE Cat.NB2)
- LTE (UE Cat.1bis)
- LTE (UE CAT.1)

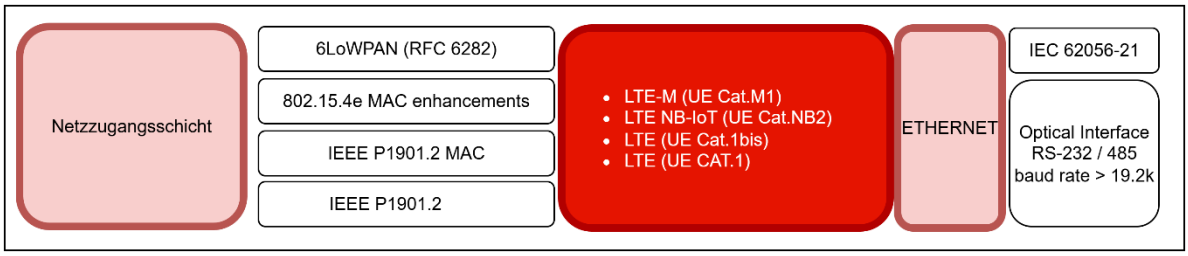


Abbildung 5: OSI Schichtmodell wireless G1

(2) Wired

Folgende Technologien sind zu unterstützen:

- Ethernet

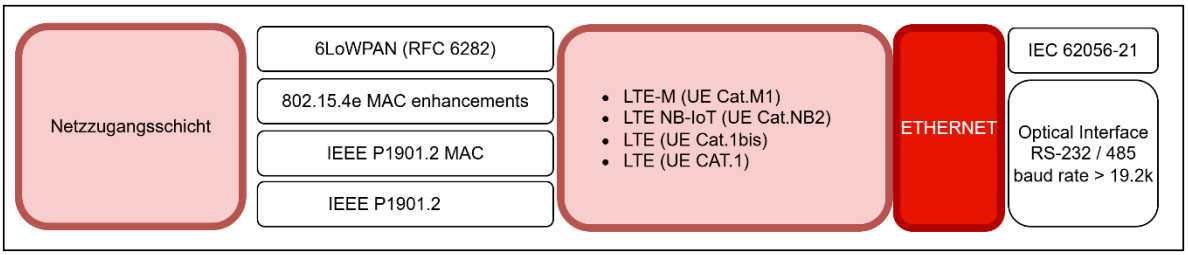


Abbildung 6: OSI Schichtmodell wirled G1

C.1.4 Kommunikationsablauf

Die Kommunikation zwischen zentralem System und Smart Meter 2.0 erfolgt mit den folgenden nach GCP Kapitel 4.2 Operationsmodus:

- PULL-Kommunikation initiiert vom Zentralen System
- PUSH-Kommunikation initiiert vom Smart Meter 2.0
- PULL-PUSH-Kommunikation initiiert vom Zentralen System

Hinweis PULL-PUSH: Mittels PULL Request wird ein im Smart Meter 2.0 definierter Push Datensatz an das zentrale System übertragen.

C.1.5 Schematische Darstellung des Kommunikationsaufbaues

In folgendem Sequenzdiagramm wird der erste Kommunikationsaufbau im Detail beschrieben.

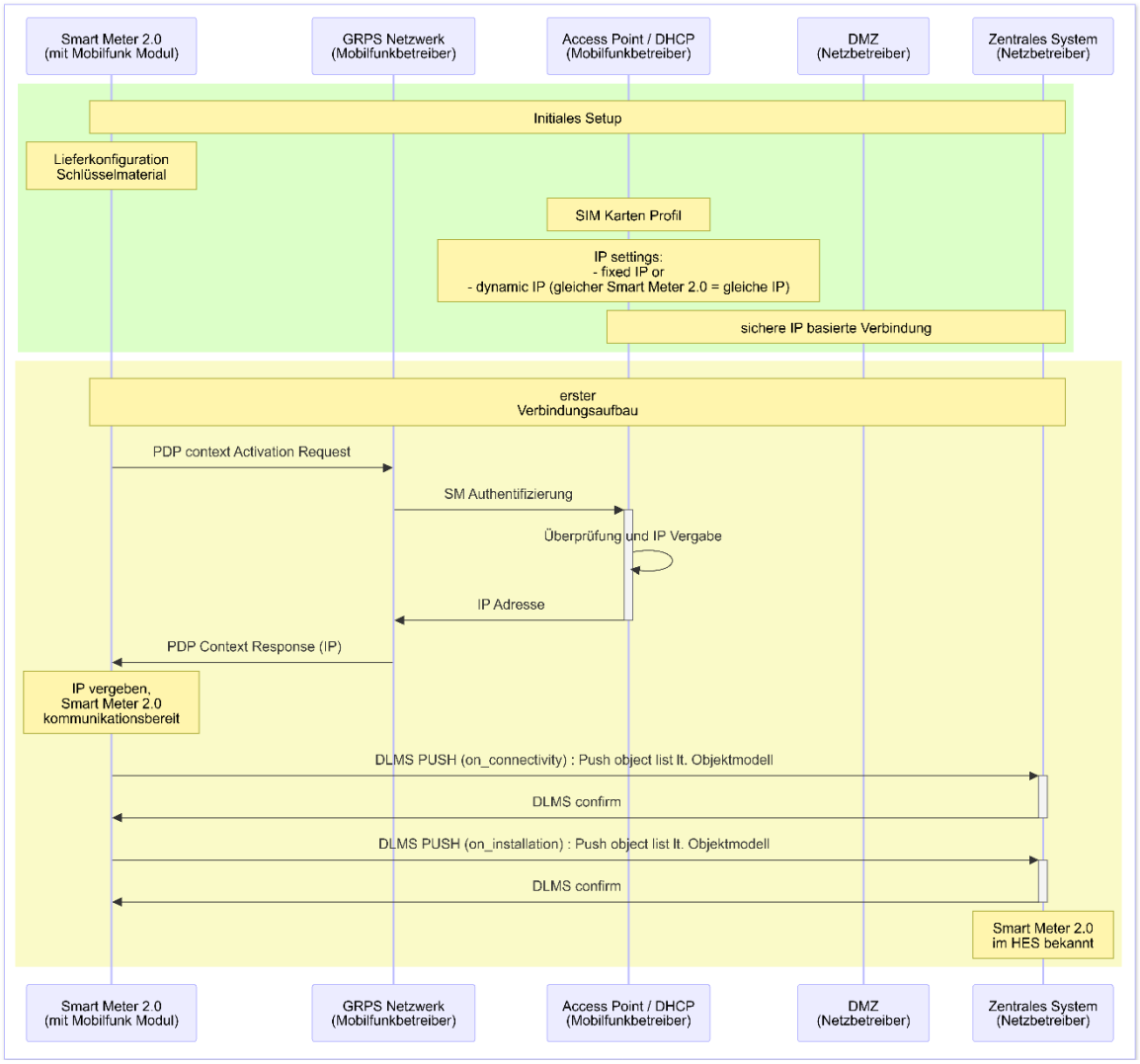


Abbildung 7: Erster Verbindungsaufbau der Kommunikation via Mobilfunk-Strecke

Das initiale Setup im Sequenzdiagramm erfolgt nach Prozess im Green Book Kapitel 9.2.6.3.3 und entsprechende Objekte im Blue Book.

Die Zähler sind bei Auslieferung mit gültigen Zertifikaten auszustatten, deren Gültigkeitsbeginn dem Jahr der Auslieferung entspricht.

C.1.6 Schematische Darstellung der PULL und PUSH Operationsmodus

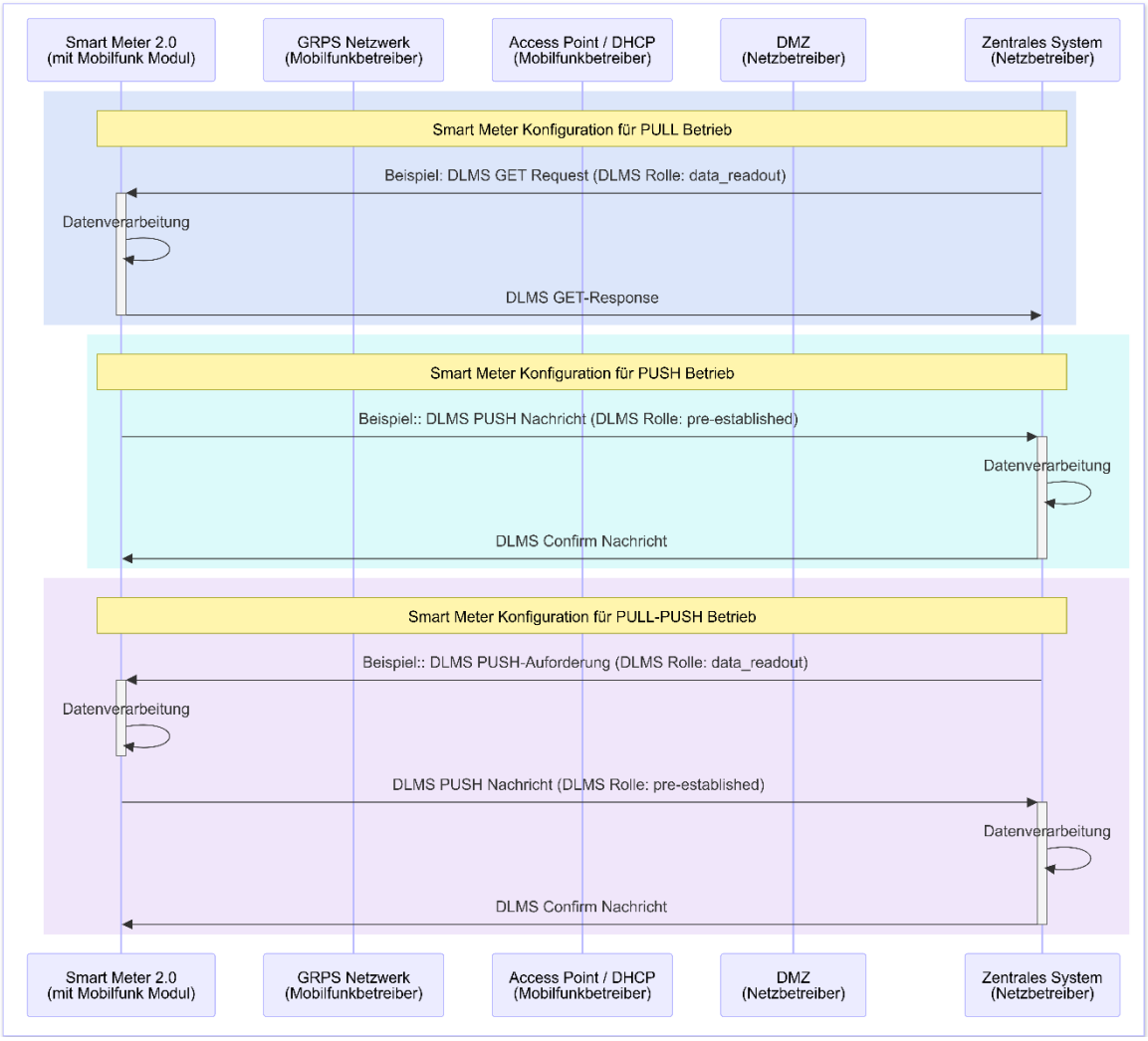


Abbildung 8: Sicherer Verbindungsaubau und PULL / PUSH Betrieb der Mobilfunk-Strecke

C.1.7 Sicherheitsmechanismen

Die Sicherheitsmechanismen sind in E2E Security Informationen bzw. GCP Kapitel 7 definiert.

Die G1 Schnittstelle muss der in Kapitel B.1.1 Sicherer DLMS Verbindungsaufbau beschriebenen Security Suite abgesichert sein.

Die Verwendung von **DLMS/COSEM Security Suite 0 und 1** nach GCP Kapitel 7.1 muss möglich sein, um eine Abwärtskompatibilität zu gewährleisten.

C.2 Schnittstelle G2

Über diese bidirektionale Schnittstelle wird der Smart Meter 2.0 über ein Dualmode-Gateway an das zentrale System angebunden. Der Kommunikationsaufbau erfolgt entweder vom Smart Meter 2.0 oder vom zentralen System. Das Dualmode-Gateway leitet die Kommunikation unverändert via Schnittstelle LAN C physisch weiter.

C.2.1 Allgemeine Informationen zur Schnittstelle G2

Die Umsetzung der G2 Schnittstelle basiert auf der in GCP Kapitel 4 „System Architecture“ definierten Schnittstelle I3.1. Präzisierungen der GCP zur Schnittstelle I3.1 sind im Dokument „H.2_OE_CS_Annex.pdf“ festgelegt.

Die Kommunikation dieser Schnittstelle lässt sich wie folgt aufteilen:

Tabelle 2: Übersicht der Verbindungen von G2

Verbindung	Schicht	Schnittstelle
Smart Meter und Dualmode-Gateway	Anwendungsschicht	G2
	Transportschicht	G2
	Vermittlungsschicht	G2
	Netzzugangsschicht	via Schnittstelle C
Dualmode-Gateway und zentrales System	Anwendungsschicht	G2
	Transportschicht	G2
	Vermittlungsschicht	G2
	Netzzugangsschicht	im CS 2.0 nicht eingeschränkt

Hervorzuheben ist, dass die Schnittstelle G2 die logische Verbindung nach auf DLMS/COSEM darstellt und unabhängig der physischen Übertragung (Netzzugangsschicht) ist.

C.2.2 Kommunikationsprofil & Services der Schnittstelle G2

Die DLMS/COSEM Kommunikation basiert auf UDP via IPv6 Stack über eine G3-PLC/G3-Hybrid Anbindung des Smart Meters 2.0 an ein Dualmode-Gateway nach dem G3-PLC/G3-Hybrid Standard (G3-PLC).

Die Kommunikation folgt der im GCP Kapitel 6 definierten Client und Server Modell. Die unterstützten Clients über die G2 Schnittstelle sind in C.1.3.1 Anwendungsschicht festgelegt. Präzisierungen der GCP zum Client und Server Model sind im Dokument „H.2_OE_CS_Annex.pdf“ festgelegt.

C.2.3 Schichtmodell der Schnittstelle G2

Die folgende Grafik stellt das Schichtmodell der Schnittstelle dar. Weitere Informationen zu den einzelnen Schichten befinden sich in den jeweiligen Unterkapiteln.

Der Verbindungsaufbau, Profile und Services zur Kommunikation via DLMS/COSEM folgen dem DLMS Standard in Green Book Kapitel 10.3, wobei die Schnittstelle G2 für die Kommunikation über das „Neighbourhood network“ und „Local network“ verwendet wird.

Festlegungen zur Netzzungangsschicht zwischen Zentrales System und Dualmode-Gateway ist nicht Bestandteil des OE Campanion Standards. Es wird auf die Schnittstelle C verwiesen, um zu verdeutlichen, dass der Smart Meter 2.0 bei Verwendung der G2 Schnittstelle über G3-PLC bzw. G3-Hybrid auf der Netzzungangsschicht angebunden ist.

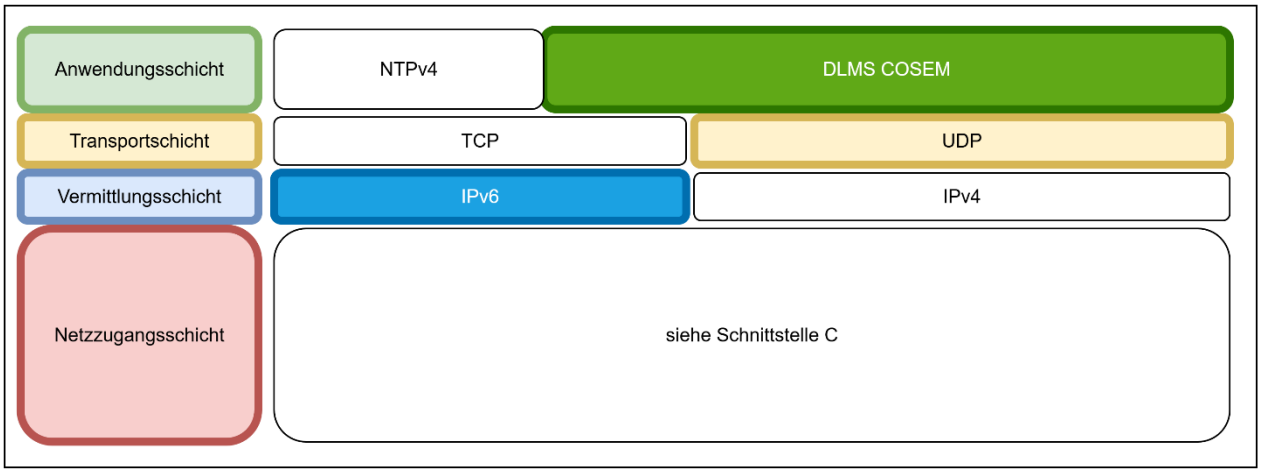


Abbildung 9: OSI Schichtmodell der Schnittstelle G2

C.2.3.1 Anwendungsschicht

Die Anwendungsschicht umfasst den DLMS/COSEM-Standard. Das umzusetzende Objektmodell ist in „D.1_OE_CS_Objektmodel.pdf“ definiert.

(1) DLMS/COSEM-Clients

Die von der G2 Schnittstelle verwendeten DLMS-Clients und die unterstützten OE Use-Cases sind in der Übersicht B.2 Übersicht der DLMS COSEM Clients zu finden.

C.2.3.2 Transportschicht

Die Transportschicht folgt der Implementierung im Green Book Kapitel 7.2.4.2

- UDP nach Green Book Kapitel 7.2.3

Die Verwendung von UDP wird via COSEM Objekt konfiguriert. Die Umsetzung folgt GCP Kapitel 6.8.

C.2.3.3 Vermittlungsschicht

Dem DLMS Green Book folgend wird IPv6 nach RFC 8200 unterstützt.

Die Verwendung von IPv6 wird via COSEM Objekt konfiguriert. Nähere Details dazu in GCP Kapitel 6.8.

C.2.3.1 Netzzugangsschicht

Folgende Kapitel beschreiben die unterschiedlichen Optionen der Kommunikation.

Die physische Verbindung wird via Schnittstelle C sichergestellt.

C.2.4 Kommunikationsablauf

Die Kommunikation zwischen zentralem System und Smart Meter 2.0 erfolgt mit den folgenden nach GCP Kapitel 4.2 Operationsmodus:

- PULL-Kommunikation initiiert vom Zentralen System
- PUSH-Kommunikation initiiert vom Smart Meter 2.0
- PULL-PUSH-Kommunikation initiiert vom Zentralen System

Hinweis PULL-PUSH: Mittels PULL Request wird ein im Smart Meter definierter Push Datensatz an das zentrale System übertragen.

C.2.5 Schematische Darstellung des Kommunikationsaufbaues

In folgendem Sequenzdiagramm wird der erste Kommunikationsaufbau im Detail beschrieben.

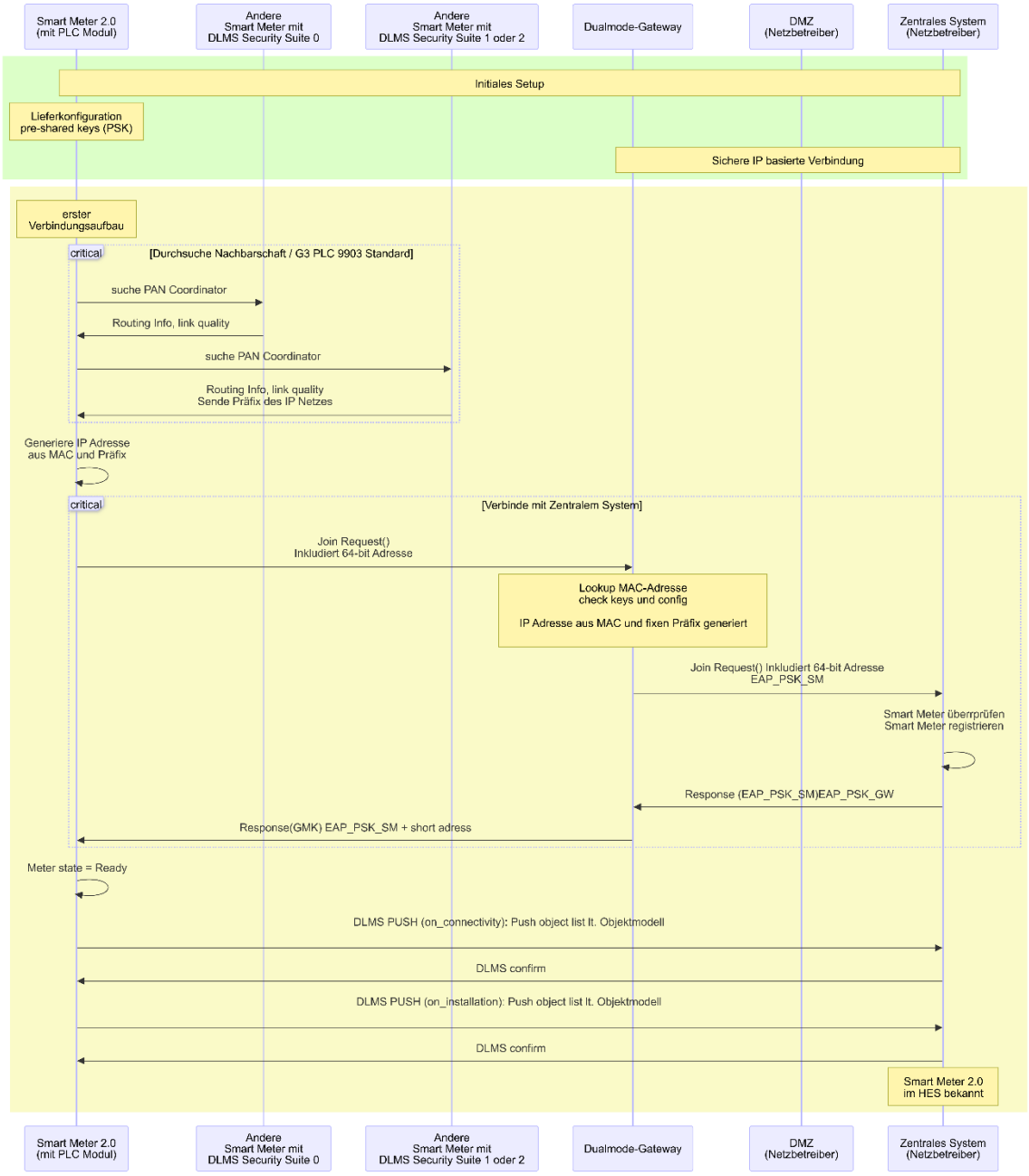


Abbildung 10: Erster Verbindungsaufbau der Kommunikation via G2 Schnittstelle.

Das initiale Setup im Sequenzdiagramm erfolgt nach Prozess im Green Book Kapitel 9.2.6.3.3 und entsprechende Objekte im Blue Book.

Die Zähler sind bei Auslieferung mit gültigen Zertifikaten auszustatten, deren Gültigkeitsbeginn dem Jahr der Auslieferung entspricht.

C.2.6 Schematische Darstellung der PULL und PUSH Operationsmodus

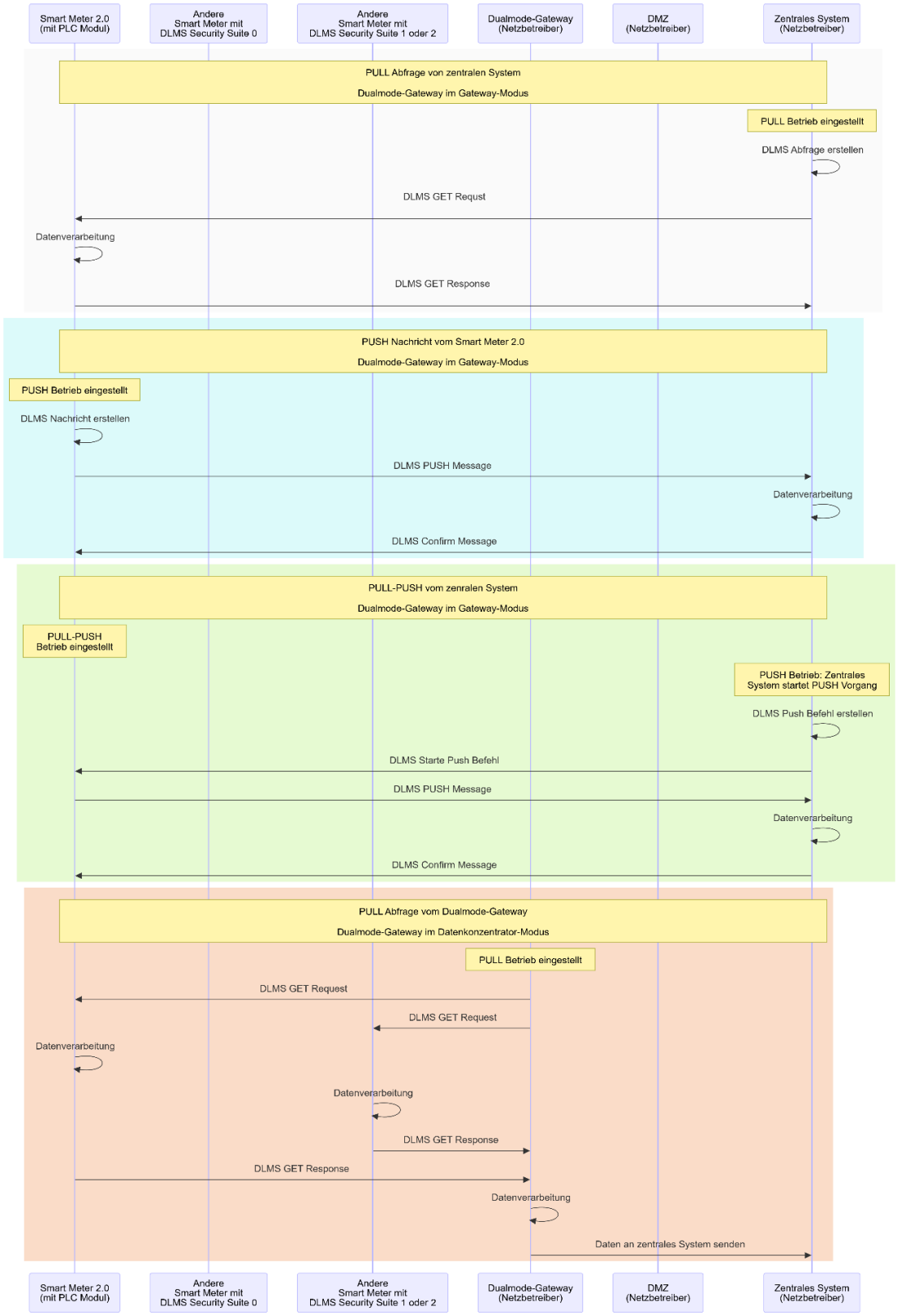


Abbildung 11: PULL und PUSH Operationsmodus

C.2.7 Sicherheitsmechanismen

Die Sicherheitsmechanismen sind in E2E Security Informationen bzw. GCP Kapitel 7 definiert.

C.2.7.1 DLMS Security Suites

Die Sicherheitsmechanismen sind in E2E Security Informationen bzw. GCP Kapitel 7 definiert.

Die G2 Schnittstelle muss der in Kapitel B.1.1 Sicherer DLMS Verbindungsaufbau beschriebenen Security Suite abgesichert sein.

Die Verwendung von **DLMS/COSEM Security Suite 0 und 1** nach GCP Kapitel 7.1 muss möglich sein, um eine Abwärtskompatibilität zu gewährleisten.

C.3 Schnittstelle C

Über diese bidirektionale Schnittstelle wird der Smart Meter 2.0 an ein Dualmode-Gateway angebunden.

Das Dualmode-Gateway kann gem. OE Ende-zu-Ende Sicherheit für Smart Metering auf folgende zwei Arten ausgeführt und betrieben werden:

- Als reines Gateway, welches ausschließlich eine transparente Kommunikationsverbindung zwischen dem Zentralen System und dem Smart Meter 2.0 herstellt. Siehe Schnittstelle G2.
- Als Dualmode-Gateway welches die Funktionen eines Datenkonzentrators mit Ausnahme von kritischen Funktionen übernimmt.

C.3.1 Allgemeine Informationen zur Schnittstelle C

Die Umsetzung der C Schnittstelle basiert auf der in GCP Kapitel 4 „System Architecture“ definierten Schnittstelle I3.1. Präzisierungen der GCP zur Schnittstelle I3.1 sind im Dokument „H.2_OE_CS_Annex.pdf“ festgelegt..

Die Kommunikation dieser Schnittstelle lässt sich je nach verwendetem Mode am Dualmode-Gateway wie folgt aufteilen:

Gateway-Mode

In diesem Modus wird die Kommunikation direkt zwischen Smart Meter 2.0 und dem zentralen System hergestellt.

- Die logische Verbindung (Anwendungs-, Transport- und Vermittlungsschicht) wird via G2 aufgebaut.
- Physisch wird die Übertragung zwischen Dualmode-Gateway und zentralem System im CS 2.0 nicht näher definiert. Die Umsetzung wird vom Netzbetreiber festgelegt.
- Die physische Weiterleitung der Pakete vom Dualmode-Gateway zum Smart Meter 2.0 erfolgt via Schnittstelle C

Datenkonzentrator-Mode

In diesem Modus findet die Kommunikation direkt zwischen Smart Meter 2.0 und Dualmode-Gateway statt.

- Die logische Verbindung (Anwendungs-, Transport- und Vermittlungsschicht) wird via DLMS/COSEM Kommunikation direkt mit dem Dualmode-Gateway aufgebaut. Diese Verbindung folgt technisch denselben Regeln wie G2.
- Die physische Weiterleitung der Pakete vom Dualmode-Gateway zum Smart Meter 2.0 erfolgt via Schnittstelle C

C.3.2 Schichtmodell der Schnittstelle C

Die folgende Grafik stellt das Schichtmodell der Schnittstelle dar. Weitere Informationen zu den einzelnen Schichten befinden sich in den jeweiligen Unterkapiteln.

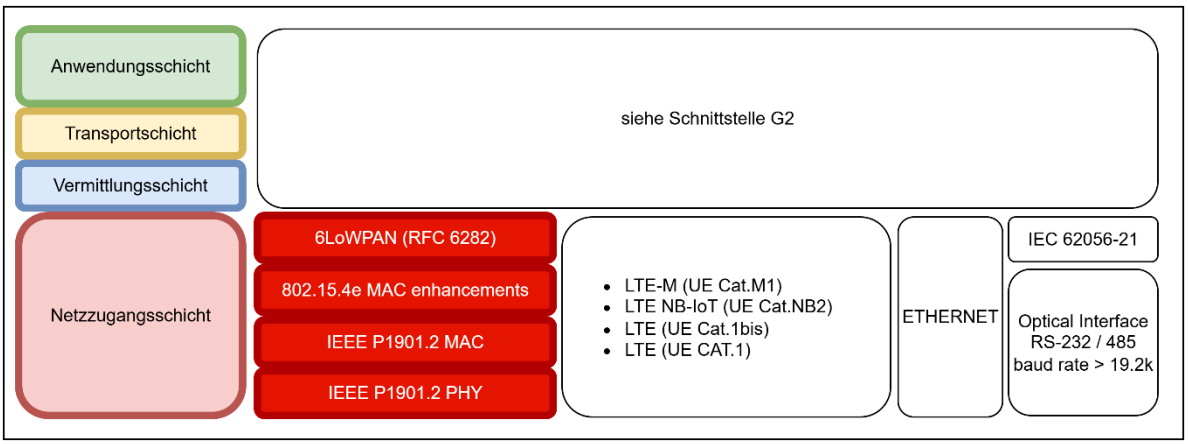


Abbildung 12: OSI-Schichtmodell der Schnittstelle C

C.3.2.1 Netzzugangsschicht

Die Verbindung folgt den Spezifikationen nach ITU-T G.9901 (Frequenzbänder) and ITU-T G.9903 (G3 PLC Standard und G3 PLC Hybrid) und muss G3-PLC konform umgesetzt sein. Siehe G3-PLC.

C.4 Modulschnittstelle M1

Die Modulschnittstelle M1 stellt die interne Kommunikation des Smart Meters 2.0 mit dem Kommunikationsmodul dar.

Die Modulschnittstelle M1 muss genügend elektrische Leistung zur Verfügung stellen, dass damit alle im P2P Guide geforderten UE PowerClasses bedient werden können.

Die Leistung an der Schnittstelle muss für die Energieversorgung von G3-PLC bzw. G3-Hybrid ausreichend sein.

C.4.1 Sicherheitsmechanismen

Es muss eine Verschlüsselung gemäß dem Stand der Technik umgesetzt werden.

C.5 Serviceschnittstelle SZ

C.5.1 Allgemeine Informationen SZ

Die Serviceschnittstelle ermöglicht die direkte, sichere und effiziente Kommunikation zwischen dem Smart Meter 2.0 und dem Service Device für Wartung, Konfiguration, Diagnose und Datenauslesung. Über diese Schnittstelle können autorisierte Servicetechniker Messdaten auslesen, Firmware-Updates durchführen, Parameter anpassen und Statusinformationen abrufen.

Die Kommunikation erfolgt über ein standardisiertes Protokoll (z. B. DLMS/COSEM) über die optische IR-Schnittstelle gemäß EN 62056-21.

C.5.2 Schichtmodell der Schnittstelle SZ

Die folgende Grafik stellt das Schichtmodell der Schnittstelle dar. Weitere Informationen zu den einzelnen Schichten befinden sich in den jeweiligen Unterkapiteln.

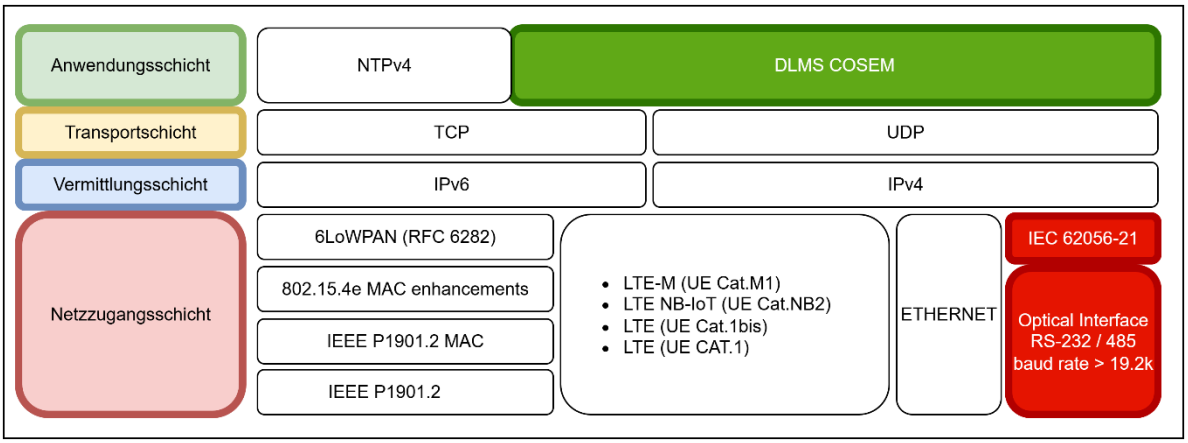


Abbildung 13: OSI-Schichtmodell der Schnittstelle SZ

C.5.2.1 Anwendungsschicht

Die Anwendungsschicht umfasst den DLMS/COSEM Standard. Das umzusetzende Objektmodell ist in „D.1_OE_CS_Objektmodel.pdf“ definiert.

(1) DLMS/COSEM Clients

Die von der SZ-Schnittstelle verwendeten DLMS-Clients und die unterstützten OE Use-Cases sind in der Übersicht B.2 Übersicht der DLMS COSEM Clients und im Objektmodell „D.1_OE_CS_Objektmodel.pdf“ zu finden.

C.5.2.2 Netzzugangsschicht

Die Serviceschnittstelle ist als optische Schnittstelle gem. EN 62056-21 auszuführen. Damit ist gewährleistet, dass die bestehenden Prüfeinrichtungen und Werkzeuge bei der Installation bzw. bei einer eventuellen Störungsbehebung auch zukünftig genutzt werden können.

Ziel ist die minimale und stabile Übertragungsrate von IR-Schnittstellen von mindestens 19.200 Baud auszunutzen.

C.5.3 Schematische Darstellung des Kommunikationsaufbaues und der Kommunikation im Regelbetrieb.

In folgendem Sequenzdiagramm wird der erste Kommunikationsaufbau im Detail beschrieben.

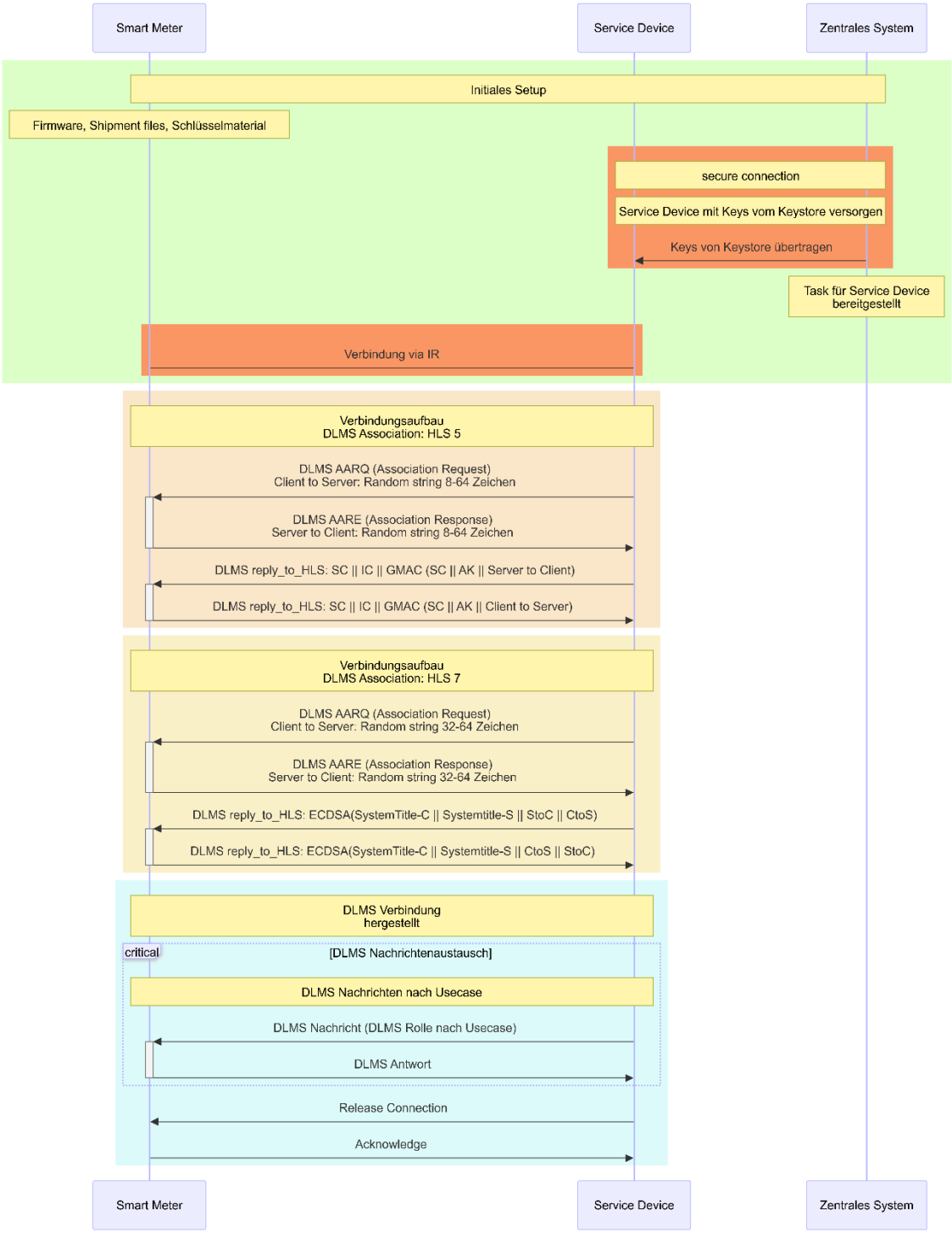


Abbildung 14: Darstellung der Kommunikation via Serviceschnittstelle

C.5.4 Sicherheitsmechanismen

Die Security hat die Vorgaben von E2E Security Informationen bzw. GCP Kapitel 7 zu erfüllen.

Die Serviceschnittstelle SZ muss mindestens **DLMS/COSEM Security Suite 2** unterstützen. Siehe dazu Green Book Kapitel 9.2.3.7. Höhere Security Standards sind zulässig.

Folgende Ausprägung ist dabei vorzusehen:

- High Level Security 5 **(HLS5)** gemäß DLMS/COSEM.
- High Level Security 7 **(HLS7)** gemäß DLMS/COSEM.

Die Verwendung von **DLMS/COSEM Security Suite 0 und 1** nach GCP Kapitel 7.1 muss möglich sein, um eine Abwärtskompatibilität zu gewährleisten.

C.6 Kundenschnittstelle H1

C.6.1 Allgemeine Informationen H1

Diese **unidirektionale** Schnittstelle H1 dient zur Bereitstellung von Daten im 1-Sekundenintervall und ist gemäß DSMR P1 auszuführen.

Die Schnittstelle muss ohne Öffnung des Klemmdeckels zugänglich sein und einen mechanischen Schutz gegen Verschmutzung aufweisen

Eine De-/Aktivierung der Kundenschnittstelle über das zentrale System und über die Serviceschnittstelle ist vorzusehen, dies wird im Standard Event Logbuch erfasst.

Das Netzteil der Schnittstelle muss kurzschlussfest sein und sämtliche Manipulationen an der Kundenschnittstelle dürfen die Funktionen des restlichen Smart Meters 2.0 nicht beeinflussen.

Falls die Kundenschnittstelle als Modulschacht ausgeführt ist, muss die Steckverbindung zum Zähler berührungssicher ausgeführt werden.

An die Kundenschnittstelle ist grundsätzlich nur ein Endgerät anzuschließen, wodurch eine Adressierung entfällt.

C.6.2 Sicherheitsmechanismen

Die Security hat die Vorgaben von E2E Security Informationen zu erfüllen.

Die Schnittstelle muss mittels **DLMS/COSEM Security Suite 0** unter Verwendung von **AES-GCM-128** verschlüsselt sein.

C.6.3 Datenausgabe

Die Schnittstelle ist unidirektional auszuführen und darf somit keinerlei Manipulationsmöglichkeit des Smart Meters 2.0 bieten.

Im Push Betrieb gibt der Smart Meter 2.0 jede Sekunde die Daten über die Schnittstelle aus.

Abweichend von DSMR P1 Kapitel 6.12, ist der in „OE_CS_Hauptdokument.pdf“ Kapitel B.4 beschriebene Datensatz über die Schnittstelle auszugeben.

C.7 Steuerausgänge SA

C.7.1 Allgemeine Informationen SA

Die Steuerausgänge sind 2 potentialfreie, mechanische Schaltrelais, die über kein Kommunikationsprotokoll verfügen.

In dieser Beschreibung wird nicht näher auf deren Ausprägung eingegangen. Die Details sind im Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“ Kapitel C.3.9 und im Dokument „E.2_OE_CS_Lastenheft_SM_Messwandler.pdf“ Kapitel C.3.9 zu finden.

Austria Annex to AC Electricity Smart Meter GCP Ed. 1.0.1

TECHNICAL REPORT

Comprehensive Semantic Model

for Energy Management

AC Electricity Smart Meter

Generic Companion Profile

Austria Annex

April 2026

Oesterreichs Energie

© Copyright 2026 Oesterreichs Energie

CONTENTS

OESTERREICHS ENERGIE INTRODUCTION & PURPOSE 6
1.1. Object Model 6
1.2. Evolution 6
2. Scope 7
3. Reference Documents 7
4. Terms and abbreviations 7
5. Aspects of the GCP 7
5.1. Background 7
5.2. Client / Server model 8
5.3. Device Type identifiers 8
5.4. Communication services 8
5.5. Set of Application Associations 9
5.6. Power down behaviour 9
5.7. Network connectivity 9
5.7.1. SMS 9
5.7.2. ICMP and similar communications 9
5.8. Communications channels 9
5.8.1. General 9
5.8.2. P2P-Wireless 9
5.8.3. P2P -Wired (Ethernet) 10
5.8.4. PLC 10
5.8.5. M-Bus and variants 10
5.8.6. Local (optical) port (service interface) 10
5.8.7. PUSH operation 10
5.8.8. Customer Information Port 10
5.9. Security 10
5.10. Gateway types 13
5.11. Instantaneous values. 13
5.12. Null data in profiles 13
5.13. Submeters 13
6. Detail use case information 13
6.1. General introduction 13
6.1.1. KPI 15
6.2. Use Case ACESM-UC01 – Meter Registration 24
6.2.1. General information from ACE SM 24
6.2.2. Details of technical variations (if any) 24
6.2.3. Commentary 24
6.3. Use Case ACESM-UC02 – Remote Tariff Programming 25
6.3.1. General information from ACE SM 25
6.3.2. Adoption 25
6.3.3. Details of technical variations (if any) 25
6.3.4. Commentary 25
6.4. Use Case ACESM-UC03 – On Demand Register Reading 25
6.4.1. General information from ACE SM 25

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.4.2. Adoption 26
6.4.3. Details of technical variations (if any) 26
6.4.4. Commentary 26
6.5. Use Case ACESM-UC04 – On-demand meter load profile reading 26
6.5.1. General information from ACE SM 26
6.5.2. Adoption 26
6.5.3. Details of technical variations (if any) 26
6.5.4. Commentary 26
6.6. Use Case ACESM-UC05 – Periodic meter reading 27
6.6.1. General information from ACE SM 27
6.6.2. Adoption 27
6.6.3. Details of technical variations (if any) 27
6.6.4. Commentary 27
6.7. Use Case ACESM-UC06 – Remote or local Disconnection and Reconnection 28
6.7.1. General information from ACE SM 28
6.7.2. Adoption 29
6.7.3. Details of technical variations (if any) 29
6.7.4. Commentary 29
6.8. Use Case ACESM-UC07 – Synchronizing the Clock 29
6.8.1. General information from ACE SM 29
6.8.2. Adoption 29
6.8.3. Details of technical variations (if any) 30
6.8.4. Commentary 30
6.9. Use Case ACESM-UC08 – Quality of supply 30
6.9.1. General information from ACE SM 30
6.9.2. Adoption 30
6.9.3. Details of technical variations (if any) 30
6.9.4. Commentary 30
6.10. Use Case ACESM-UC09 – Load management by relay 31
6.10.1. General information from ACE SM 31
6.10.2. Adoption 31
6.10.3. Details of technical variations (if any) 31
6.10.4. Commentary 31
6.11. Use Case ACESM-UC10 – Firmware update 31
6.11.1. General information from ACE SM 31
6.11.2. Adoption 32
6.11.3. Details of technical variations (if any) 32
6.11.4. Commentary 32
6.12. Use Case ACESM-UC11 – Meter supervision 33
6.12.1. General information from ACE SM 33
6.12.2. Adoption 33
6.12.3. Details of technical variations (if any) 33
6.12.4. Commentary 33
6.13. Use Case ACESM-UC12 – Consumer Information 33
6.13.1. General information from ACE SM 33

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.13.2. Adoption 34
6.13.3. Details of technical variations (if any) 34
6.13.4. Commentary 34
6.14. Use Case ACESM-UC13 – Communication supervision 34
6.14.1. General information from ACE SM 34
6.14.2. Adoption 34
6.14.3. Details of technical variations (if any) 35
6.14.4. Commentary 35
6.15. Use Case ACESM-UC14 – Enabling and disabling functionalities 35
6.15.1. General information from ACE SM 35
6.15.2. Adoption 35
6.15.3. Details of technical variations (if any) 35
6.15.4. Commentary 35
6.16. Use Case ACESM-UC15 – Power control 35
6.16.1. General information from ACE SM 35
6.16.2. Adoption 36
6.16.3. Details of technical variations (if any) 36
6.16.4. Commentary 36
6.17. Use Case ACESM-UC16 – Event management and alarm reporting 36
6.17.1. General information from ACE SM 36
6.17.2. Adoption 37
6.17.3. Commentary 37
6.18. Use Case ACESM-UC17 – Meter availability Control 37
6.18.1. General information from ACE SM 37
6.18.2. Adoption 37
6.18.3. Details of technical variations (if any) 37
6.18.4. Commentary 37
6.19. Use Case ACESM-UC18 – Display messages on meter display 38
6.19.1. General information from ACE SM 38
6.19.2. Adoption 38
6.19.3. Details of technical variations (if any) 38
6.19.4. Commentary 38
6.20. Use Case ACESM-UC19 – Configuration of meter locally 39
6.20.1. General information from ACE SM 39
6.20.2. Adoption 39
6.20.3. Details of technical variations (if any) 39
6.20.4. Commentary 39
6.21. Use Case ACESM-UC20 – Manage meter security settings 39
6.21.1. General information from ACE SM 39
6.21.2. Adoption 40
6.21.3. Details of technical variations (if any) 40
6.21.4. Commentary 40
6.22. Use Case ACESM-UC21 – Prepayment metering 40
6.22.1. General information from ACE SM 40
6.22.2. Adoption 41

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.22.3. Details of technical variations (if any) 41
6.22.4. Commentary 41
6.23. Use Case Oe-01 – Communications Configuration. 41
6.23.1. Description of the use case 41
6.23.2. Further information to the use case for classification/mapping 43
6.23.3. Diagrams of use case 44
6.23.4. Technical details 45
6.23.5. Step by step analysis of use case 46
6.23.8. Information exchanged 71
6.23.9. Common terms and definitions 74
6.24. Use Case Oe-02 – Calibration and maintenance 76
6.24.1. Description of the use case 76
6.24.2. Diagrams of use case 78
6.24.3. Technical details 79
6.24.4. Step by step analysis of use case 80
6.24.5. Information exchanged 90
6.24.6. Requirements (optional) 91
6.24.7. Common terms and definitions 92
6.25. Use Case Oe-03 – Communications module management 93
6.25.1. Description of the use case 93
6.25.2. Diagrams of use case 95
6.25.3. Technical details 96
6.25.4. Step by step analysis of use case 97
6.25.5. Information exchanged 106
6.25.6. Common terms and definitions 107
7. Configuration of protection of the Service (optical) interface. 107

Table 1 - GCP security clauses and commentary 10
Table 2 - Use Case summary 13
Table 3 – KPI overview 15
Table 4 – UC01 Scenarios 24
Table 5 – Cryptographic Algorithms 40

© Copyright 2026 Oesterreichs Energie. All rights reserved

OESTERREICHS ENERGIE INTRODUCTION & PURPOSE

This document is to be read in conjunction with the DLMS User Association ACE SM GCP Version 1.0.1 which provides the core activity for meter communications. There are specific additional needs to support the needs of smart metering stakeholders in Austria, and this document's purpose is to detail these needs.

For clarity, this document details the differences from the ACE SM GCP specific to application in Austria, mainly in the use cases, but in other areas as well. This document also clarifies the mandatory, optional and conditional elements of the use cases and their scenarios and provides extensions for some use cases. This document also provides clarification on interpretation of the ACE SM GCP where there are items that are not clear.

This document is within a structure defined in the companion standard main document "OE_CS_Hauptdokument.pdf" as noted within the reference documents.

1.1. Object Model

The Object Model spreadsheet as available contains only the IPR of Oesterreichs Energie. It is anticipated that a complete version of the spreadsheet will be available shortly, but in the interim it should be straightforward to insert the object model content from DLMS UA to build the spreadsheet as a whole.

1.2. Evolution

It is to be noted that the ACE SM GCP as well as other related documents will be the subject of ongoing change. Later versions of related documents may cause review of this document. Co-publication of this document with DLMS UA and Oesterreichs Energie is agreed in principle and further work will be delivered in due course.

© Copyright 2026 Oesterreichs Energie. All rights reserved

2. Scope

This document provides the AC Electricity Smart Meter Generic Companion Profile (ACESM GCP) as an interoperability specification for electricity smart meters, based on DLMS/COSEM standards, with necessary adjustments for deployment in Austria. This profile therefore applies DLMS/COSEM as described in Blue Book 17 and Green Book 12 and applies and further develops the IDIS Package 3 interoperability specification. Furthermore, the purpose of this profile is for the compatibility certification, based on DLMS/COSEM standards.

3. Reference Documents

Referenced documents are listed in the AC Electricity Meter GCP, and the Austrian Smart Metering overview document, OE_CS_Hauptdokument.pdf.

4. Terms and abbreviations

General terms and definitions are included in OE_CS_Hauptdokument.pdf. and the ACE SM GCP.

Term	Definition	Comment
Command	An instruction to a meter	This will be a DLMS/COSEM command, and will in almost all cases, elicit a response[1].
Response	A message from a meter in reply to a command/instruction	
Push message ,	A message from a meter at the meter's behest to the Head End/Central System	This can be stimulated from the meter due to an Alarm, or a scheduled transmission or data, or stimulated by a Command. This may also be referred to as a Data-Notification.
Central System	The system operated by the DSO to operate and collect data from smart electricity meters	Note that the Head-end system is a component of the Central System, and this may be supported by security elements and data management systems depending on the DSO
Head-end system	The system directly referenced within the ACE SM GCP	
Dualmode-gateway	A gateway with additional functionality including collecting readings from the meter	More detailed description in document .4_OE_CS_Lastenheft_Dualmode-Gateway

Abbreviation	Description	
SUC	System Use Case	
GCP	Generic Companion Profile	
SEM	Smart Electricity Meter	

5. Aspects of the GCP

5.1. Background

The ACE SM GCP has been prepared by the DLMS User Association as a means to increase levels of interoperability between meter deployments, in turn delivering standardised functionality to ensure that high standards of operation can be achieved at reasonable meter and implementation costs. Version 1.0.1 of this GCP has received significant input from Oesterreichs Energie members to clarify the Use Cases.

[1] Meters may not send a response to a Command when the Command is to activate new firmware, for example.

© Copyright 2026 Oesterreichs Energie. All rights reserved

Because of the extensions needed in Austria, a dedicated version of the Object Model Spreadsheet has been developed. This dedicated version of the spreadsheet shall be used as the reference for Objects, Events, Alarms, and Role based access control.

5.2. Client / Server model

DLMS/COSEM uses a client server model, where the meter is a server. Clients include:

- The head end system,
- Hand-held equipment used by meter workers and meter installers,
- Dualmode-Gateway equipment.

Because these will have different rights and needs for data and control, a selection of Application Associations has been designated.

These are outlined in 5.5.

Note. The customer port on the meter is using the DSMR P1 interface specification, and configured using UC12.

The Object Model defines the DLMS Application Associations and derived COSEM clients in detail.

5.3. Device Type identifiers

The ACE SM GCP core design is for direct acting meters. Requirements in Austria include the need for CT meters, and, because these meters require some variation in the Object Model, a device type identifier is needed.

6.2.1 of the ACE SM GCP identifies T1 as 106 for single phase, and 107 as poly phase (direct) meter. To identify the poly phase CT meter, the meter vendor shall adopt a value of 090 for T1 and shall comply with the requirements of 6.2.1 for T2 and Serial Number and all other aspects of the System Title.

Example System Title:

An LGZ (4c, 47, 5a) ACESM Poly Phase CT meter (090) with no extension and with serial number 12345678 (bc,61,4e) results in the following system title (hex coded):

byte1	byte 2	byte 3	byte 4	byte 5	byte 6	byte 7	byte 8
4c	47	5a	5a	00	bc	61	4e

6.2.2 of the ACE SM GCP shall be used for the Logical Device Name of the meter substituting the value 090 for T1 where the meter is a polyphase CT meter.

Example Logical Device Name:

An Itron ACESM Poly Phase meter with extension Disconnector and Load management, and with serial number 12345678 results in the following Logical Device Name:

byte1	byte 2	byte 3	byte 4	byte 5	byte 6	byte 7	byte 8
61	63	65	1	0	7	0	3

byte9	byte 10	byte 11	byte 12	byte 13	byte 14	byte 15	byte 16
1	2	3	4	5	6	7	8

5.4. Communication services

The services described in 6.4 of the ACE SM GCP shall be supported. Note that Data-Notification is used for sending Alarms.

The service- specific ciphering described in 6.4.3 of the GCP is not supported.

© Copyright 2026 Oesterreichs Energie. All rights reserved

The General-Signing and General-Ciphering services shall be supported.

5.5. Set of Application Associations

Meters to be used in Austria shall support the Application Associations as defined in the Object model, Roles tab.

Details of the objects supported and the security setup are included in the Oe - Object Model ("D.1_OE_CS_Objektmodel.xlsx").

The AA-establishment process for Application Associations other than [16] [102],and [103] shall use HLS authentication mechanism id = 5 or 7. Note that use of mechanism 7 for local connections may present security risks that should be analysed.

Meter manufacturers shall not include any additional Application Association without disclosing its purpose and credentials to the meter purchaser.

5.6. Power down behaviour

With respect to the power down behaviour, the SEM shall behave according to ACE SM GCP 6.5.1 and 6.5.3 applied to any open AA that is not pre-established. Note that the ACE SM GCP refers only to the management AA.

AAs that are established before the power down, other than the security officer AA, may re-establish if there is no change to the IP address at power up,

5.7. Network connectivity

Where the meter uses P2P communications, then auto connect mode 101 shall be applied. Note that mode 101 is defined in 6.6 of the ACE SM GCP as "The ACESM is permanently connected to the IP network and can be reached by the HES or DC via its known IP address".

The meter need not support the wake-up process described in ACE SM GCP 6.7.

5.7.1. SMS

The ACE SM GCP references that SMS may be used to deliver "wake up" messages and also be used for specific Push Alarm messages. This function shall be disabled in Austria.

5.7.2. ICMP and similar communications

ICMP and similar communications shall be securely disabled if not needed by upper layers, other than for bootstrapping and for IP assignment, those functions needed for G3 network management and the meter shall respond to and generate a Ping request.

List of use cases:

- G3-Certification Tests (FER Testcases use ICMP PING)
- G3-PLC IPv6 Address
- G3-PLC functionality (Router advertisments, Router solicitation)
- G3-PLC and mobile radio troubleshooting (PING from HES / Network devices to and from meter)
    - Path MTU discovery
    - Routing and Firewall Troubleshooting

5.8. Communications channels

5.8.1. General

DSOs in Austria use field-changeable communications modules. In the situation where the module is an independent device and has its own identity on the network then it shall support the objects necessary for its management and monitoring, and have equivalent WAN communications functionality as an integrated meter.

5.8.2. P2P-Wireless

The ACE SM GCP supports 3GPP communications, and this will be applied in full for LTE in accordance with 6.8.6.2 of the ACE SM GCP, with constraints as defined in "D.3_OE_CS_Implementation_Guide_Mobilunk.pdf".

© Copyright 2026 Oesterreichs Energie. All rights reserved

5.8.3. P2P -Wired (Ethernet)

The ACE SM GCP supports Ethernet connections, and this will be applied in full for Ethernet in accordance with 6.8.6.3 of the ACE SM GCP where meters use Ethernet for a wide area connection. Constraints are defined in "D.4_OE_CS_Implementation_Guide_Ethernet.pdf".

5.8.4. PLC

The ACE SM GCP supports G3-PLC and G3-Hybrid communications. OE will apply these communications capabilities, with constraints as defined in "D.2_OE_CS_Implementation_Guide_G3-PLC_und_G3-Hybrid.pdf".

5.8.5. M-Bus and variants

Although the ACE SM GCP supports local communications based on M-Bus and/or Wireless M-Bus, this is not used in Austria.

5.8.6. Local (optical) port (service interface)

Local port is required, and is configured using the objects within the ACE SM GCP with the default settings on the Object Model.

Requirement for minimum 19200 baud, but manufacturers should support up to 115200 baud.

5.8.7. PUSH operation

The meters shall support Push operations, using the principal data connection for the meter (P2P or G3-PLC). This will be applied for routine sending of data and for sending alarms.

5.8.8. Customer Information Port

The Customer Information Port is detailed in the document „B.3_OE_CS_Anhang_Schnittstellen_Details.pdf"

The data shall be encrypted but not authenticated.

The frame counter for the Customer information interface shall operate exactly as a normal frame counter – that is it will increment with every package. It will be sent in plain text to the customer to allow the initialisation vector to be calculated.

Note that the frame counter will not overflow for over 100 years at one second intervals.

Note that a specific object exists within the object model to allow other Clients to readout the frame counter.

5.9. Security

In general, the security features shall align with Clause 7 of the ACE SM GCP, noting document „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf" from Oesterreichs Energie for Smart Meter 2.0 security, noting the comments in the table below.

Table 1 - GCP security clauses and commentary

GCP Clause	*Requirement*	*Comment*
7.1 (General)	Suite 2 or stronger security suite (when available) shall be delivered.	Note that there will be a need to follow the state of the art into the future, including new suites as they become available. Note that there is a specific Object to control the application of V.44 from the meter.
7.1.1 (Wake up)	Meters shall not support the wake-up functions in any form.	There should be no circumstances or transport that will execute a wake up command from the HES to the meter, as meters are required to maintain a connection.
7.2 (SMS)	Reception on the meter and/or communications module of SMS	SMS transmission and reception on the meter shall be disabled.

© Copyright 2026 Oesterreichs Energie. All rights reserved

GCP Clause	Requirement	Comment
	(including embedded modems) shall be disabled	
7.3 (Push/Pull)	<Applies, noting that service General Glo Ciphering & General Ded Ciphering are not used >	
7.3.1 Invocation counters Use	Store of invocation counter shall be in non-volatile storage, Counters shall only increment after the message is authenticated. The push of the CII shall include the frame counter value within the message header	This is to ensure that the customer can retrieve the data on the customer port.
7.4 (Security Setup Objects)	Other than the Public Application Association and the CII, the security policy shall be configured to use authenticated encryption in client to server and server to client messages for local and WAN communications and encrypted only for Customer Port communications. Each Application Association will have its own AK and GUEK. Associations with multicast/broadcast capabilities shall have their own GBEK.	Note that the KEK for the security officer acts as the master key for all roles – to be confirmed.
7.4.1	Observing that there are additional security setups, all Security Setup Objects shall be configured as described as appropriate for their port(s). The SEM shall support the AAs that are designated in the Object Model and shall restrict their operations as described in the object model	
7.4.2	Use of ephemeral ("Dedicated") keys is not supported. All roles shall populate the store for the master (KEK) key. However, only roles that are permitted to perform key updates are those that are so designated in 6.21.3.	DLMS uses the term "dedicated" to describe ephemeral keys – that is keys that are established as part of the AA establishment process and which are destroyed when the AA is released or aborted. Clearly, therefore, a pre- established AA cannot use dedicated keys.
7.4.3	Receive invocation counters for all Application Associations will be accessible via the Public client.	
7.4.4	AA establishment will be conducted using HLS5 or HLS7 for remote AAs and local AAs, except for the Public AA as noted in 5.5. Note that each AA has its own counters allied to the relevant keys, as described in the Object Model.	
7.4.5 (Putting meter into the field)	The requirements in section 7.4.5 are not in place.	Meters will need to be delivered with security credentials and security suites in

© Copyright 2026 Oesterreichs Energie. All rights reserved

GCP Clause	Requirement	Comment
	Meters shall be delivered with a complete set of unique security credentials in place (including key locations that will not be applied by the DSO). The manufacturer and the customer shall agree a secure method of transfer of necessary keys such that the customer can proceed with installation without delay.	place and active. The buyer of the meters is expected to receive the credentials in a secure manner from the meter manufacturer, and use these credentials to commission the meter in the field. It will then be a matter of buyer's policy to replace the credentials in due course. Note that the EU Cyber Resilience Act (and the standards under development to support this act) may impact the security requirements.
7.4.7 (changing the security policy)	The Security officer role shall be capable of changing the security policy. Other roles (including the Management Role) shall not be capable of changing the security policy	

Other security requirements are:

1. Meters that contain radios for M-Bus shall have this functionality disabled.
2. The Security Officer Role shall be the only role capable of changing the Security Suite.
3. The security setup objects (IC = 64) listed in the Object Model have optional methods according to the Blue Book Part 2. the following methods:
    a. Security_activate,
    b. Key_transfer,
    c. Key_agreement,
    d. Generate_key_pair,
    e. Generate_certificate_request,
    f. Import_certificate,
    g. Export_certificate, and
    h. Remove_certificate are mandatory.
4. With respect to ACE SM GCP 6.10.1.3 Security on the Consumer Information Interface The keys (CIP keys) used for the data pushed to the CII are managed in the AMI infrastructure. The SEM shall use the keys as provided according to UC20. Keys will be distributed by the DSO.
5. Management of Root Certificates. It is anticipated that a DSO may (or may not) operate its own design of PKI, and either manage its own Root Cert or contract to an external provider. It is anticipated that the DSO's nominated Root Cert will be inserted into the meter at manufacture, and this certificate will be used as a basis to authenticate all communications.
6. The public key for firmware update shall be contained within the firmware itself.
7. Update of the Root Certificate is carried out by updating the Client Certificate in a dedicated Security Setup Object and hence only possible to the security officer role, or by firmware update.
8. Certificates shall be validated against the root certificate when they are imported into the security setup object.

Note also the requirements added within 6.21.3 of this document.

Use of test keys. Production meters, that is, meters to be used in supply points, will have a process for key initialisation and sharing agreed between the vendor and the customer. Meters for test use may use different key

© Copyright 2026 Oesterreichs Energie. All rights reserved

arrangements, including the use of the test keys specified within the ACE SM GCP section 7.4.4. Note that these test keys shall not be used for production meters under any circumstances.

This again to be agreed between the vendor and the purchaser of meters.

5.10. Gateway types

Gateways are applied on PLC communications. The gateways vary in capability, and their specification is outside the scope of this document.

Simple gateways are devices that pass through and/or store and forward messages in both directions, providing simple communications capabilities.

Dualmode-Gateways are advanced devices that have the capability to generate and send commands to meters and receive both responses and push messages from meters. For clarity, many of the use cases that refer to a HES can also be delivered by a Dualmode-gateway, taking note of the Table 2 below. Gateways are also controlled by head-end systems, but the data exchange between a gateway is out of scope of both the GCP and this document.

5.11. Instantaneous values.

By their nature, instantaneous values of AC parameters need to be integrated over a short period. For the purposes of this annex, “instantaneous” measured values shall be integrated over one second. For clarity, this one second need not be synchronised with actual time seconds. For clarity, Objects with OBIS codes “1-{0..255}:{0..128}.**7**.{0..255}.255” are considered instantaneous measured values.

5.12. Null data in profiles

An additional object, described in the Object Model, is applied to enable and disable the use of null-data and this is configurable from the HES. Note that if null data is applied, then it applies to all interval profiles and event logs See ACE SM GCP 1.0.1 9.12.6.1.2 for worked example.

5.13. Submeters

Submeters are not supported by meters meeting this companion specification, and any reference to submeters in the use cases should be regarded as superfluous information.

6. Detail use case information

6.1. General introduction

The table below provides an overview of the Use Cases referenced in this document. The roles that are permitted to operate Use Cases and their scenarios are detailed in the Object Model spreadsheet.

Table 2 - Use Case summary

ID	Use Case	Description	Function of Dualmode-Gateway[2]	Commentary
ACE SM GCP Use Cases				
UC1	Meter Registration	Process of incorporating devices (ACESMs, submeters, …) into the system.	Pass-through	
UC2	Remote Tariff Programming	Process of remotely programming the parameters necessary to support a time of use (TOU) based tariff contract.	Pass-through	
UC3	On Demand Meter Register reading for multi-utility meters	Process of collecting meter register readings upon a specific request.	Pass-through and direct execution	
UC4	On Demand Meter Load Profile reading for multi-utility meters	Process of collecting load profile register readings upon a specific request.	Pass-through and direct execution	

[2] Dualmode-Gateway functionality is defined in „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ .

© Copyright 2026 Oesterreichs Energie. All rights reserved

ID	Use Case	Description	Function of Dualmode-Gateway[2]	Commentary
UC5	Periodic Meter reading for multi-utility meters	Process of periodically collecting meter readings for billing purposes (periodic reading)	Configuration is pass-through, but the Hub/gateway may be the recipient of the data.	
UC6	Remote or local Disconnection and Reconnection (E, G)	Process of disconnecting or reconnecting the electricity I or gas (G) supply of a customer.	Pass through	
UC7	Clock Synchronization	Process of adjusting the internal clock of the metering equipment	The Dualmode-gateway may fulfil the role of HES and/or NTP server.	
UC8	Quality of Supply	Process of supervising Power Outages, Sags and Swells,	Pass-through, or the Dualmode-gateway may be the recipient.	
UC9	Load Management by relay (E only)	Process of controlling specific local loads by means of relays.	Pass-through	
UC10	Firmware update	Process of downloading new firmware to a device	Pass through, or possibly may deliver the firmware image to meters	
		Process of activation	Pass through	
UC11	Meter supervision	Process of supervising any events which could comprise the meter and the system.	Pass-through, and may be the recipient of the data.	
UC12	Consumer Information	Process of periodically transmitting meter reads and consumer information via a local digital interface	Pass-through	
UC13	Communication Supervision	Process of supervising events affecting the meter to HES communication.	Pass-through or the Dualmode-gateway may be the recipient.	
UC14	Enabling / disabling functionalities	Process of enabling or disabling a functionality.	Pass-through	
UC15	Power Control	Process of activating or deactivating the demanded power control mode in meters	Pass-through	
UC16	Alarm and event Management	Process of management of events and equipment alarms	Pass-through, and may be the recipient of the data.	
UC17	Meter Availability Control	Process to ping a meter to check that communication works	Pass-through and direct execution	
UC18	Display messages on meter display	Process of displaying pre-defined or on-the-fly messages such as supply of energy or tariffs	Pass-through	
UC19	Configuration of meter locally	Process of initial installation or in-service control	Not applicable	
UC20	Manage security settings	Process of setting and updating security credentials can be done remotely and cover setting new security keys or certificates in the meter	Pass-through	
UC21	Prepayment	Process for prepayment functions of the electricity meter	Not Applicable	The approach for prepayment in Austria does not require this Use Case.
Use Cases developed specifically for OE				
Oe01	Communications Configuration	Configuration of communications parameters needed for PLC and P2P technologies.	Pass-through	

© Copyright 2026 Oesterreichs Energie. All rights reserved

ID	Use Case	Description	Function of Dualmode-Gateway[2]	Commentary
Oe02	Test and Calibration	Change of meter operational mode to permit testing and return to service.	Not Applicable	
Oe03	Exchange of communications module	Replacement of a communications module to adopt a new communications technology	Pass-through	Note that this only contains general principles and it is expected that a high degree of reliance will be placed on the meter manufacturer or vendor to make this successful

The sections below give more detail about each Use Case, it's applicability and any variances required for Austria. Please note "General information from ACE SM" subclauses are normally direct quotations from the Use Case, and therefore may describe features that are not applied to this Annex.

6.1.1. KPI

For clarity, the requirements in this section over-ride any KPI within the ACE SM GCP Use Cases.

Remarks:

- The KPIs are defined for each use case individually, however they must be fulfilled while all the use cases are running concurrently in the smart meter system.
- The individual components of the smart meter system (e.g. Smart Meter, Dualmode-Gateway, HES, MDM, MNO for P2P, Backhaul for PLC) have to provide sufficient performance that the KPIs below can be fulfilled. To support this, all participants (meter vendor, HES vendor, comms provider and the DSO) are expected to agree a duty to co-operate to achieve these KPIs.
- KPIs become effective at the start of "business as usual" operations, as defined by the DSO. KPIs may be suspended by the DSO in circumstances where communications are inoperable or extreme events (including severe weather events) are being managed.
- It is a prerequisite that the meter is configured correctly and measures, collects and stores the required measurement values, data and events and performs actions immediately.
- It is expected that KPIs will be evaluated monthly but will be the subject of DSO's contracts.
- Explanation
    - Remote single: Ad-hoc communication to a single meter
    - Remote bulk: Up to the maximum number of meters attached to a Dualmode-Gateway or a radio base station. The HES has to provide the capabilities to achieve the KPI for all the meters of the DSO.
    - Local: Local communication using the service interface (optical port) via HHU

Table 3 – KPI overview

Use Case		Local/remote	KPI	Comment
UC1	Meter Registration	Remote, single	99 % of the meters are registered in the HES and	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
			ready for operational communication in <= 60 min of power up in a live installation.	
		Remote, bulk	99 % of the meters are registered in the HES and ready for operational communication in <= 6 hrs of power up in a live installation.	e.g. power outage, change of Dualmode-Gateway
UC2	Remote *(& local)* Tariff Programming	Remote, single	99 % of the meters are programmed successfully in <= 3 min after sending the command from the HES.	Successfully means HES received confirmation from the meter
		Remote, bulk	99 % of the meters are programmed successfully in <= 3 hrs min after sending the command from the HES.	Successfully means HES received confirmation from the meter
		Local	Meter is programmed successfully in <= 5 s after sending the command from the HHU.	Successfully means HHU received confirmation from the meter
UC3	On Demand Meter Register reading for multi-utility meters	Remote, single	For 99% of the meters the read out data (i.e. 6 registers) is available in the HES in <= 2 min after sending the read out command from the HES to the meter.	
		Remote, bulk	For 99% of the meters the read out data (i.e. 6 registers) is available in the HES in <= 3 hrs min after sending the read out command from the HES to the meter.	
		Local	Read out data (i.e. 6 registers) is available in the HHU in <= 20 s after sending the read out command from the HHU.	
UC4	On Demand Meter Load Profile reading for multi-utility meters	Remote, single	For 99% of the meters the read out data (i.e. 6 channels with 96 values each) is available in the HES in <= 3 min after sending the read out	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
			command from the HES to the meter.	
		Remote, bulk	For 99% of the meters the read out data (i.e. 6 channels with 96 values each) is available in the HES within in <= 4 hrs after sending the read out command from the HES to the meter.	
		Local	The read out data (i.e. 6 channels with 5760 values each) is available in the HHU within in <= 10 min after sending the read out command from the HHU.	
UC5	Periodic Meter reading for multi-utility meters	Remote, bulk	The read out data (i.e. 6 channels with 96 values each) of 99 % of all the DSO meters is available in the HES within in <= 3 hrs after sending the read out command from the HES or Dualmode-Gateway to the meters or the meters pushing the data to the HES.	Minimum legal requirement (IMA-V 2026, §3, Abs. 7): Readout of the daily data and providing it in the DSO web portal until 12:00h on the following day
UC6	Remote or local Disconnection and Reconnection (E, G)	Remote, single	99% of the meters are disconnected or reconnected successfully within in <= 3 min after sending the command from the HES.	
		Local	The meter is disconnected or reconnected successfully within in <= 5 s after sending the command from the HHU.	
UC7	Clock Synchronization	Remote, single	99 % of the meters are synchronized successfully within in <= 3 min after sending the command from the HES.	Minimum legal requirement (IMA-V 2026, §3, Abs. 16): Meters have to be synchronized once a day
		Remote, bulk	99 % of the meters are synchronized successfully in <= 3 hrs after sending the command from the HES.	
		Local	The meter is synchronized successfully in <= 5 s after	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
			sending the command from the HHU.	
UC8	Quality of Supply	Remote, single	For 99% of the meters the read out power quality data (i.e. power quality profiles 15 channels with 144 values and event logs) is available in the HES in <= 5 min after sending the read out command from the HES to the meters.	Minimum legal requirement (IMA-V 2026, §3, Abs. 8): Readout of the whole power quality data in a weekly manner.
		Remote, bulk	For 99% of the meters the read out power quality data (i.e. power quality profiles 15 channels with 144 values and event logs) is available in the HES in <= 4 hrs after sending the read out command from the HES to the meters.	
		Local	Read out power quality data (i.e. power quality profiles 15 channels with 1440 values and event logs) is available in the HHU in <= 5 min after sending the read out command from the HHU.	
UC9	Load Management by relay (E only)	Remote, single	For 99% of the meters the relays are disconnected or reconnected successfully in <= 3 min after sending the command from the HES.	
		Remote, bulk	For 90% of the meters the relays are disconnected or reconnected successfully in <= 15 min after sending the command from the HES.	
		Local	The relays are disconnected or reconnected successfully in <= 5 s after sending the command from the HHU.	
UC10	Firmware update	Remote, single	For 99% of the meters the firmware update carried out by the HES or Dualmode-gateway is successfully performed in <= 10 min.	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
		Remote, bulk	For 90% of the meters the firmware update carried out by the HES or Dualmode-gateway is successfully performed in <= 5 days.	
		Local	The firmware update (whole image) from the HHU to the meter is successfully performed in <= 10 min.	Delta updates of firmware should be faster.
UC11	Meter supervision	Remote, single	Event logs: For 99% of the meters the read out event logs are available in the HES in <= 3 min after sending the read out command from the HES to the meter. Alarms: The alarms are pushed immediately and available in <= 1 min in the HES.	
		Remote, bulk	Event logs: For 99% of the meters the read out event logs are available in the HES in <= 4 hrs after sending the read out command from the HES to the meter. Alarms: The alarms are pushed immediately and available in <= 15 min in the HES.	
		Local	Event logs: The read out of the event log to the HHU is successfully performed in <= 1 min.	
UC12	Consumer Information	Remote, single	Configuration: 99 % of the meters are configured successfully in <= 3 min after sending the command from the HES.	
		Remote, bulk	Configuration: 99 % of the meters are configured successfully in <= 3 hrs after sending the command from the HES.	
		Local	Configuration: Meter is configured successfully in <= 5 s after sending the command from the HHU.	Minimum legal requirement (IMA-V 2026, §3, Abs. 9): Information to the customer

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
			Deliver Consumer Information: If activated the meter successfully delivers information to the customer equipment every second.	equipment every second.
UC13	Communication Supervision	Remote, single	Event logs: For 99% of the meters the read out event logs are available in the HES in <= 3 min after sending the read out command from the HES to the meter. Alarms: The alarms are pushed immediately and available in <= 1 min in the HES.	
		Remote, bulk	Event logs: For 99% of the meters the read out event logs are available in the HES in <= 4 hrs after sending the read out command from the HES to the meter. Alarms: The alarms are pushed immediately and available in <=15 min in the HES.	
		Local	Event logs: The read out of the event log to the HHU is successfully performed in <= 1 min.	
UC14	Enabling / disabling functionalities	Remote, single	99 % of the meters are configured successfully in <= 3 min after sending the command from the HES.	
		Remote, bulk	99 % of the meters are configured successfully in <= 3 hrs after sending the command from the HES.	
		Local	Meter is configured successfully in <= 5 s after sending the command from the HHU.	
UC15	Power Control	Remote, single	Configuration: 99 % of the meters are configured successfully in <= 3 min after sending the command from the HES.	
		Remote, bulk	Configuration: 99 % of the meters are configured successfully in <= 3 hrs after sending the command from the HES.	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
		Local	Configuration: Meter is configured successfully <= 5 s after sending the command from the HHU. Action: If the according criteria is fulfilled, the meter performs the action immediately.	
UC16	Alarm and event Management	Remote, single	Event logs: For 99% of the meters the read out event logs are available in the HES in <= 3 min after sending the read out command from the HES to the meter. Alarms: The alarms are pushed immediately and available in <= 1 min in the HES.	
		Remote, bulk	Event logs: For 99% of the meters the read out event logs are available in the HES in <= 4 hrs after sending the read out command from the HES to the meter. Alarms: The alarms are pushed immediately and available in <=15 min in the HES.	
		Local	Event logs: The read out of the event log to the HHU is successfully performed in <= 1 min.	
UC17	Meter Availability Control	Remote, single	The meter responds to a request from the HES in <= 1 min.	
UC18	Display messages on meter display	Remote, single	Configuration: 99 % of the meters are configured successfully in <= 3 min after sending the command from the HES.	
		Remote, bulk	Configuration: 99 % of the meters are configured successfully in <= 3 hrs after sending the command from the HES.	
		Local	Configuration: The meter is configured successfully in <= 5 s after sending the command from the HHU.	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
			Display Information: The message or data is displayed on the meter display correctly.	
UC19	Configuration of meter locally	Local	Configuration: Meter is configured successfully in <= 5 s after sending the command from the HHU.	Local usecases are listed for each usecase separately
UC20	Manage security settings	Remote, single	Configuration or Key Update via Key transfer or HES/SubCA Certificate Update: 99 % of the meters are configured successfully in <= 3 min after sending the command from the HES. Key Update via Key agreement or Meter Certificate Update: 99 % of the meters are configured successfully in <= 12 min after sending the command from the HES.	
		Remote, bulk	Configuration or Key Update via Key transfer or HES/SubCA Certificate Update: 99 % of the meters are configured successfully in <= 3 hrs after sending the command from the HES. Key Update via Key agreement or Meter Certificate Update: 99 % of the meters are configured successfully in <= 12 hrs after sending the command from the HES.	
		Local	Configuration or Key Update via Key transfer or HES/SubCA Certificate Update: Meter is configured successfully in <= 5 s after sending the command from the HHU. Key Update via Key agreement or Meter Certificate Update: Meter is configured successfully in <= 5 min after initiating the process from the HHU.	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
UC21	Prepayment	-	-	The approach for prepayment in Austria does not require this Use Case.
UcOe-01	Communications configuration	Remote, single	Configuration: 99 % of the meters are configured successfully in <= 3 min after sending the command from the HES. Configuration is activated immediately after time based activation, if used.	
		Remote, bulk	Configuration: 99 % of the meters are configured successfully in <= 3 hrs after sending the command from the HES. Configuration is activated immediately after time based activation, if used.	
		Local	Configuration: Meter is configured successfully in <= 5 s after sending the command from the HHU. Configuration is activated immediately after time based activation, if used. After activation of the new communication configuration, the meter returns to previous configuration immediately after timeout.	
UC Oe-02	Calibration & maintenance	Local	Configuration: Meter is configured successfully in <= 5 s after sending the command from the HHU.	
UC Oe-03	Communications Module exchange	Remote	Preconditioning: If FW-update see UC10. If only configuration: The meter is configured successfully in <= 3 min after sending the command from the HES.	
		Local	Preconditioning: If FW-update see UC10. If configuration: Meter is configured successfully in <= 5 s after sending the command from the HHU.	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Use Case		Local/remote	KPI	Comment
			After module exchange meter performs immediate action and registration, see UC1.	

6.2. Use Case ACESM-UC01 – Meter Registration

6.2.1. General information from ACE SM

6.2.1.1. Scope

This Use Case covers the events from the meter being provisioned with initial information and being powered up in location, to the meter having established initial communications with the Head end System

6.2.1.2. Objective(s)

Meter fully operational: The meter has all the security credentials and configuration required for operation.

6.2.1.3. Short Description

Process of incorporating the Smart Meters and optionally Submeters into the system. Smart Meters are AC Electricity Smart Meters (ACESM) and Submeters are Gas, Heat or Water Submeters.

6.2.1.4. Scenarios

UC01-S1 Smart Meter Registration with Push on Installation
Description: This scenario describes the main activities to provide Smart Meter Identification Information and Connectivity information to Head End System with Pushing from Smart Meter on Installation.

UC01-S2 HES initiated registration
Description: This scenario describes the main activities to provide Smart Meter Identification Information and Connectivity information to Head End System with HES reading it from Smart Meter.

UC01-S3 Submeter registration
Adoption

Meters must support both scenarios S1 and S2. Scenario S3 is not permitted.

Table 4 – UC01 Scenarios

Scenario	Title	Status	Note
UC01-S1	Smart Meter Registration with Push on Installation	This scenario shall be included.	
UC01-S2	HES initiated registration	This scenario shall be included.	
UC01-S3	Submeter registration	This scenario shall not be included.	

6.2.2. Details of technical variations (if any)

Austrian utilities may require that push on connectivity object is applied rather than or as well as push on installation.

6.2.3. Commentary

The Use Case requires that meters have a certain amount of information in advance, for example some security credentials and the IP address of the HES and/or Gateway that they are to communicate with. It is expected that some of these items will be nationally specified in the Object Model (for example Security Suites, Application

© Copyright 2026 Oesterreichs Energie. All rights reserved

Association Objects) and some will be set by the DSO (for example, head end system identifiers, Certificates, and similar). The manufacturer should be consulted with as to how much of this information can be predetermined into the meter at manufacture, and how data can be included into the meter at the point of installation.

6.3. Use Case ACESM-UC02 – Remote Tariff Programming

6.3.1. General information from ACE SM

6.3.1.1. Scope

This use case delivers billing period recording and time of use for consumption and maximum demand operation.The scope is determined by SM WG Use Cases for Generic Smart Metering Profile

6.3.1.2. Objective(s)

Correct billing of energy and demand: The Electricity Meter correctly delivers time of use and records and resets maximum demand as per market requirements.

6.3.1.3. Short Description

Process of remotely programming a time of use (TOU) based tariff contract and/or setting end of billing period information for maximum demand operations.

6.3.1.4. Scenarios

UC02-S1 Send Tariff information

Description: This scenario describes the main activities to send tariff information from the Head End System to the Smart Meter

6.3.2. Adoption

The scenario is mandatory.

6.3.3. Details of technical variations (if any)

None

6.3.4. Commentary

The key feature of this use case to be applied is the “End of billing period” (EoBP) configuration. EoBP is essential to correct reading and resetting of maximum demand applications. Time of use tariffs are not required, and their objects are optional.

6.4. Use Case ACESM-UC03 – On Demand Register Reading

6.4.1. General information from ACE SM

6.4.1.1. Scope

This UC covers the reading of any register on the meter, predominantly registers for billing purposes.

6.4.1.2. Objective(s)

On demand reading of meter and submeter registers.: Meter register values are obtained in a timely manner. Optionally, submeter register values are obtained in a timely manner.

6.4.1.3. Short Description

Process of collecting meter readings upon a specific request

6.4.1.4. Scenarios

UC03-S1 On Demand reading through PULL Commands

Description: Reading on Demand may be performed by the GET or the ACCESS service from the HES or from the Hub/Gateway.

© Copyright 2026 Oesterreichs Energie. All rights reserved

UC03-S2 On Demand reading through PUSH Commands
Description: PUSH operation offers the HES or Hub/Gateway the possibility to (re)trigger a Data-Notification service to retrieve missing data from the last reading period(s).

6.4.2. Adoption

Both scenarios are mandatory. Note that Scenario 2 invokes UC05 scenario 3.

6.4.3. Details of technical variations (if any)

Scenario 1 can be executed by a Dualmode-gateway as well as a Head-end system.

Details on scenario 2 are covered in UC05 S03 details.

6.4.4. Commentary

It is likely that this use case will be primarily used to make fast reads – for example in the event of a consumer's query, or where a repeat of data is required for some reason.

Note. The value of the data from the meter will be in the range 0..4,294,967,295, and this will be representative of whole Wh for direct meters, and 1/10 Wh for CT meters. Meter displays will roll over at values of 9 999 999 kWh, or other decade values. It is necessary for the individual DSO to determine how the meter will behave at the condition of roll over, and how the data provided to billing systems will inform that a roll-over has occurred.

6.5. Use Case ACESM-UC04 – On-demand meter load profile reading

6.5.1. General information from ACE SM

6.5.1.1. Scope

This use case collects load profile information for billing and other uses from meters and submeters.

6.5.1.2. Objective(s)

Collection of load profiles for business purposes

6.5.1.3. Short Description

Collection by direct request of load profile profile_generic objects, that have been configured to deliver interval data, possibly daily and in-day intervals.

6.5.1.4. Scenarios

UC04-S1 Smart Meter Load Profile Reading
Description: Retrieval using Push of the meter's load profile(s)

UC04-S2 Submeter Load Profile Reading

6.5.2. Adoption

Scenario S1 is mandatory.

Scenario S2 is not required.

6.5.3. Details of technical variations (if any)

Where indicated in the Object Model, data items are to be accessible from this Use Case.

Selective access by range is mandatory and by entry and row is mandatory.

6.5.4. Commentary

This UC is used to read out interval profiles on an ad-hoc basis.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.6. Use Case ACESM-UC05 – Periodic meter reading

6.6.1. General information from ACE SM

6.6.1.1. Scope

This UC is intended to facilitate the routine collection of data from the meter, including billing and other data, by means of meter initiated Push, client initiated Push, and client initiated Pull. The scope is determined by METER WG Use Cases for Generic Smart Metering Profile.

6.6.1.2. Objective(s)

Set up push data: Configure the objects necessary to schedule periodic reads from the meter to be sent to the HES. Namely this will be the Push Set up, Schedule, Activity Calendar and Script Table objects. Set up system-originated requests: Where a meter relies on connection establishment from a HES or Gateway, the data to be routinely sent is pre configured for efficient transmission. Reliable data delivery: Accurate data is sent from the meter as configured.

6.6.1.3. Short Description

System Use Case (SUC) used to periodically read Smart Meter data for billing and other purposes, either using Push or Pull techniques, both directly and also applying a Gateway.

6.6.1.4. Scenarios

UC05-S0 (New) Configuration of routine data
Description: The HES sets the parameters on the Meter in order to execute routine readings

UC05-S1 Periodic Meter Reads - Meter originated push to HES
Description: This scenario describes the main activities to obtain meter readings from the Smart Meter by use of push on a routine basis controlled by the meter.

UC05-S2 Periodic Meter Reads - System or Gateway originated Pull

Description: This scenario describes the main activities to obtain meter readings from the Smart Meter using a Head End System or hub/gateway originated request.

UC05-S3 Periodic Meter Reads - System or Gateway-Initiated Push
Description: This scenario describes the main activities to obtain meter readings from the Smart Meter by use of a HES or Gateway-initiated PUSH.

UC05-S4 (New) Periodic Meter Reads - Meter originated push to Gateway
Description: This scenario describes the main activities to obtain meter readings from the Smart Meter by use of push, where the system that generated and delivered the configuration of the Push Setup and associated Objects is not the recipient, but a Gateway is applied.

6.6.2. Adoption

This use case is mandatory

6.6.3. Details of technical variations (if any)

use of null data. An additional object is applied to enable and disable the use of null-data and this is configurable using S0. Note that if null data is applied, then it applies to all interval profile logs and event logs.

4 ToU MD registers are required.

6.6.4. Commentary

This use case is applied most commonly to deliver billing register reads and interval data.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.7. Use Case ACESM-UC06 – Remote or local Disconnection and Reconnection

6.7.1. General information from ACE SM

6.7.1.1. Scope

The Use case configures and operates disconnectors in the electricity meter and optionally in submeters. The Use case describes the operations undertaken by a Head end System and these operations may be undertaken by a handheld unit via a local interface on the meter, if suitable security credentials are available. The scope is determined by SM WG Use Cases for Generic metering profile

6.7.1.2. Objective(s)

The objective is to disconnect and reconnect supply via a meter or optionally a sub-meter locally or remotely.

6.7.1.3. Short Description

Process of locally or remotely disconnecting or reconnecting supply at a meter or optionally an MBUS sub-meter.

6.7.1.4. Scenarios

UC06-S00 Configuration of Disconnector
Description: This controls the setting of the control mode of the disconnector.

This also controls the other settings related to disconnector objects, including the activity calendar, the schedule, and the arbitrator[3].
Control mode configures the behaviour of the disconnect control object for all triggers, i.e. the possible state **transitions.**

UC06-S01 Remote connection/disconnection of electricity breaker without arbitration
Description: The HES invokes scripts to control the remote_connect()/remote_disconnect() methods of Disconnect control object
A result is sent back to the HES - but this does not indicate a change of state, just that the command is accepted.

UC06-S02 Remote connection/disconnection of electricity breaker with Arbitrator IC
Description: Unlike non- arbitrator implementations, the HES invokes method 1 - request_action() of Arbitrator with request_actor = 1 and request_action_list = ‘00100’ or ‘000100’

UC06-S03 schedule-driven connection/disconnection of electricity breaker
Description: The meter has been pre-configured with a schedule to change the condition of the supply control at specific times/dates. At the appropriate time, the application process within the meter invokes the script required by the schedule. This script may directly operate the disconnect control, or it may make a request of the arbitrator to determine whether the supply control should be changed.
Scenario 10 is executed, either directly, or by Scenario 11 if the arbitrator so determines.

UC06-S05 activity calendar-driven connection/disconnection of electricity breaker
Description: The meter has been pre-configured with an activity calendar to change the condition of the supply control at specific times/dates.

UC06-S07 Remote connect/disconnect in M-Bus Device

UC06-S08 schedule-driven connect/disconnect in M-Bus device

UC06-S09 Activity calendar driven connect/disconnect in M-Bus device

[3] The arbitrator interface class is not applied in this Annex.

© Copyright 2026 Oesterreichs Energie. All rights reserved

UC06-S10 Disconnector Script invoked

Description: The SM triggers a disconnector script

UC06-S11 Arbitrator IC drives Disconnector

Description: Only required for Prepayment UC21. Optional in other situations. A script is invoked that causes the Arbitrator to recalculate and operate the Disconnector as appropriate

6.7.2. Adoption

Note that the Use Case does not contain Scenarios S04 or S06 – these were removed as part of the DLMS UA ACE SM GCP 1.0.1 review.

Scenarios S00, S01, S03, S05 and S10 are mandatory. Other scenarios are not permitted.

6.7.3. Details of technical variations (if any)

Additional entries shall be added to the script table for disconnector – these shall select the control mode of the disconnector object.

Limiter (IC=71) and Register Monitor (IC=21) objects have threshold values, and if these values are zero or arrays of zero entries then the object is disabled from controlling the disconnector.

6.7.4. Commentary

Some meters in Austria are dedicated to metering and control of controllable loads (often heating loads), and these will generally use the schedule or activity calendar configurations to control the supply control switch to activate or deactivate these loads.

6.8. Use Case ACESM-UC07 – Synchronizing the Clock

6.8.1. General information from ACE SM

6.8.1.1. Scope

This Use Case is applied to adjust the real time clock within the Meter

6.8.1.2. Objective(s)

Time is sufficiently accurate. This is for billing and other purposes including security.

6.8.1.3. Short Description

This use case describes how the HES is able to synchronize the real time clock of a meter. Setting the current time can be performed by applying the SET or ACCESS service to the attribute “time” of the “clock” object. In addition, NTP synchronization is possible as an option.

6.8.1.4. Scenarios

UC07-S1 Send NTP information to meter

Description: This scenario describes how the HES is able to synchronize the real time clock of a Meter using an NTP server.

UC07-S2 Send Time information

Description: This scenario uses the time in the HES, or gateway to set the meter's clock. While the scenario describes setting from the HES, it can be set from a suitable hub/gateway as well.

6.8.2. Adoption

Scenario 2 is mandatory. Scenario 1 may be included at the request of the purchaser. Note that Scenario 1 shall only be used if the secure credentials are applied and these are managed via the UC20. For clarity, the secure NTPv4 in accordance with RFC5905 is mandatory.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.8.3. Details of technical variations (if any)

The clocktime_shift_limit value, which is used to trigger clock adjustment events, has a maximum value of 9 seconds.

6.8.4. Commentary

Note that Dualmode-Gateways may, in addition to the head-end system, have the capability and credentials to manage the time for the meters in some deployments, and this does not affect the head-end system ability to set the clock or receive events.

6.9. Use Case ACESM-UC08 – Quality of supply

6.9.1. General information from ACE SM

6.9.1.1. Scope

Recording of power quality information. This will include both values of power parameters and occurrences of power quality events.

6.9.1.2. Objective(s)

Quality of Supply Reporting - Electricity: Meters provide Quality of Supply Reporting by monitoring and logging Current/power/voltage average values, and Event-Logs and counters

6.9.1.3. Short Description

Process of supervising Power Outages, Sags and Swells. Quality of Service parameters are logged in a Power Quality profile.

6.9.1.4. Scenarios

UC08-S01 - Quality Of Supply Configuration
Description: Configuration of Quality of Supply elements

UC08-S02 - Recording of QoS data
Description: This scenario outlines potential processes within the meter while it monitors power parameters.

UC08-S03 - Quality of Supply profiles retrieval
Description: The HES initiates collection of Quality of Supply interval and event logs

UC08-S04 - Push of Quality of Supply profiles
Description: Routine sending of interval logs and event logs

6.9.2. Adoption

This use case is mandatory for all scenarios.

6.9.3. Details of technical variations (if any)

Additional Objects for minimum and maximum voltages each phase, maximum current each phase, and power factors each phase are required in Austria and these are included in the Object Model. Note that other elements required by the regulations are included in the generic UC.

The log is required to capture 15 registers for 10 days
Capture periods 10 minute and 15 minutes are required.
Selective access by range is mandatory and by entry is mandatory.

6.9.4. Commentary

Power quality data will become of higher and higher priority in the future.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.10. Use Case ACESM-UC09 – Load management by relay

6.10.1. General information from ACE SM

6.10.1.1. Scope

Control of loads within the customer premises by means of relays managed by the meter managed by an activity_calendar and also by direct command in real time.

6.10.1.2. Objective(s)

Specific load(s)/source(s) are controlled: The meter controls the controllable loads or sources in accordance with the configuration selected.

6.10.1.3. Short Description

Process of controlling specific local loads or power sources by means of relays.

6.10.1.4. Scenarios

UC09-S1 Configuration of load management by relay
Description: Configuration and direct control of Load Management by relay

UC09-S2 Timed relay operations
Description: The relay(s) change state according to the time plan configuration

UC09-S3 Ad-hoc operation (proposed)
Description: The HES sends instructions to the meter to change the state of the relay(s)

6.10.2. Adoption

This use case is mandatory

6.10.3. Details of technical variations (if any)

Entry into the log book for switching – seperate log book for relays.
Relays may be controlled by the prime or an additional Limiter Object. One to four additional limiter objects are required and these are included in the Object Model. These act on the script table entries for relay control (rather than the main supply control switch) and they may be controlled by import or export power, current or voltage values.

6.10.4. Commentary

Control of night storage heating and similar loads is likely to be augmented with additional load control needs, some of which may require sensitivity to grid conditions.

6.11. Use Case ACESM-UC10 – Firmware update

6.11.1. General information from ACE SM

6.11.1.1. Scope

This Use Case covers the execution of a firmware update process between HES and Electricity Meter. Images may be transferred directly from the HES or from an external delivery tool - this may be a gateway or other network element.

- The Use Case may be applied for:
- metrological firmware
- non-metrological firmware
- firmware for other meter elements (e.g. software defined radio or modem)

© Copyright 2026 Oesterreichs Energie. All rights reserved

- patches and incremental updates

6.11.1.2. Objective(s)

Delivery and activation of appropriate firmware image

6.11.1.3. Short Description

Process of downloading new firmware to Smart Meter or Submeter

6.11.1.4. Scenarios

UC10-S1 Update firmware on a Smart Meter-Detailed Description: This is the traditional approach. The HES (or a similar server) delivers the whole process, pushing blocks to the Meter.

UC10-S4 Update firmware on a Submeter

Description: The HES delivers an image to the Electricity Meter and this is forwarded to the Submeter and activated.

UC10-S5 Verification of update

Description:The HES verifies that the firmware image has deployed correctly.

6.11.2. Adoption

Only scenario S1 is mandatory. Scenario 4 is not used in Austria. Scenario 5 is desirable.

6.11.3. Details of technical variations (if any)

Oe Energie notes the following additional requirements:

1. The update of the legally relevant firmware is subject to legal metrological certification.
2. The update must be registered in a certification protected event log
3. The event log itself is part of the functionality under legal control.
4. The recorded information contains the currently active FW version and the client system title for the identification of who initiated the certification relevant change.
5. The event log is not allowed to be deleted and no further updates are possible in case the event log is full.
6. This event log must also be shown on the meter display
7. Firmware version must be higher, or rejected by the meter
8. Meter shall validate the firmware signature and reject if the signature is not valid.
9. Meter data shall not be altered by the firmware update
10. Higher level signature to Suite 2 is mandatory

The scenario 1 may be delivered by multiple clients: the HES is required to initiate the firmware update process if this is remote, but an external device, a Dualmode-Gateway or other device may be that responsible. The scenario 1 shall be capable of being delivered via the service interface.

6.11.4. Commentary

It should be noted that the meter, on receipt of the activation command, will verify the digital signature of the assembled firmware image and, if the image is not correct, then abort the activation process and return an error message.

Note that current regulations seem to conflict regarding application of firmware images – for example there is a perceived requirement in RED and CRA for firmware to be updated rapidly when there is a security incident that contradicts the approval process required to comply with the MID.

Multicast of firmware images using the FW upload client. A pre-shared multicast (GBEK) is used by the FW client to multicast images to meters. This Key is controlled from the maintenance or security associations. This permits

© Copyright 2026 Oesterreichs Energie. All rights reserved

a firmware image device to multicast the image packets to meters. The FW upload client may use a pre-established AA.

6.12. Use Case ACESM-UC11 – Meter supervision

6.12.1. General information from ACE SM

6.12.1.1. Scope

This use case controls the configuration and execution of meter operations related events and alarms performed by the meter using push functionality and as direct readouts. Note that delivery of the Event Logs by routine datanotification is configured in UC16 / UC05.

6.12.1.2. Objective(s)

Meter reports correctly: Meter supervision event and alarm occurrences are delivered in accordance with the HES needs.

6.12.1.3. Short Description

Use case used to manage Smart Meter and optionally submeter Events and Alarms supervision.

6.12.1.4. Scenarios

UC11-S1 Configure meter supervision events and alarms
Description: This scenario describes the main activities to send meter supervision configuration information from the Head End System to the Smart Meter

6.12.2. Adoption

This use case is mandatory.

6.12.3. Details of technical variations (if any)

Submeter objects are not included and not required.

Additional object is required as the metrological error register, which is a Data type Object with OBIS code 0-0:97.97.1.255. The content of this register will be a bit string, and the content of the bit string will be one or more errors that the meter records where metrology is compromised. Any error in this register is considered as legally relevant and causes the cancellation of its metrological certification. The meter shall display this error register as part of the automatic display sequence if one or more bits within the bit string are set. The bit-allocation in this Fatal Error Register is manufacturer specific. This register may not be reset.

6.12.4. Commentary

This use case covers events and alarms covering the operations of the meter itself, and includes events similar to cover removal and tamper indications.

6.13. Use Case ACESM-UC12 – Consumer Information

6.13.1. General information from ACE SM

6.13.1.1. Scope

This use case controls the configuration of the Customer Interface including the actual physical port, the security applied and the data items and the frequency of sending.

6.13.1.2. Objective(s)

Consumer Information Delivery: Deliver information to customer equipment.

6.13.1.3. Short Description

This use case enables configuration of, protection of, and delivery of meter data to customer equipment via a physical customer port on the meter.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.13.1.4. Scenarios

UC12-S1 Deliver Consumer Information

Description: The meter sends the required customer information to a remote display via the customer interface.

UC12-S2 Configure Consumer Information set

Description: The HES configures the meter to deliver information via the customer interface.

6.13.2. Adoption

Customer Information Port is mandatory in Austria.

6.13.3. Details of technical variations (if any)

An additional object, 0-0:96.3.3.255 is added to the list of items that may be displayed. This object's attribute 2 will indicate status elements, for example, status of load control relays, in the first instance.

6.13.4. Commentary

It is necessary to share a security key between the meter and the customer equipment. DSOs will execute their own approach to sharing this key.

Enablement and disablement of the customer information is to be achieved by configuring the time at which the push setup object delivers data to the CII.

6.14. Use Case ACESM-UC13 – Communication supervision

6.14.1. General information from ACE SM

6.14.1.1. Scope

This UC covers the monitoring and recording of the status of communications between the meter and the HES, and the meter and local port.

6.14.1.2. Objective(s)

To facilitate diagnostics of the communications between meter and HES: The data assists in diagnosing issues with the meter's configuration and location within a specific network and can facilitate changes of configuration including placement into alternative network.

6.14.1.3. Short Description

Intention is to collect and provide information regarding the communication network(s) that would be useful to identify potential communication problems and service performance.

6.14.1.4. Scenarios

UC13-S01 Get Communication Logs

Description: The scenario describes main activities to collect communication logs from the Smart Meter by the Head End System

UC13-S02 Get Communication Network Statistic

Description: Collection of counters and other measured values related to the performance and effectiveness of the relevant data transport.

UC13-S03 Get Communication Alarms

Description: The Smart Meter monitors activities on the local port and notifies the Head End System if there is any communication attempt on the local port and logs those activities.

6.14.2. Adoption

This use case is mandatory.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.14.3. Details of technical variations (if any)

<none>

6.14.4. Commentary

This use case is extended by UC-Oe-01 and to some extent by UC-Oe-03.

6.15. Use Case ACESM-UC14 – Enabling and disabling functionalities

6.15.1. General information from ACE SM

6.15.1.1. Scope

This Use Case allows the activation or deactivation of specific functions, e.g. enabling and disabling of interval data logs, primarily for data protection reasons, and activation or deactivation of the optical interface.

6.15.1.2. Objective(s)

Functionalities controlled: Functions within the scope of this use case are enabled and disabled as appropriate.

6.15.1.3. Short Description

This use case is used to enable or disable functionalities using Function control interface class objects (class 122).

6.15.1.4. Scenarios

UC14-S1 Send Enable/Disable functionality request
Description: This scenario describes the main activities to send requests to enable and disable a functionality from the Head End System to the ACESM Meter

UC14-S2 Send Scheduled Enable/Disable Functionality Request
Description: In this scenario, the HES configures a schedule to execute a series of scripts to operate the function control objects to enable/disable the functionalities.

6.15.2. Adoption

Both scenarios are adopted, noting that the objects related to submetering logging are not supported.

6.15.3. Details of technical variations (if any)

1) Objects supporting control of the submeter logs are not supported.
2) An additional object is applied for the control of the service (optical) interface. This is a communications port object, and this is described in the Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**.

6.15.4. Commentary

See chapter 7 for more details of the protection of the service interface.

6.16. Use Case ACESM-UC15 – Power control

6.16.1. General information from ACE SM

6.16.1.1. Scope

This UC covers operation of supply control switch and other relays, and recording events, due to network and load conditions.

6.16.1.2. Objective(s)

Reduction in export: To limit customer production where network constraints or oversupply are indicated. Supply reliability: Use of fuse supervision allows the meter to isolate supply in the event of an overload condition, reducing the occurrence of fuse blowing and consequential site visits. NOTE that the use of fuse supervision DOES NOT replace the need for a fused cutout at the supply point. Reduction in load: The customer load is to be reduced or prevented in situations where there is excessive demand.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.16.1.3. Short Description

Process of executing specific actions depending on the power limits reached by the supervised values

6.16.1.4. Scenarios

UC15-S0 Configuration of power control systems
Description: This scenario configures the behaviour of the meter with respect to operation of supply control and load control elements and other indications due to customer demand.

UC15-S1 Limiter Action on Supply Control
Description: When load is outside configured thresholds, the meter records limiter threshold events.

UC15-S2 Limiter action on Load Control
Description: When a load condition is outside the permitted thresholds, the events are recorded and the meter may, if so configured, act by operating the load control in accordance with the configured options.

UC15-S3 Current Supervision
Description: The meter monitors current over a sliding average and recording events when thresholds are crossed, and, by configuration, effecting a change of state of the supply control switch as per conditions which would also generate events.

6.16.2. Adoption

The use case is mandatory and extended as per the details below.

6.16.3. Details of technical variations (if any)

1. Additional Limiter objects. 3 additional limiter objects are required to provide import and export functions, and two levels of action.
2. Additional events for the additional limiters are also required:
3. Alarm function (and identification) is needed that can operate by configuration with scenarios 1..3.

6.16.4. Commentary

Further consideration may be needed in order to prevent unexpected interactions between the limiter objects.

6.17. Use Case ACESM-UC16 – Event management and alarm reporting

6.17.1. General information from ACE SM

6.17.1.1. Scope

This use case covers the activities of the meter and the HES in the situation where an event occurs, and possibly triggers an alarm, and the resetting of the alarm.
Note that push of event logs using routine data methods is covered in UC05 - periodic meter reading.

6.17.1.2. Objective(s)

Meter responds correctly to the occurrence.: When the occurrence takes place, the meter records the event and, as appropriate, sends the alarm datanotification as part of the alarm process.
Should the alarm process be triggered, then the HES will, in response to the datanotification, take action to clear the meter alarm state.

6.17.1.3. Short Description

This use case describes the process of managing events and reporting and acknowledging alarms detected in the Meter to the HES.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.17.1.4. Scenarios

UC16-S1 Event management and Alarming process

Description: This scenario describes the main activities to store detected events, send alarms from the ACESM Meter to the Head End System, and acknowledge them.

6.17.2. Adoption

This use case is mandatory.

Details of technical variations (if any)

An additional set of alarm registers is added to the object model. These registers will function identically to the alarm register, descriptor, monitor & filter objects in the existing use case.
The meter shall support the extra objects as per the Object Model and extra events as per the Object Model. Some Events have specific definitions in the Object Model and meters shall comply with these definitions.

Some Event Logs for fraud, security and certification may not be over-written or reset, and relevant requirements are included in the Object Model.

Randomization of Alarm push. The default setting in the ACE SM GCP for pushing of Alarms is without randomization, but Austria will require that a time randomization is configured.

6.17.3. Commentary

<none>

6.18. Use Case ACESM-UC17 – Meter availability Control

6.18.1. General information from ACE SM

6.18.1.1. Scope

The HES is required to verify that communications can be established with a meter, and reads out the meter identifier to confirm the meter reads correctly. In some situations it can also be used to confirm that the correct meter is read.

6.18.1.2. Objective(s)

Understanding the meter availability: Verification that the meter is available for communications on the data network. This can aid in diagnosing unmanaged networks (e.g. GSM).

6.18.1.3. Short Description

This use case checks the availability of the smart meter in the communication network.

6.18.1.4. Scenarios

UC17-S01 Check meter availability

Description: The scenario describes checking of the smart meter communication availability on the remote communication interface either in case of wide area or neighbourhood network connection.

6.18.2. Adoption

This use case is mandatory.

6.18.3. Details of technical variations (if any)

None.

6.18.4. Commentary

This is a simple “Meter Ping” Use Case.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.19. Use Case ACESM-UC18 – Display messages on meter display

6.19.1. General information from ACE SM

6.19.1.1. Scope

This Use Case covers display of measured values and other information on the meter's display. The scope is determined by SM WG Use Cases for Generic Smart Metering Profile.

6.19.1.2. Objective(s)

Manage information presented on meter display: The objective is to manage the display of measurements and other information on the meters display.

6.19.1.3. Short Description

SUC used to display meter readings and other information on Smart Meter local display.

6.19.1.4. Scenarios

UC18-S1 Meter Displays Information

Description: The Electricity meter displays measured and other information items according to the configuration.

UC18-S2 Configure display information

Description: The HES sets up the lists of information that is displayed in automatic and manual scroll modes.

6.19.2. Adoption

This use case is mandatory.

6.19.3. Details of technical variations (if any)

1) When a fatal error occurs, then the display shall show that this has occurred and the event code as the default display on the automatic display sequence and the display shall not show a fatal event code otherwise.
2) There is a requirement for harmonized control of the time to revert to automatic scrolling, and this is controlled in 0-0:94.43.20.255.
3) There is a requirement for harmonized control of the time between displayed items in the auto scroll operation, and this is controlled in 0-0:94.43.21.255
4) There is a requirement that load profile data is displayed on the meter, and this is available for the last 60 days. This is for two load profiles, the 15 minute profile and the 24h profile. These are outlined in the Object Model. The Object to manage this display profile is 0-0:21.0.3.255.
5) There is a requirement that load profile data should not be shared with a new occupier. There is a need, therefore, to establish control of the display of the load profile on the meter display. When there is a change of occupier, the load profiles shall be prevented from display by changing the configuration of the manual display sequence. When 60 days have elapsed, then the profile data shall become available again to the occupier of the premises.
6) When there is need to display a text message to the consumer, that will be displayed as the default item in place of the automatic display sequence. The meter will have a method for clearing this text message when the viewer interacts with the buttons on the meter.

6.19.4. Commentary

<none>

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.20. Use Case ACESM-UC19 – Configuration of meter locally

6.20.1. General information from ACE SM

6.20.1.1. Scope

This UC covers the changes of configuration items by a field technician at any point during the life cycle of the meter.

6.20.1.2. Objective(s)

Meter operating in accordance with the configuration: The configuration has been successfully delivered.

6.20.1.3. Short Description

This use case handles the process of adjusting of the meter configuration at the installation location during installation,deployment, maintenance and end of life cycle phase.

6.20.1.4. Scenarios

UC19-S1 Deliver configuration locally

Description: This use case handles the process of adjusting of the Smart Meter configuration at the installation location during deployment, maintenance and end of life cycle phase

6.20.2. Adoption

This is mandatory. It shall be capable of being applied to any configuration scenario of any other use case where applicable.

6.20.3. Details of technical variations (if any)

Only roles applicable to the service interface shall be permitted to control the configuration of the meter as defined in the Object Model.

6.20.4. Commentary

The meters will have unique security keys. Therefore DSOs will require a mechanism for the secure distribution and replacement of the keys related to the delivery of this Use Case.

6.21. Use Case ACESM-UC20 – Manage meter security settings

6.21.1. General information from ACE SM

6.21.1.1. Scope

This use case describes the methods used to change security credentials on meters and submeters where appropriate, and change other security settings as needed - for example, security_suite, security_policy.

6.21.1.2. Objective(s)

Data and messages are protected: Data and messages are provided with protection for confidentiality, integrity, and authenticity.

6.21.1.3. Short Description

Setting and updating security credentials and other security settings in the Smart Meter and optionally Submeter

6.21.1.4. Scenarios

UC20-S0 Meter security configuration

Description: This scenario describes the main activities to change the security configuration, specifically to Set Security Policy, and import certificates.

UC20-S1 Smart Meter key update

Description: This scenario describes the main activities to transfer Smart Meter Security Information from the Head End System to the Smart Meter.

© Copyright 2026 Oesterreichs Energie. All rights reserved

UC20-S2 Submeter Security Settings

UC20-S3 Meter Certificate update

Description: This scenario describes the main activities to create and transfer Meter Certificates between the Head End System to the Smart Meter.

6.21.2. Adoption

Scenarios S0, S1 and S3 are mandatory. Scenario S2 is not applicable.

6.21.3. Details of technical variations (if any)

Security suite 2 in accordance with table 27 of Green Book shall be used, that is:

Table 5 – Cryptographic Algorithms

Protection	Algorithm
Authenticated Encryption	AES-GCM-256
Digital Signature	ECDSA with P-384
Key Agreement	ECDH with P-384
Hash	SHA-384
Key transport	AES-256 key wrap

The meter shall comply with the requirements of the E2E-Sicherheit-Anforderungskatalog ("F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf"), especially requirement SPR_02.

This will need extended objects to map additional Application Associations, and these are outlined in the Object Model

When Scenario 0 is applied to update the current Application Association, then the Meter shall release the AA immediately after sending any responses.

When Scenario 1 is applied to update keys, this is only applied using the Security Officer Role using the key wrapping key (master key) appropriate to the Application Association being updated.

The generation of keys requires a certain standard of randomness. the meter shall generate keys in accordance with SPR_02 Other key generation (that is, within the AMI ecosystem) shall generate keys in accordance with relevant requirements of the „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf".

CSRs provided by the meter shall comply with PKCS # 10, noting the following fields are to be completed as agreed between the vendor and the DSO. Note that the PKI section in the DLMS Green Book 12, clause 9.2.6.3 provides guidance on certificates.

Certificate locations within the SEM shall be managed by agreement between the vendor and the DSO.

6.21.4. Commentary

Note that the submeter scenario is not permitted.

6.22. Use Case ACESM-UC21 – Prepayment metering

6.22.1. General information from ACE SM

6.22.1.1. Scope

Prepayment includes configuration, credit adjustments, payment token processing. This applies to processing within the meter - where the payment processing takes place in the HES or related systems then the control of the SCS is covered by UC06.

6.22.1.2. Objective(s)

To enable the implementation of payment metering in smart electricity meters and submeters, and maintain interoperability as such is done.

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.22.1.3. Short Description

Process of managing payment metering. This use case is largely based on the payment metering processes and functions defined in IEC 62055-21.

6.22.1.4. Scenarios

UC21-S1 Switching to payment mode, remotely

UC21-S2 Top-up Token Credit manually

UC21-S3 Top-up Token Credit remotely

UC21-S4 Collection of consumption charges

UC21-S5 Collection of standing charges

UC21-S6 Management of non-disconnect period

UC21-S7 Provision of emergency credit

UC21-S8 Manage available credit

UC21-S9 Switch to credit mode

6.22.2. Adoption

This use case shall be disabled.

6.22.3. Details of technical variations (if any)

This is an optional use case in the ACE SM GCP. Meters intended for use in Austria shall have this functionality disabled. Note that one option to achieve this is to ensure that any Objects related to prepayment have all access rights disabled in all Application Associations.

6.22.4. Commentary

Prepayment in Austria is achieved by direct control of the supply control switch using Use Case 06.

6.23. Use Case Oe-01 – Communications Configuration.

6.23.1. Description of the use case

6.23.1.1. Name of use case

Use case identification		
ID	***Area(s)/Domain(s)/Zone(s)***	***Name of use case***
	Austria	Oe-UC-01 Communications Configuration

6.23.1.2. Scope and objectives of use case

Scope and objectives of use case	
Scope	Configuration of the meter's PLC and other communications parameters, including enablement and disablement, and fallback to previous settings. NOTE that, where a communications module is attached to the meter, but the communications module has a separate identity, this use case is likely to be applied. Configuration of hubs/gateways is not in scope of this use case.
Objective(s)	Communications Control: Control of communications elements allows reliable communications to be maintained.
Related business case(s)	

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.23.1.3. Narrative of Use Case

Narrative of use case
Short description
Configuration of communications parameters needed for PLC and P2P technologies.
Complete description
Configuration of communication parameters for P2P and PLC communication technologies. Specifically parameters related to G3 technology, changing of frequency bands and notching tables, with the addition of a fallback option so that communications is attempted using the previous settings unless communications is established using the new settings. This also covers the situation where multiple communication technologies are possible, or where there is a requirement to switch off wide area communications completely. Summary of use case • **UC-Oe01-S1 Cellular configuration design and delivery** Description: The HES receives a Cellular configuration design to be delivered to the meter and delivers it. • **UC-Oe01-S2 G3 configuration design and delivery** Description: The HES receives a G3 configuration design to be delivered to the meter and delivers it. • **UC-Oe01-S3 Configuration of multiple transports** Description: This scenario allows the enablement and disablement of individual transport technologies, including the ability to disable all the wide area capability of the meter. • **UC-Oe01-S4 Configuration activation and fail over** Description: The new communications configuration is activated by a schedule. If this communications implementation does not succeed then the meter returns to previous configuration settings. • **UC-Oe01-S5 Ethernet configuration design and delivery** Description: The HES receives an ethernet configuration design to be delivered to the meter and delivers it.

6.23.1.4. Key performance indicators (KPI)

Key performance indicators			
ID	***Name***	***Description***	***Reference to mentioned use case objectives***
1	Dependable Communications	Communications are reliable to meet national requirements.	Communications Control
2	Effective fail over	Communications failure due to misconfiguration is recoverable without site visit.	Communications Control

6.23.1.5. Use case conditions

Use case conditions	
Assumptions	
1	Correct AA set: The Correct Application Association is already set up and communication is possible. Application Association is the role based relationship used to establish the rules for the communication session.

© Copyright 2026 Oesterreichs Energie. All rights reserved

	Prerequisites
1	Communications is possible: The Electric Meter can be communicated with (either through the WAN or via a site visit)

6.23.2. Further information to the use case for classification/mapping

Classification information
Relation to other use cases
<<BUC>> Extensions <<SUC>> Oe-UC-03 Communications Module Management
Level of depth
Overview
Prioritisation
Mandatory for Austria.Note that Scenarios 1,2 and 5 are applied when the appropriate transports are employed.
Generic, regional or national relation
Austria
Nature of the use case
SUC
Further keywords for classification

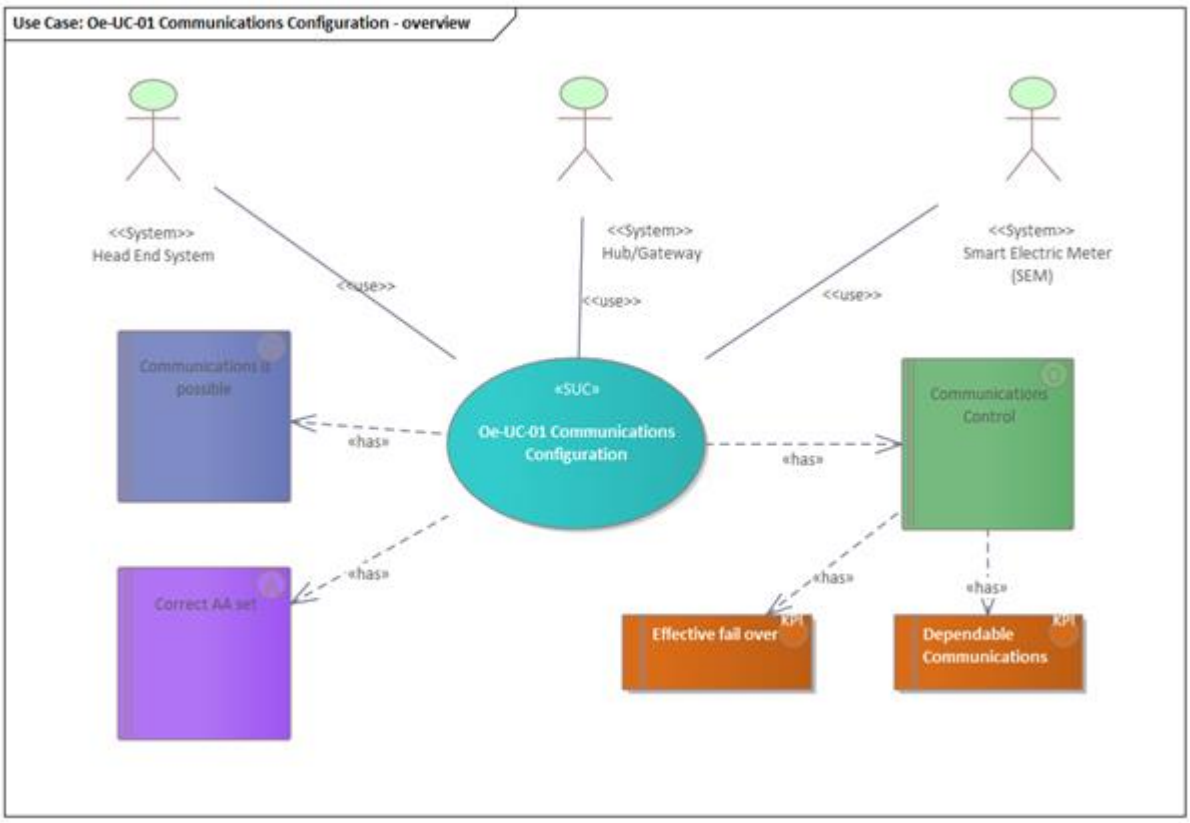
6.23.2.1. General remarks

General remarks
G3 Configuration Interface Classes: The G3 related interface classes are extremely complex, and are detailed in the Blue Book.
P2P interface classes: The P2P interface classes are complex and are detailed in the Blue Book
WAN communications disablement: TO BE DISCUSSED Is there a requirement that all remote communications be disabled? Input expected from the security workstream.
Configuration errors: Configurations will be made up of sequences of commands. each element in the sequence is likely to be a seperate SET command. DLMS provides responses to each SET command, and the HES should have methods to manage the process depending on the error response received. The responses are: success (0), hardware-fault (1), temporary-failure (2), read-write-denied (3), object-undefined (4), object-class-inconsistent (9), object-unavailable (11), type-unmatched (12), scope-of-access-violated (13), data-block-unavailable (14), long-get-aborted (15), no-long-get-in-progress (16), long-set-aborted (17), no-long-set-in-progress (18), data-block-number-invalid (19), other-reason (250)

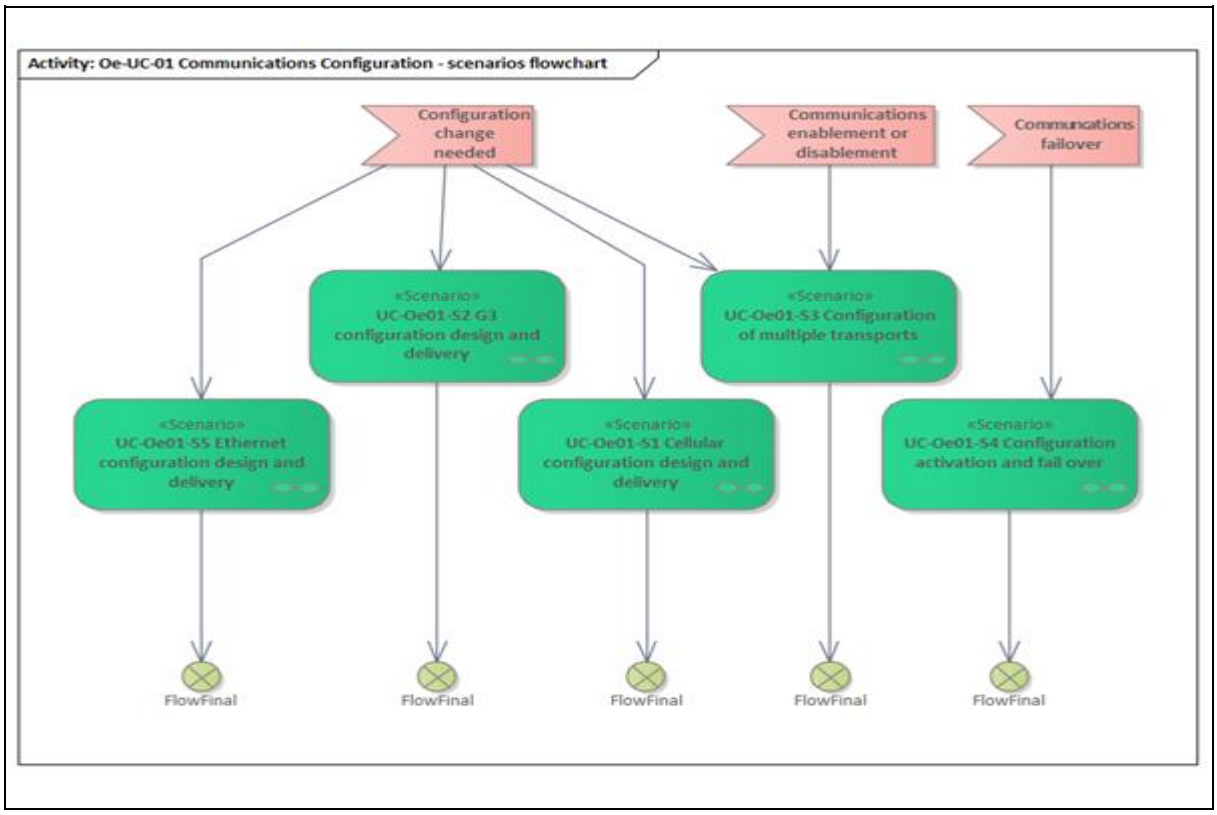
© Copyright 2026 Oesterreichs Energie. All rights reserved

When one of these responses is received, the HES needs to retry or take other appropriate action. Note that it is possible that when configuring a sub-device (e.g. a modem) that the device will set an inappropriate value into the sub-device, and mis-handle the error it receives (an example may be that the HES attempts to change the modem in a meter to limit to 2G CSD communications when the modem is only capable of 4G, but the meter sends the command to the modem and does not correctly handle the error message from the modem).

6.23.3. Diagrams of use case

Diagram(s) of use case


© Copyright 2026 Oesterreichs Energie. All rights reserved



6.23.4. Technical details

6.23.4.1. Actors

Actors			
Grouping (e.g. domains, zones)		***Group description***	
Actor name	***Actor type***	***Actor description***	***Further information specific to this use case***
Head End System	System	Head End System offers services to collect metering data and also to deliver configuration and other commands to the meters. It usually interacts with other business systems to deliver the meter data and other services to other business units and to wider industry.	
Hub/Gateway	System	Hub/Gateway is an intermediate device that is interposed between the Smart Meter and the HES. It may be a simple relay device or have intelligence to read meters and perform other functions directly.	
Smart Electric Meter (SEM)	System	Smart Meter is an AC Electricity Meter with additional functions.	

6.23.4.2. References

References						
No.	***Reference Type***	***Reference***	***Status***	***Impact on use case***	***Originator / organisation***	***Link***

© Copyright 2026 Oesterreichs Energie. All rights reserved

1	Standard	ITU-T G.9903 (2017) Amd. 2 (03/2023)	Published	Description of the G3 technology	ITU	https://www.itu.int/rec/T-REC-G.9903
2	Standard	TS 24.301	Published	P2P standard	3GPP	
3	Standard	TS 36.101	Published	P2P standard	3GPP	
4	Standard	TS 36.331	Published	P2P standard	3GPP	
5	Standard	TS 36.306	Published	P2P Standard	3GPP	
6	Standard	TS 36.3213	Published	P2P Standard	3GPP	

6.23.5. Step by step analysis of use case

6.23.5.1. Overview of scenarios

Scenario conditions						
No.	***Scenario name***	***Scenario description***	***Primary actor***	***Triggering event***	***Pre-condition***	***Post-condition***
1	UC-Oe01-S1 Cellular configuration design and delivery	The HES receives a Cellular configuration design to be delivered to the meter and delivers it.	Head End System	Configuration change needed: Data reliability measurements and experiments determine that a new configuration is preferable. Time for activation may or may not be configured.	New configuration designed: A new configuration is designed for the cellular modem of the meter.	New configuration delivered.: The new configuration is delivered and waiting on the meter for time_based activation
2	UC-Oe01-S2 G3 configuration design and delivery	The HES receives a G3 configuration design to be delivered to the meter and delivers it.	Head End System	Configuration change needed: Data reliability measurements and experiments determine that a new configuration is preferable. Time for activation may or may not be configured.	New configuration designed: A new configuration is designed for the G3 of this meter	New configuration delivered: The new configuration is delivered and waiting on the meter for time based activation.

© Copyright 2026 Oesterreichs Energie. All rights reserved

3	UC-Oe01-S3 Configuration of multiple transports	This scenario allows the enablement and disablement of individual transport technologies, including the ability to disable all the wide area capability of the meter.	Head End System	Configuration change needed: Data reliability measurements and experiments determine that a new configuration is preferable. Time for activation may or may not be configured. Communications enablement or disablement: Communications from a specific device is to be disabled or re-enabled.	Proposed change to transports configuration: The HES has a design for a change to the configuration of transport priorities	Meter applying new priorities: The meter is using the new priorities to determine which communications transports to use.
4	UC-Oe01-S4 Configuration activation and fail over	The new communications configuration is activated by a schedule. If this communications implementation does not succeed then the meter returns to previous configuration settings.	Smart Electric Meter (SEM)	Communcations failover: Time has passed and the E Meter has been unable to communicate using the new settings, and therefore reverts to the previous settings.	Pending configuration present: A pending configuration change is in place on the meter	Communications is established: The Meter can communicate with the Head End System
5	UC-Oe01-S5 Ethernet configuration design and delivery	The HES receives an ethernet configuration design to be delivered to the	Head End System	Configuration change needed: Data reliability measurements and experiments determine that a	New Ethernet Configuration designed: A new configuration for the	New configuration delivered.: The new configuration is delivered and waiting on the

© Copyright 2026 Oesterreichs Energie. All rights reserved

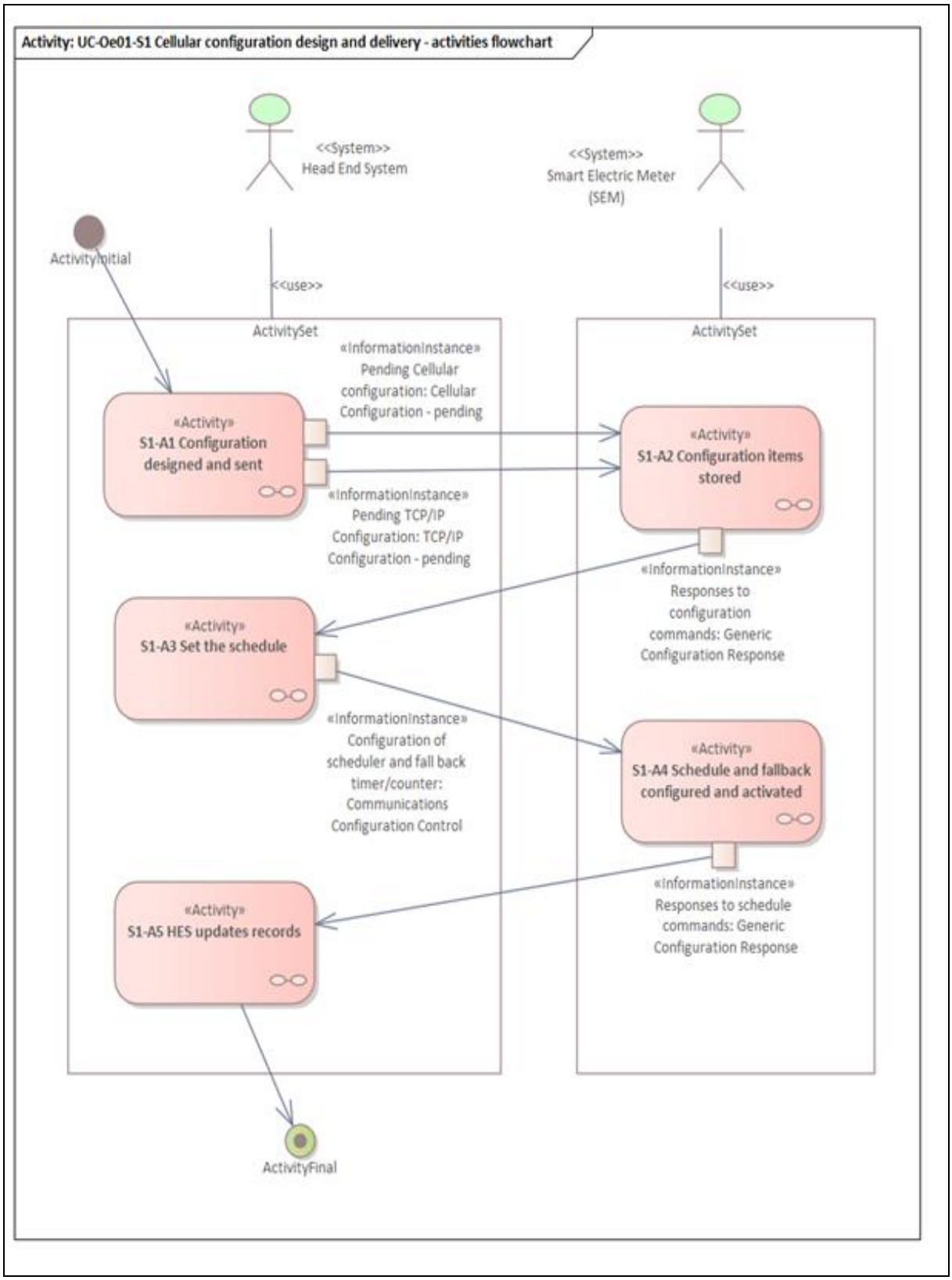
		meter and delivers it.		new configuration is preferable. Time for activation may or may not be configured.	ethernet is proposed.	meter for time_based activation

6.23.5.2. Steps - Scenarios

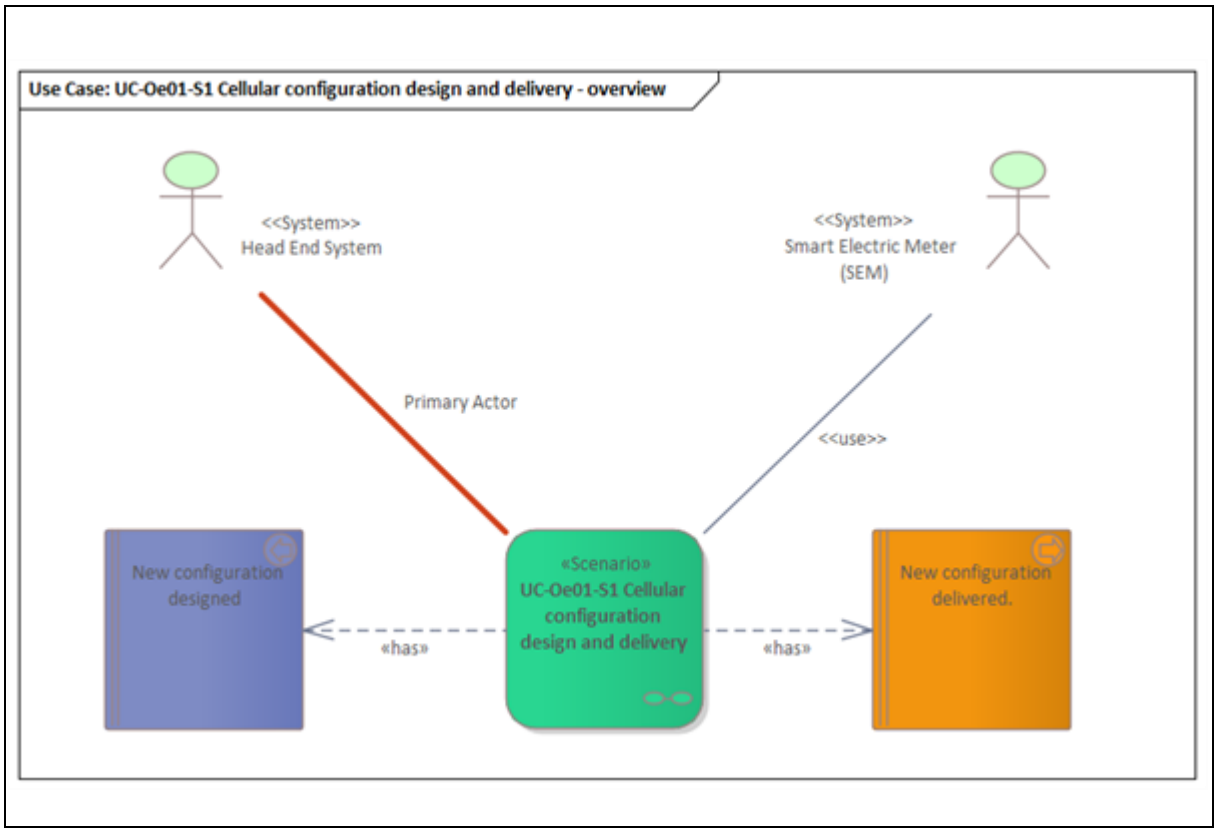
6.23.5.2.1. UC-Oe01-S1 Cellular configuration design and delivery

© Copyright 2026 Oesterreichs Energie. All rights reserved

The HES receives a Cellular configuration design to be delivered to the meter and delivers it.



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	UC-Oe01-S1 Cellular configuration design and delivery							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
1.1		S1-A1 Configuration designed and sent	The HES has a configuration planned and sends it to the meter.		Head End System	Smart Electric Meter (SEM)	Info1-Cellular Configuration - pending, Info2-TCP/IP Configuration - pending	
1.2		S1-A2 Configuration items stored	The items are stored in the pending objects awaiting activation.		Smart Electric Meter (SEM)	Head End System	Info3-Generic Configuration Response	
1.3		S1-A3 Set the schedule	The timer to initiate the comms change is activated.		Head End System	Smart Electric Meter (SEM)	Info4-Communications Configuration Control	
1.4		S1-A4 Schedule and fallback configured and activated	The timer for fallback is set.		Smart Electric Meter (SEM)	Head End System	Info3-Generic Configuration Response	

© Copyright 2026 Oesterreichs Energie. All rights reserved

1.5		S1-A5 HES updates records	The HES receives the responses and updates its records and any external systems accordingly.		Head End System			

- 1.1. S1-A1 Configuration designed and sent

Information Overview: UC-Oe01-S1 Cellular configuration design and delivery/S1-A1 Configuration designed and sent

The HES has a configuration planned and sends it to the meter.
Information sent:

Information object	*Instance name*	*Instance description*
Cellular Configuration - pending	Pending Cellular configuration	configuration items related to cellular communications, may include APN information, network choices, etc.
TCP/IP Configuration - pending	Pending TCP/IP Configuration	Items related to the configuration of IP communications

- 1.2. S1-A2 Configuration items stored

Information Overview: UC-Oe01-S1 Cellular configuration design and delivery/S1-A2 Configuration items stored

The items are stored in the pending objects awaiting activation.
Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Responses to configuration commands	The meter sends response(s) as appropriate.

- 1.3. S1-A3 Set the schedule

Information Overview: UC-Oe01-S1 Cellular configuration design and delivery/S1-A3 Set the schedule

The timer to initiate the comms change is activated.

Information sent:

Information object	*Instance name*	*Instance description*
Communications Configuration Control	Configuration of scheduler and fall back timer/counter	These attributes are the time for activation, and also a timeout after which the meter returns to previous settings.

- 1.4. S1-A4 Schedule and fallback configured and activated

Information Overview: UC-Oe01-S1 Cellular configuration design and delivery/S1-A4 Schedule and fallback configured and activated

The timer for fallback is set.

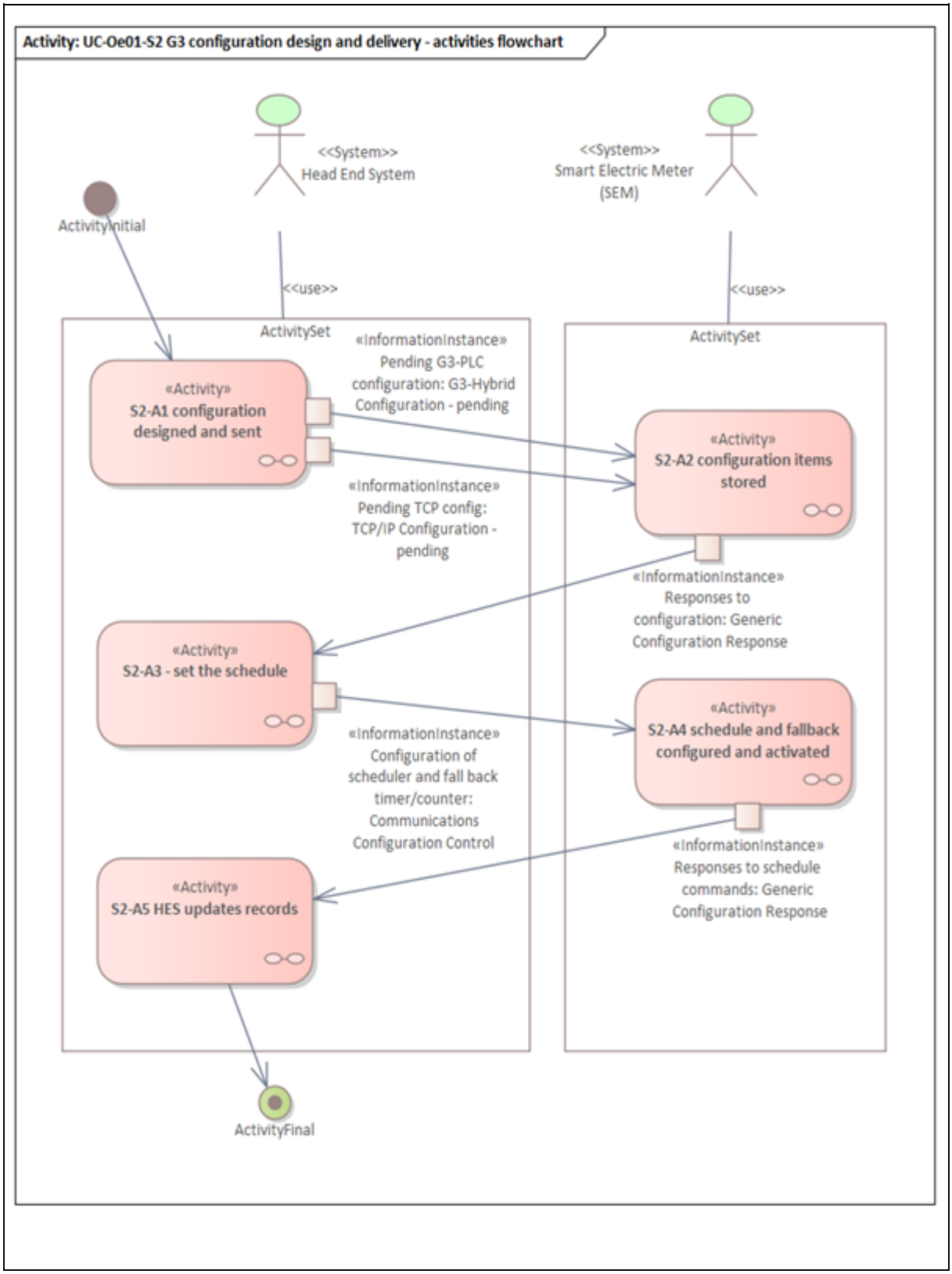
Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Responses to schedule commands	(generic response)

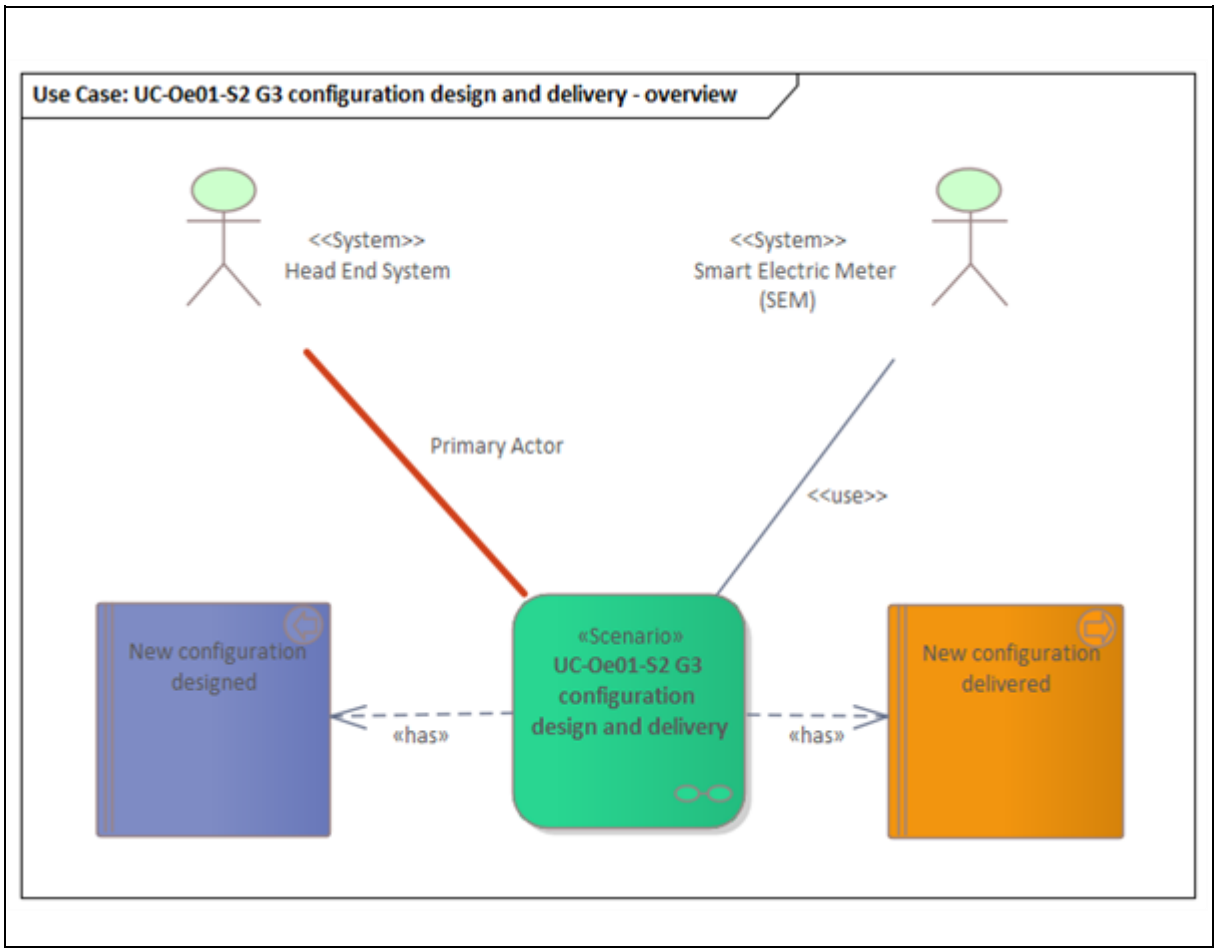
6.23.5.2.2. UC-Oe01-S2 G3 configuration design and delivery

© Copyright 2026 Oesterreichs Energie. All rights reserved

The HES receives a G3 configuration design to be delivered to the meter and delivers it.



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	UC-Oe01-S2 G3 configuration design and delivery							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
2.1		S2-A1 configuration designed and sent	The HES creates and sends the configuration.		Head End System	Smart Electric Meter (SEM)	Info5-G3-Hybrid Configuration - pending, Info2-TCP/IP Configuration - pending	
2.2		S2-A2 configuration items stored	The meter receives the commands, validates and processes them, and sends responses.		Smart Electric Meter (SEM)	Head End System	Info3-Generic Configuration Response	
2.3		S2-A3 - set the schedule	The HES sets the activation and any fallback		Head End System	Smart Electric	Info4-Communications	

© Copyright 2026 Oesterreichs Energie. All rights reserved

			information into the meter.			Meter (SEM)	Configuration Control	
2.4		S2-A4 schedule and fallback configured and activated	The schedule is set and active for the activation time		Smart Electric Meter (SEM)	Head End System	Info3-Generic Configuration Response	
2.5		S2-A5 HES updates records	The HES stores and forwards response information to other systems		Head End System			

- 2.1. S2-A1 configuration designed and sent

  Information Overview: UC-Oe01-S2 G3 configuration design and delivery/S2-A1 configuration designed and sent

  The HES creates and sends the configuration.

  Information sent:

Information object	*Instance name*	*Instance description*
TCP/IP Configuration - pending	Pending G3-PLC configuration	Pending G3 objects
G3-Hybrid Configuration - pending	Pending TCP config	Pending internet protocol objects

- 2.2. S2-A2 configuration items stored

  Information Overview: UC-Oe01-S2 G3 configuration design and delivery/S2-A2 configuration items stored

  The meter receives the commands, validates and processes them, and sends responses. Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Responses to configuration	(generic response)

- 2.3. S2-A3 - set the schedule

  Information Overview: UC-Oe01-S2 G3 configuration design and delivery/S2-A3 - set the schedule

  The HES sets the activation and any fallback information into the meter. Information sent:

Information object	*Instance name*	*Instance description*
Communications Configuration Control	Configuration of scheduler and fall back timer/counter	Configuration of timers.

- 2.4. S2-A4 schedule and fallback configured and activated

  Information Overview: UC-Oe01-S2 G3 configuration design and delivery/S2-A4 schedule and fallback configured and activated

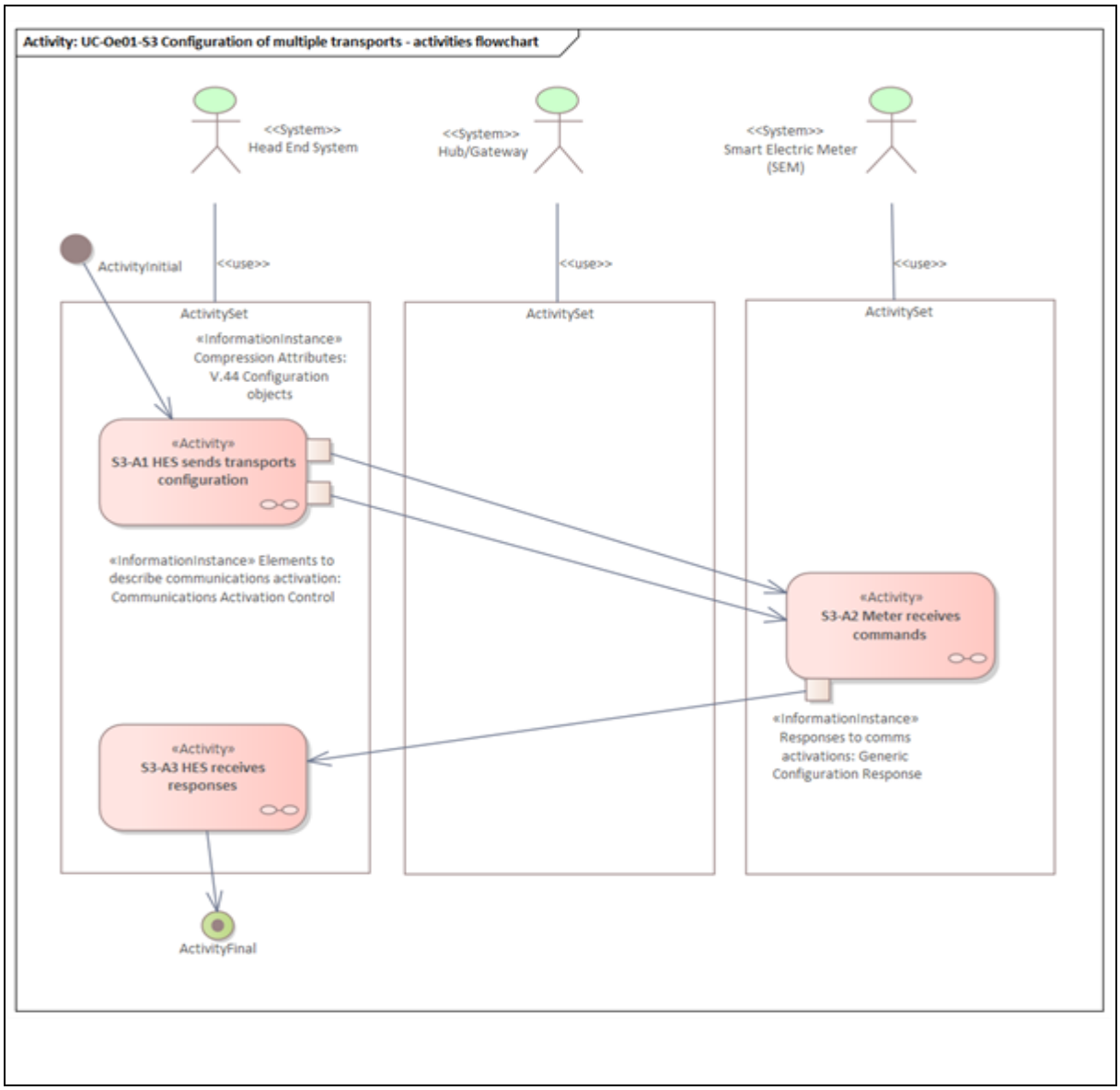
  The schedule is set and active for the activation time Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Responses to schedule commands	(generic response)

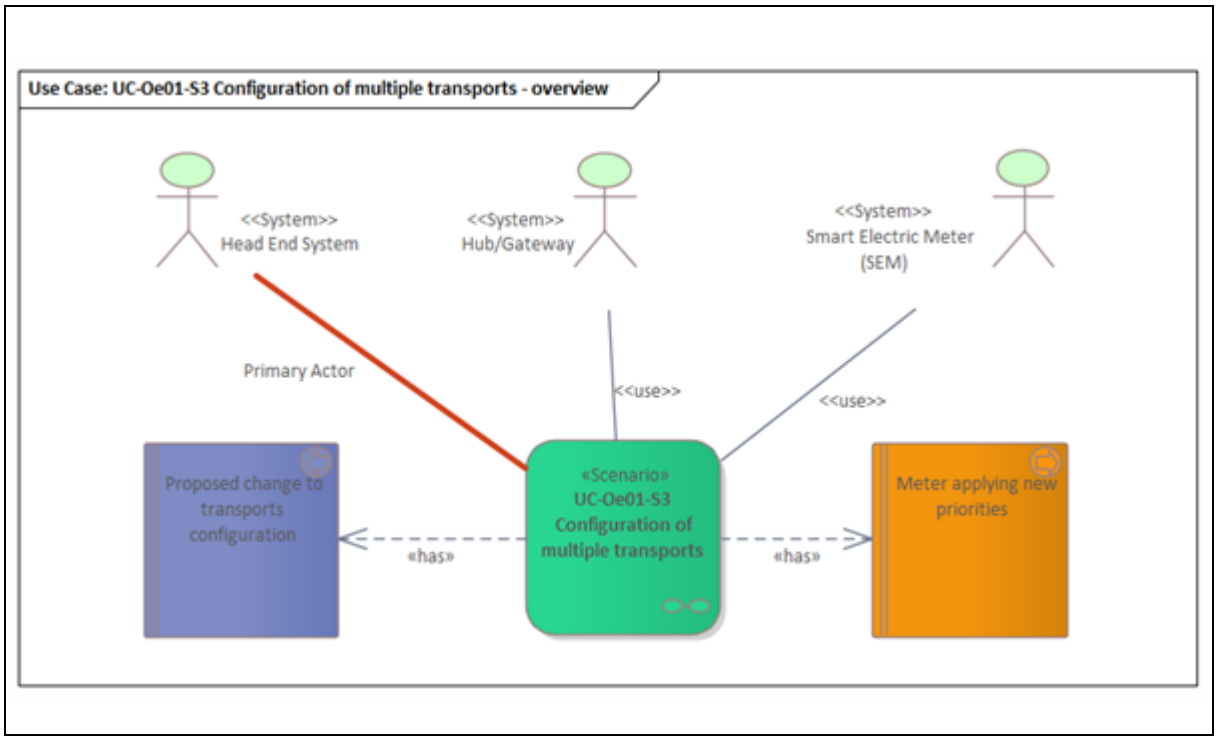
© Copyright 2026 Oesterreichs Energie. All rights reserved

6.23.5.2.3. UC-Oe01-S3 Configuration of multiple transports

This scenario allows the enablement and disablement of individual transport technologies, including the ability to disable all the wide area capability of the meter.



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	UC-Oe01-S3 Configuration of multiple transports							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
3.1		S3-A1 HES sends transports configuration	The HES sends the configuration to the Meter		Head End System	Smart Electric Meter (SEM)	Info6-V.44 Configuration objects, Info7-Communications Activation Control	
3.2		S3-A2 Meter receives commands	The meter receives, verifies and processes the configuration commands, The meter activates the new configuration (noting that changes to communications activation will take place after the current session is terminated. The meter sends responses to the		Smart Electric Meter (SEM)	Head End System	Info3-Generic Configuration Response	

© Copyright 2026 Oesterreichs Energie. All rights reserved

			configuration commands.					
3.3		S3-A3 HES receives responses	The HES receives responses to the configuration of the activations.		Head End System			

- 3.1. S3-A1 HES sends transports configuration

  Information Overview: UC-Oe01-S3 Configuration of multiple transports/S3-A1 HES sends transports configuration

  The HES sends the configuration to the Meter

  Information sent:

Information object	*Instance name*	*Instance description*
V.44 Configuration objects	Compression Attributes	(To Be determined)
Communications Activation Control	Elements to describe communications activation	This will indicate the communications type and its priority

- 3.2. S3-A2 Meter receives commands

  Information Overview: UC-Oe01-S3 Configuration of multiple transports/S3-A2 Meter receives commands

  The meter receives, verifies and processes the configuration commands, The meter activates the new configuration (noting that changes to communications activation will take place after the current session is terminated. The meter sends responses to the configuration commands.

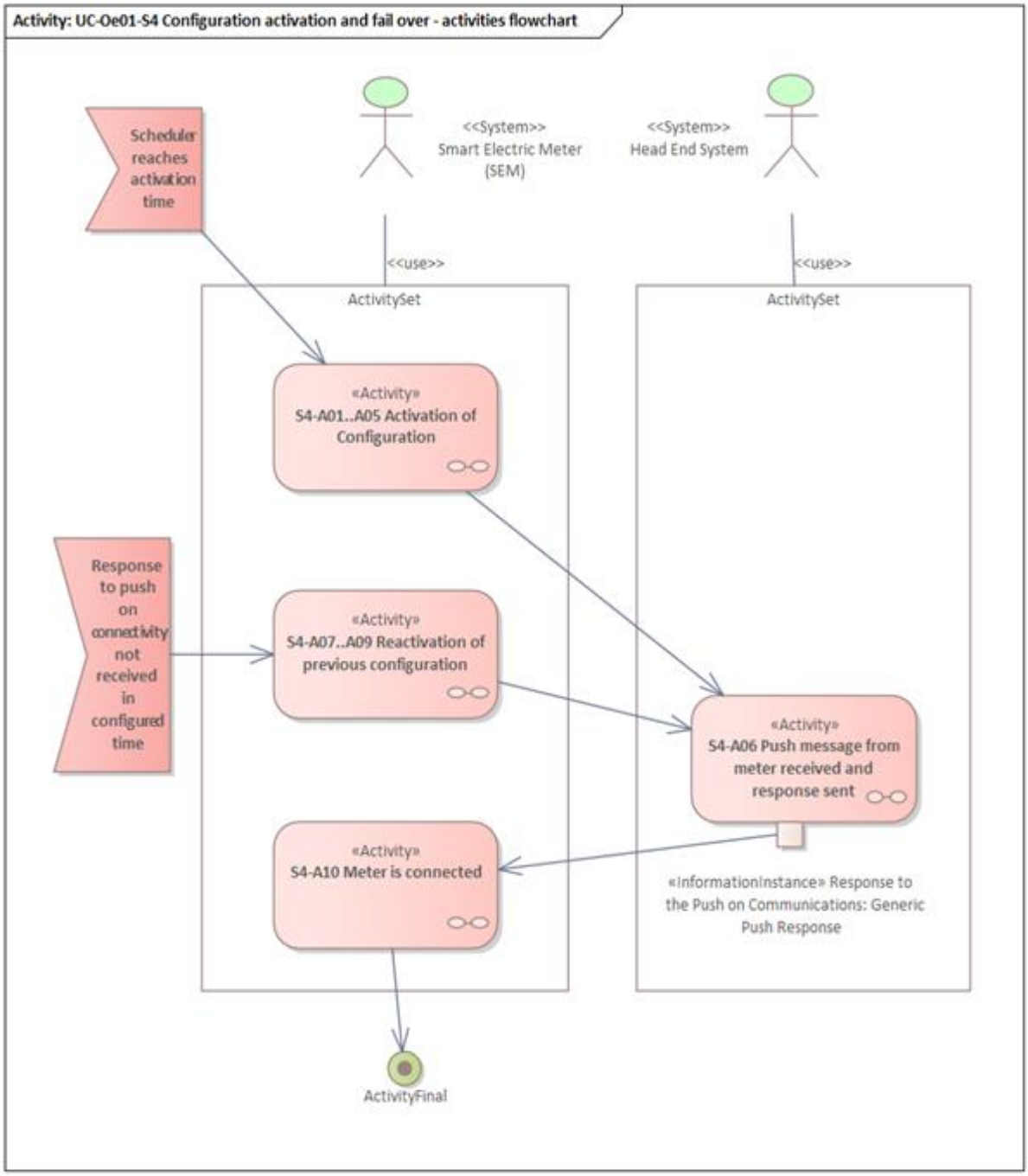
  Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Responses to comms activations	(generic response)

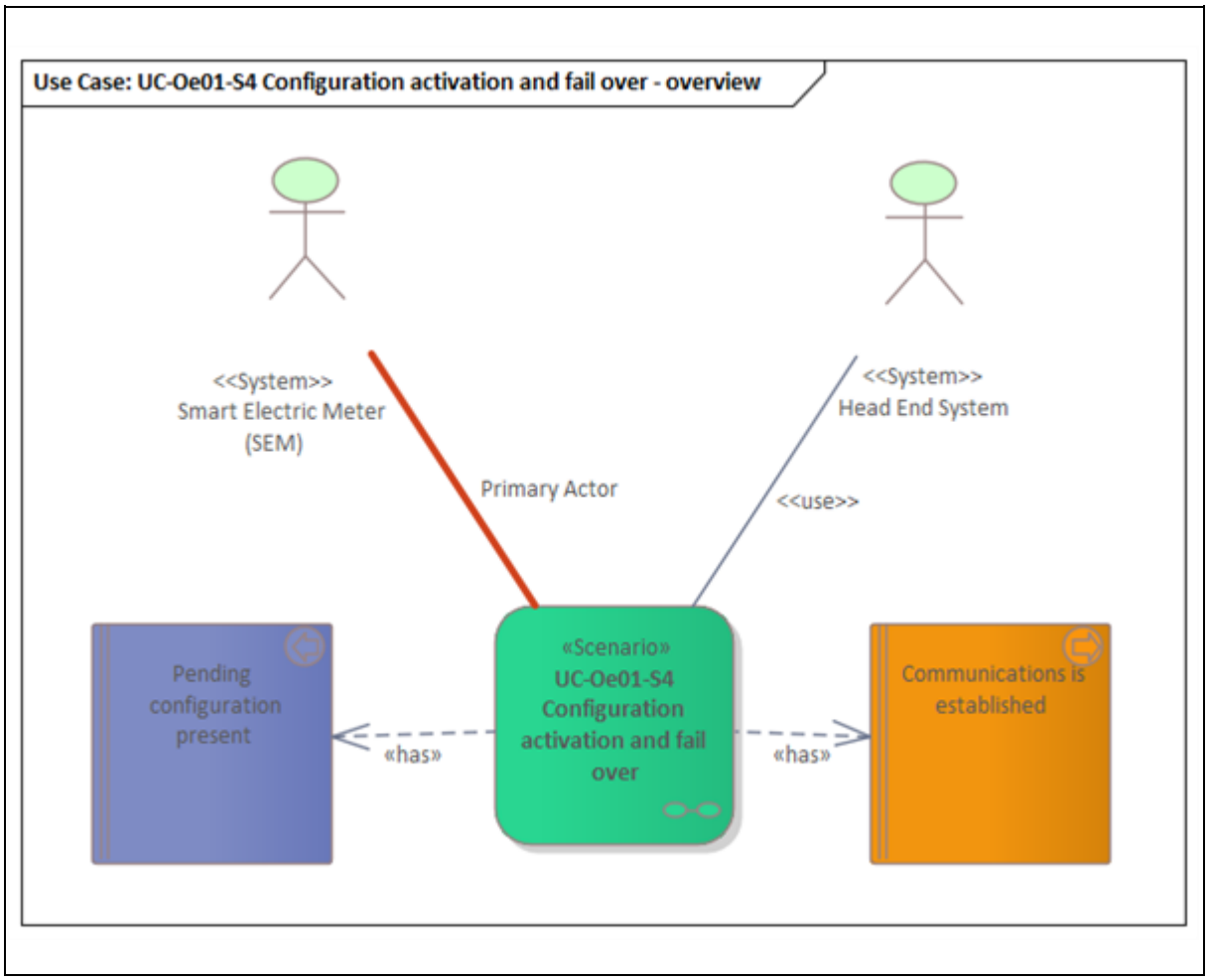
6.23.5.2.4. UC-Oe01-S4 Configuration activation and fail over

© Copyright 2026 Oesterreichs Energie. All rights reserved

The new communications configuration is activated by a schedule. If this communications implementation does not succeed then the meter returns to previous configuration settings.



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	UC-Oe01-S4 Configuration activation and fail over							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
4.1		S4-A01..A05 Activation of Configuration	A current configuration is backed up, and a preset configuration is applied and activated.		Smart Electric Meter (SEM)			
4.2		S4-A06 Push message from meter received and response sent	The HES receives the push message (push on connectivity) that is sent from the meter to announce its presence on the network, and sends		Head End System	Smart Electric Meter (SEM)	Info14-Generic Push Response	

© Copyright 2026 Oesterreichs Energie. All rights reserved

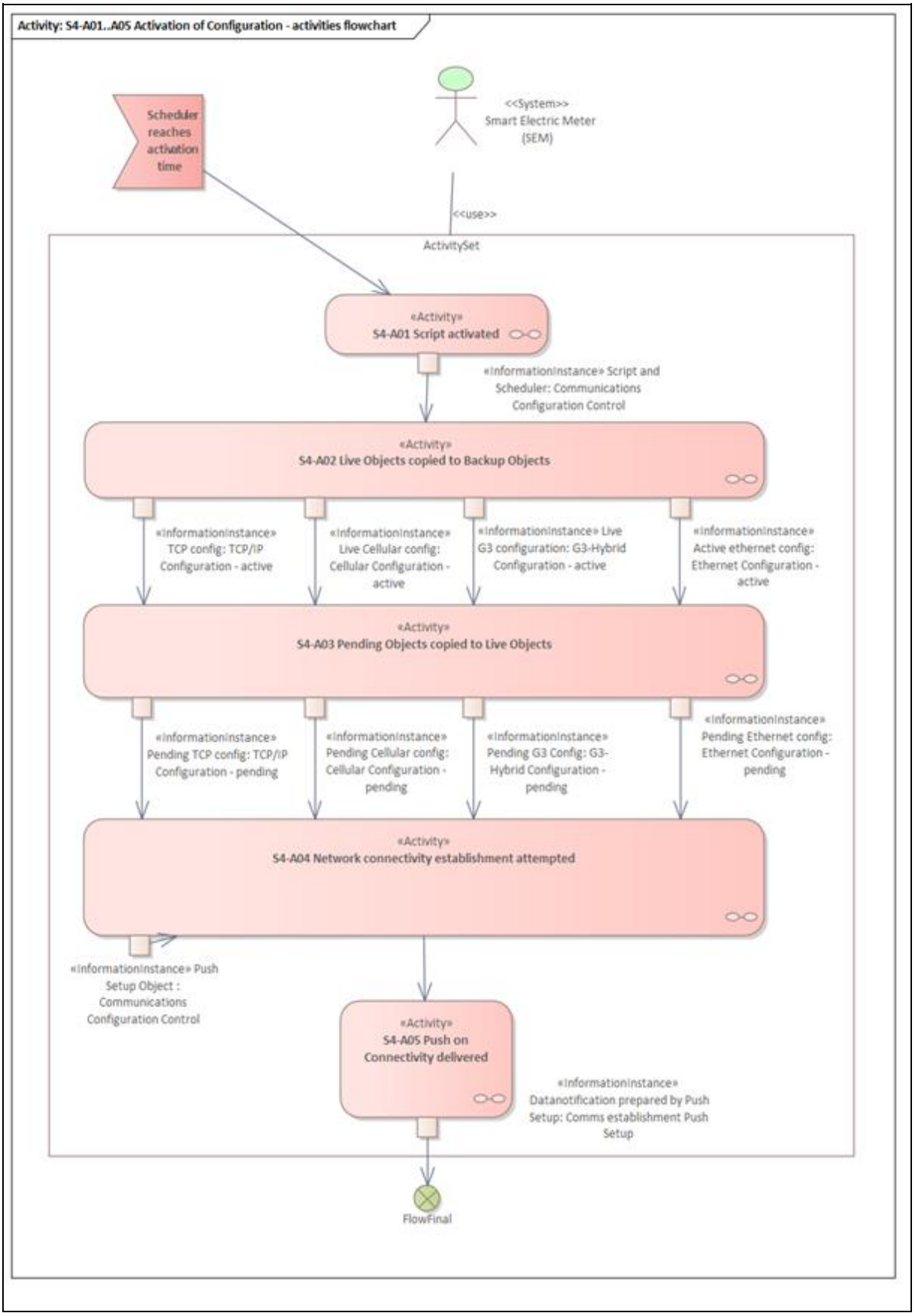
			a response to the meter.					
4.3		S4-A07..A09 Reactivation of previous configuration	If response to the push on connectivity is not received within a set time, then the meter assumes that there is an issue with the new configuration. Therefore it reads the backup configuration back into the current configuration, and initiates a new push on connectivity.		Smart Electric Meter (SEM)			
4.4		S4-A10 Meter is connected	The meter has received a response to a push on connection message. If necessary, the timer controlling roll back is cancelled.		Smart Electric Meter (SEM)			

- 4.1. S4-A01..A05 Activation of Configuration

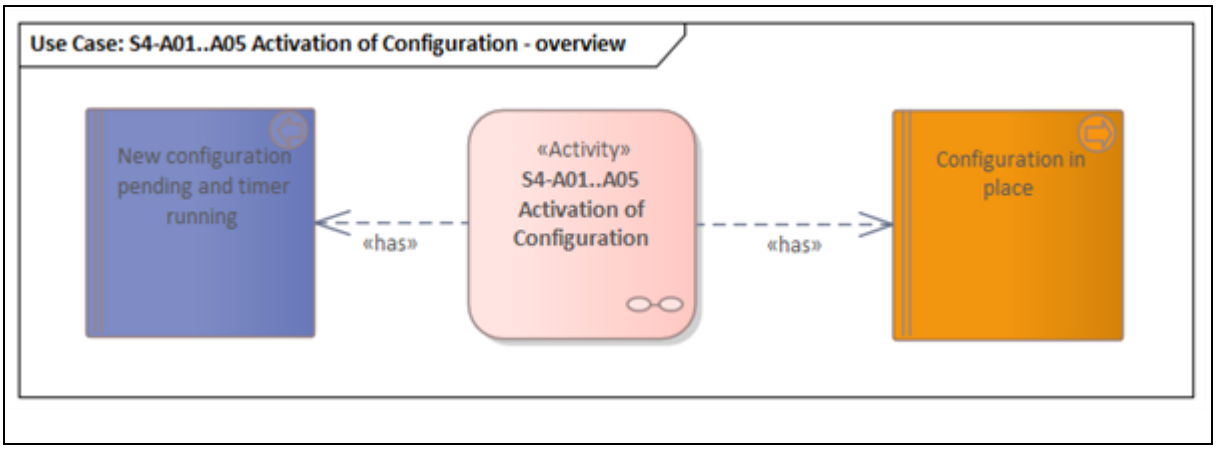
Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A01..A05 Activation of Configuration

A current configuration is backed up, and a preset configuration is applied and activated.

© Copyright 2026 Oesterreichs Energie. All rights reserved



© Copyright 2026 Oesterreichs Energie. All rights reserved



Activity step by step analysis

Scenario								
Scenario name	UC-Oe01-S4 Configuration activation and fail over							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
4.1.1		S4-A01 Script activated	The communications configuration activation script is activated.		Smart Electric Meter (SEM)	Smart Electric Meter (SEM)	Info4-Communications Configuration Control	
4.1.2		S4-A02 Live Objects copied to Backup Objects	The script copies the values in the current objects into the backup objects		Smart Electric Meter (SEM)	Smart Electric Meter (SEM)	Info8-Ethernet Configuration - active, Info9-Cellular Configuration - active, Info10-G3-Hybrid Configuration - active, Info11-TCP/IP Configuration - active	
4.1.3		S4-A03 Pending Objects copied to Live Objects	The pending objects are copied to the live objects, and this implements the change to the new configuration.		Smart Electric Meter (SEM)	Smart Electric Meter (SEM)	Info1-Cellular Configuration - pending, Info12-Ethernet Configuration - pending, Info5-G3-Hybrid Configuration - pending, Info2-TCP/IP	

© Copyright 2026 Oesterreichs Energie. All rights reserved

							Configuration - pending	
4.1.4		S4-A04 Network connectivity establishment attempted	The meter establishes low level communications based on the new configuration		Smart Electric Meter (SEM)	Smart Electric Meter (SEM)	Info4-Communications Configuration Control	
4.1.5		S4-A05 Push on Connectivity delivered	The meter sends the push on connectivity datanotification.		Smart Electric Meter (SEM)		Info13-Comms establishment Push Setup	

- 4.1.1. S4-A01 Script activated

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A01..A05 Activation of Configuration/S4-A01 Script activated

The communications configuration activation script is activated.

Information sent:

Information object	*Instance name*	*Instance description*
Communications Configuration Control	Script and Scheduler	The script applied to execute the copy activities below.

- 4.1.2. S4-A02 Live Objects copied to Backup Objects

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A01..A05 Activation of Configuration/S4-A02 Live Objects copied to Backup Objects

The script copies the values in the current objects into the backup objects

Information sent:

Information object	*Instance name*	*Instance description*
Ethernet Configuration - active	Active ethernet config	Ethernet objects
Cellular Configuration - active	Live Cellular config	(GSM objects)
G3-Hybrid Configuration - active	Live G3 configuration	G3-hybrid objects.
TCP/IP Configuration - active	TCP config	(internet protocol objects)

- 4.1.3. S4-A03 Pending Objects copied to Live Objects

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A01..A05 Activation of Configuration/S4-A03 Pending Objects copied to Live Objects

The pending objects are copied to the live objects, and this implements the change to the new configuration.

Information sent:

Information object	*Instance name*	*Instance description*
Cellular Configuration - pending	Pending Cellular config	Cellular objects
TCP/IP Configuration - pending	Pending Ethernet config	Ethernet objects
G3-Hybrid Configuration - pending	Pending G3 Config	G3-Hybrid objects
Ethernet Configuration - pending	Pending TCP config	Internet protocol objects

© Copyright 2026 Oesterreichs Energie. All rights reserved

- 4.1.4. S4-A04 Network connectivity establishment attempted

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A01..A05 Activation of Configuration/S4-A04 Network connectivity establishment attempted

The meter establishes low level communications based on the new configuration

Information sent:

Information object	*Instance name*	*Instance description*
Communications Configuration Control	Push Setup Object	Push on connection.

- 4.1.5. S4-A05 Push on Connectivity delivered

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A01..A05 Activation of Configuration/S4-A05 Push on Connectivity delivered

The meter sends the push on connectivity datanotification.

Information sent:

Information object	*Instance name*	*Instance description*
Comms establishment Push Setup	Datanotification prepared by Push Setup	The meter sends a push setup to identify itself on the communications network.

- 4.2. S4-A06 Push message from meter received and response sent

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A06 Push message from meter received and response sent

The HES receives the push message (push on connectivity) that is sent from the meter to announce its presence on the network, and sends a response to the meter.

Information sent:

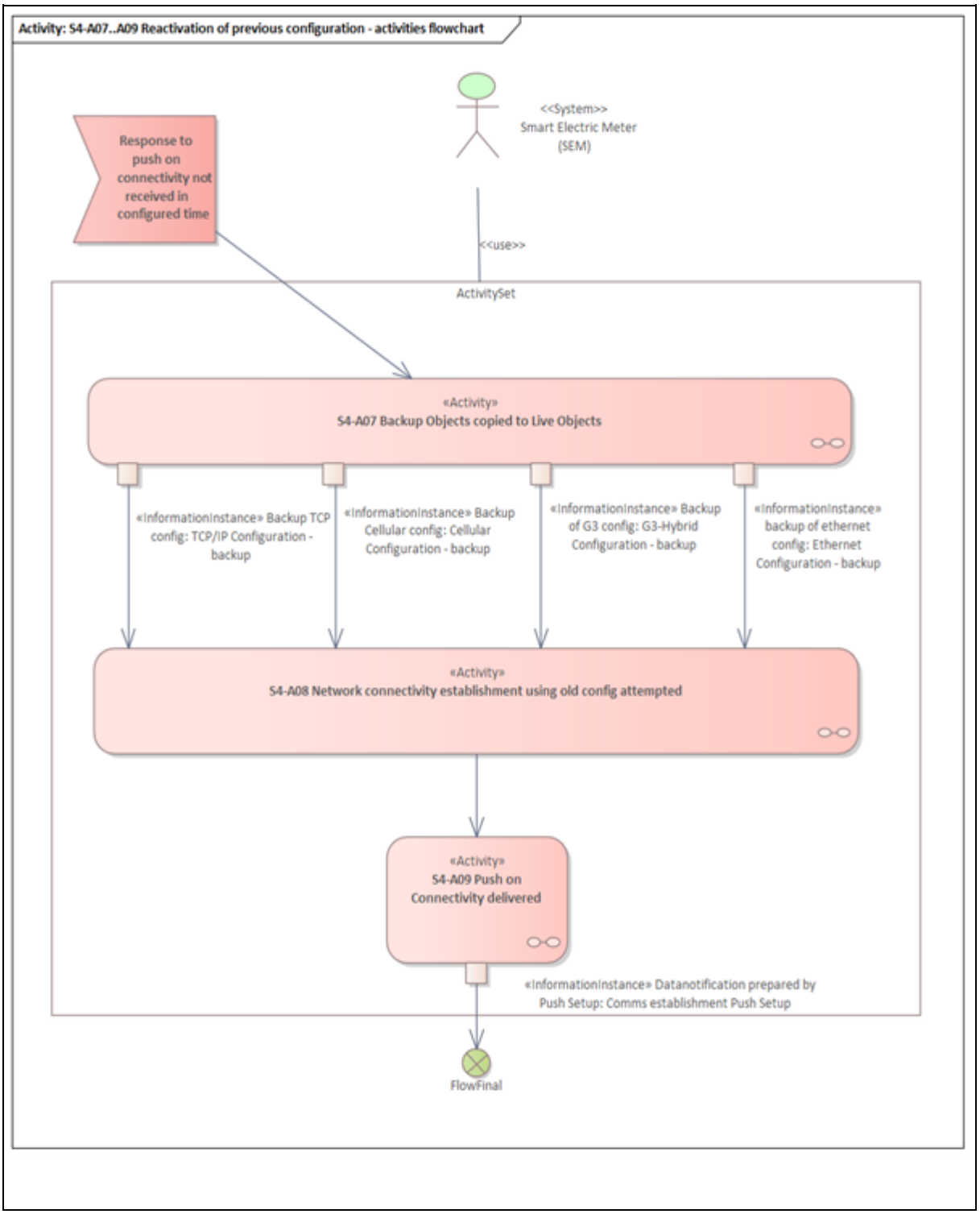
Information object	*Instance name*	*Instance description*
Generic Push Response	Response to the Push on Communications	This response is necessary to establish that the communications changes have been successful.

- 4.3. S4-A07..A09 Reactivation of previous configuration

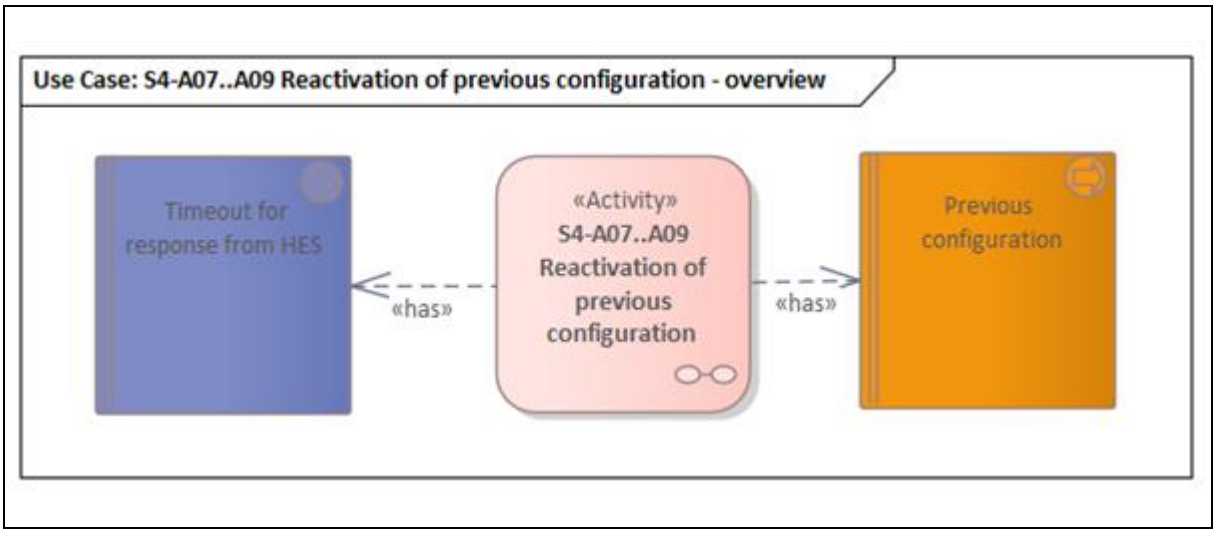
Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A07..A09 Reactivation of previous configuration

If response to the push on connectivity is not received within a set time, then the meter assumes that there is an issue with the new configuration. Therefore it reads the backup configuration back into the current configuration, and initiates a new push on connectivity.

© Copyright 2026 Oesterreichs Energie. All rights reserved



© Copyright 2026 Oesterreichs Energie. All rights reserved



Activity step by step analysis

Scenario								
Scenario name	UC-Oe01-S4 Configuration activation and fail over							
Step No	**Event**	**Name of process/activity**	**Description of process/activity**	**Service**	**Information producer (actor)**	**Information receiver (actor)**	**Information exchanged (IDs)**	**Requirement, R-IDs**
4.3.1		S4-A07 Backup Objects copied to Live Objects	The previous configuration elements which were stored in backup are loaded into the live configuration.		Smart Electric Meter (SEM)	Smart Electric Meter (SEM)	Info15-Cellular Configuration - backup, Info16-Ethernet Configuration - backup, Info17-G3-Hybrid Configuration - backup, Info18-TCP/IP Configuration - backup	
4.3.2		S4-A08 Network connectivity establishment using old config attempted	The meter attempts reconnection using the old settings		Smart Electric Meter (SEM)			
4.3.3		S4-A09 Push on Connectivity delivered	The meter sends a push on connectivity message.		Smart Electric Meter (SEM)	Head End System	Info13-Comms establishment Push Setup	

- 4.3.1. S4-A07 Backup Objects copied to Live Objects

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A07..A09 Reactivation of previous configuration/S4-A07 Backup Objects copied to Live Objects

The previous configuration elements which were stored in backup are loaded into the live configuration.

Information sent:

Information object	Instance name	Instance description

© Copyright 2026 Oesterreichs Energie. All rights reserved

Cellular Configuration - backup	Backup Cellular config	Cellular objects
Ethernet Configuration - backup	backup of ethernet config	Ethernet objects
G3-Hybrid Configuration - backup	Backup of G3 config	G3-Hybrid objects
TCP/IP Configuration - backup	Backup TCP config	Internet protocol objects

- 4.3.3. S4-A09 Push on Connectivity delivered

Information Overview: UC-Oe01-S4 Configuration activation and fail over/S4-A07..A09 Reactivation of previous configuration/S4-A09 Push on Connectivity delivered

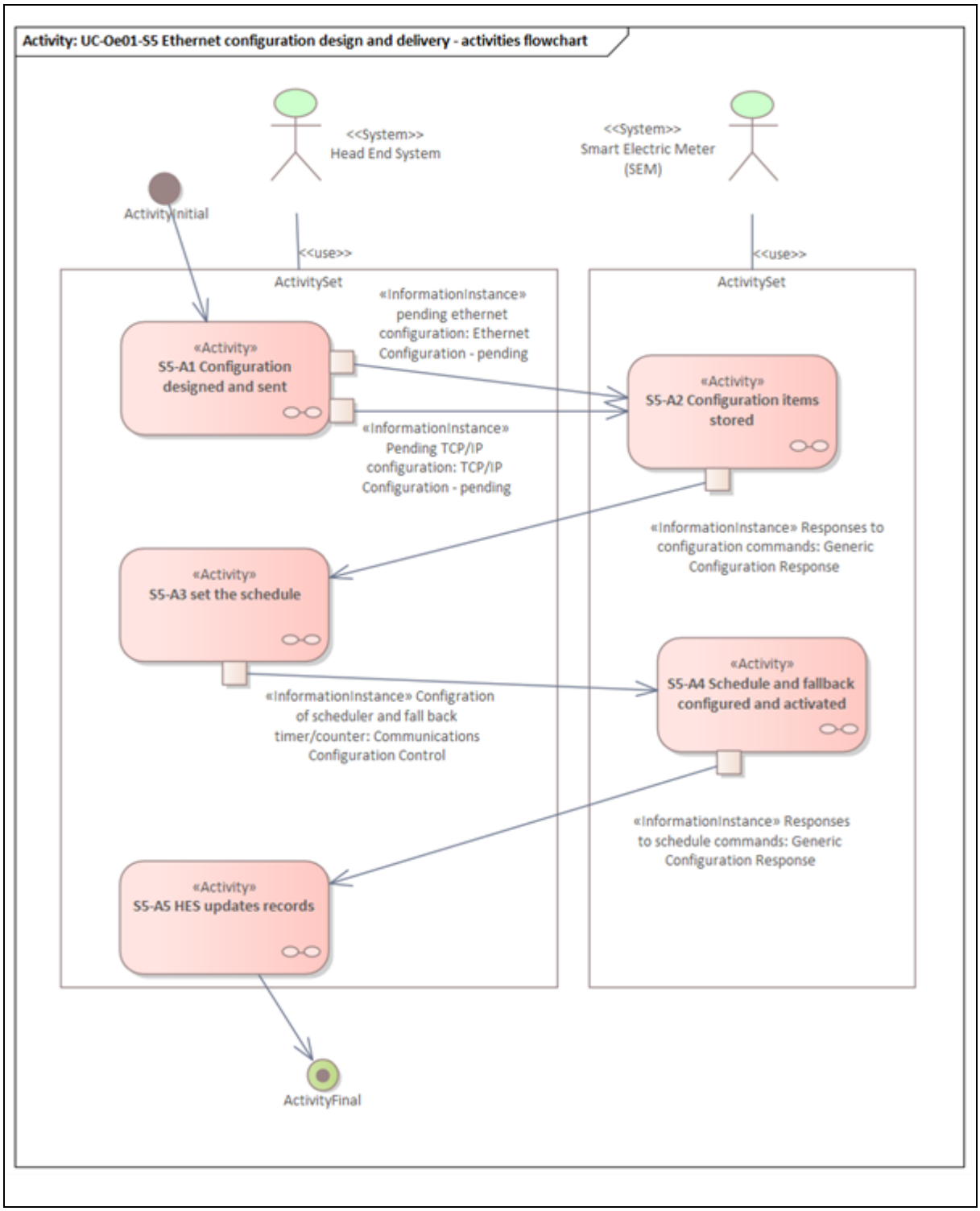
The meter sends a push on connectivity message. Information sent:

Information object	*Instance name*	*Instance description*
Comms establishment Push Setup	Datanotification prepared by Push Setup	The meter sends a push setup to identify itself on the communications network.

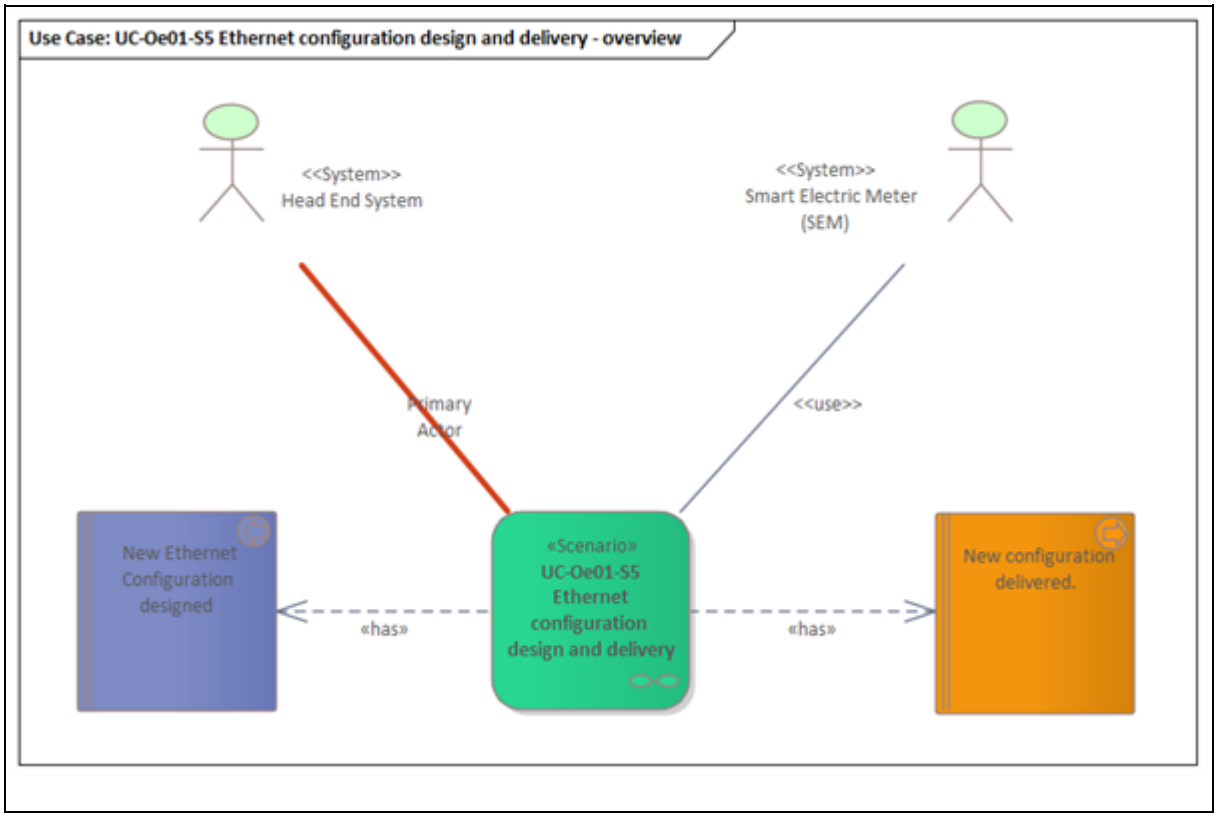
6.23.5.2.5. UC-Oe01-S5 Ethernet configuration design and delivery

The HES receives an ethernet configuration design to be delivered to the meter and delivers it.

© Copyright 2026 Oesterreichs Energie. All rights reserved



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	UC-Oe01-S5 Ethernet configuration design and delivery							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
5.1		S5-A1 Configuration designed and sent	The HES has a configuration planned and sends it to the meter.		Head End System	Smart Electric Meter (SEM)	Info12-Ethernet Configuration - pending, Info2-TCP/IP Configuration - pending	
5.2		S5-A2 Configuration items stored	The items are stored in the pending objects awaiting activation.		Smart Electric Meter (SEM)	Head End System	Info3-Generic Configuration Response	
5.3		S5-A3 set the schedule	The timer to initiate the comms change is activated.		Head End System	Smart Electric Meter (SEM)	Info4-Communications Configuration Control	
5.4		S5-A4 Schedule and fallback configured and activated	The timer for fallback is set.		Smart Electric Meter (SEM)	Head End System	Info3-Generic Configuration Response	

© Copyright 2026 Oesterreichs Energie. All rights reserved

5.5		S5-A5 HES updates records	The HES updates its records and informs other systems as appropriate		Head End System			

- 5.1. S5-A1 Configuration designed and sent

Information Overview: UC-Oe01-S5 Ethernet configuration design and delivery/S5-A1 Configuration designed and sent

The HES has a configuration planned and sends it to the meter.

Information sent:

Information object	*Instance name*	*Instance description*
TCP/IP Configuration - pending	pending ethernet configuration	configuration items related to ethernet communications, may include VPN network choices, etc.
Ethernet Configuration - pending	Pending TCP/IP configuration	Items related to the configuration of IP communications

- 5.2. S5-A2 Configuration items stored

Information Overview: UC-Oe01-S5 Ethernet configuration design and delivery/S5-A2 Configuration items stored

The items are stored in the pending objects awaiting activation.

Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Responses to configuration commands	The meter sends response(s) as appropriate.

- 5.3. S5-A3 set the schedule

Information Overview: UC-Oe01-S5 Ethernet configuration design and delivery/S5-A3 set the schedule

The timer to initiate the comms change is activated.

Information sent:

Information object	*Instance name*	*Instance description*
Communications Configuration Control	Configration of scheduler and fall back timer/counter	These attributes are the time for activation, and also a timeout after which the meter returns to previous settings.

- 5.4. S5-A4 Schedule and fallback configured and activated

Information Overview: UC-Oe01-S5 Ethernet configuration design and delivery/S5-A4 Schedule and fallback configured and activated

The timer for fallback is set.

Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Responses to schedule commands	(generic response)

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.23.6. Information exchanged

Information exchanged			
Information exchanged, ID	***Name of information***	***Description of information exchanged***	***Requirement, R-IDs***
Info1	Cellular Configuration pending	From ACE SM GCP - all are pending GPRS modem setup, IC=45, 0-0:25.4.0.0 Modem configuration, IC=27, 0-0:2.0.0.0 Auto answer, IC=28, 0-0:2.2.0.0 GSM Diagnostic, IC=47, 0-0:25.6.0.0 CHAP Password IC=1, 0-0:94.43.0.0 Telecom CAT-M switch threshold - pending IC=1, 0-0:96.61.3.0 Telecom CATM-NBIOT switch threshold - pending IC=1, 0-0:96.61.4.0 Module system configuration - pending IC=1, 0-0:94.43.8.0	
Info2	TCP/IP Configuration pending	Pending objects. TCP-UDP setup, IC=41, 0-0:25.0.0.0 IPv4 setup, IC=42, 0-0:25.1.0.0 IPv6 setup, IC=48, 0-0:25.7.0.0 PPP setup, IC=44, 0-0:25.3.0.0	
Info3	Generic Configuration Response	This will be one or more responses to SET or ACTION commands used to deliver a full or partial configuration of the Meter. OBIS codes are dependent on the Commands.	
Info4	Communications Configuration Control	This contains the elements to control the changes of configuration. Script table - Activation of communications configuration elements Schedule - Activation of communications configuration elements Push Setup - On connectivity, IC=40, 0-0:25.9.0.255	
Info5	G3-Hybrid Configuration pending	Objects applied in ACE SM GCP - all are pending G3-PLC MAC layer counters, IC=90, 0-0:29.0.0.0 G3-PLC MAC setup, IC=91, 0-0:29.1.0.0	

© Copyright 2026 Oesterreichs Energie. All rights reserved

		G3-PLC MAC 6LoWPAN adaption layer setup IC=92, 0-0:29.2.0.0 G3-PCL MAC Hybrid RF layer counters IC=160, 0-0:29.3.0.0 G3-PLC MAC Hybrid RF MAC setup IC = 161, 0-0:29.4.0.0 G3-PLC Hybrid 6LoWPAN adaption layer setup IC = 162, 0-0:29.5.0.0	
Info6	V.44 Configuration objects	Austria-specific Objects ToDo - define parameters and OBIS codes.	
Info7	Communications Activation Control	This sets priorities for different communication types, and permits wide area communications to be completely enabled or disabled. Objects are TBC.	
Info8	Ethernet Configuration active	- Ethernet configuration - current IC = 1, 0-0:94.43.140.255 Ethernet filter - current IC = 1, 0-0:94.43.141.255 Ethernet status IC = 1, 0-0:94.43.142.255	
Info9	Cellular Configuration active	- From ACE SM GCP - all are active GPRS modem setup, IC=45, 0-0:25.4.0.255 Modem configuration, IC=27, 0-0:2.0.0.255 Auto answer, IC=28, 0-0:2.2.0.255 GSM Diagnostic, IC=47, 0-0:25.6.0.255 CHAP Password IC=1, 0-0:94.43.0.255 Telecom CAT-M switch threshold IC=1, 0-0:96.61.3.255 Telecom CATM-NBIOT switch threshold IC=1, 0-0:96.61.4.255 Module system configuration IC=1, 0-0:94.43.8.255	
Info10	G3-Hybrid Configuration active	- Objects applied in ACE SM GCP. G3-PLC MAC layer counters, IC=90, 0-0:29.0.0.255 G3-PLC MAC setup, IC=91, 0-0:29.1.0.255 G3-PLC MAC 6LoWPAN adaption layer setup IC=92, 0-0:29.2.0.255 G3-PCL MAC Hybrid RF layer counters	

© Copyright 2026 Oesterreichs Energie. All rights reserved

		IC=160, 0-0:29.3.0.255 G3-PLC MAC Hybrid RF MAC setup IC = 161, 0-0:29.4.0.255 G3-PLC Hybrid 6LoWPAN adaption layer setup IC = 162, 0-0:29.5.0.255 Additional Objects TBC	
Info11	TCP/IP Configuration - active	TCP-UDP setup, IC=41, 0-0:25.0.0.255 IPv4 setup, IC=42, 0-0:25.1.0.255 IPv6 setup, IC=48, 0-0:25.7.0.255 PPP setup, IC=44, 0-0:25.3.0.255	
Info12	Ethernet Configuration - pending	Ethernet configuration - pending IC = 1, 0-0:94.43.140.0 Ethernet filter - pending IC = 1, 0-0:94.43.141.0 Ethernet status IC = 1, 0-0:94.43.142.0	
Info13	Comms establishment Push Setup	Push setup - On connectivity. IC = 40, 0-0:25.9.0.255	
Info14	Generic Push Response	This may depend on the lower layers employed. It may be an Application layer response from the cosem Client, or it may be a lower layer acknowledgement of datagram delivery.	
Info15	Cellular Configuration - backup	From ACE SM GCP - all are backup GPRS modem setup, IC=45, 0-0:25.4.0.254 Modem configuration, IC=27, 0-0:2.0.0.254 Auto answer, IC=28, 0-0:2.2.0.254 GSM Diagnostic, IC=47, 0-0:25.6.0.254 CHAP Password IC=1, 0-0:94.43.0.254 Telecom CAT-M switch threshold IC=1, 0-0:96.61.3.254 Telecom CATM-NBIOT switch threshold IC=1, 0-0:96.61.4.254 Module system configuration IC=1, 0-0:94.43.8.254	
Info16	Ethernet Configuration - backup	Ethernet configuration - backup IC = 1, 0-0:94.43.140.255 Ethernet filter - backup IC = 1, 0-0:94.43.141.255	

© Copyright 2026 Oesterreichs Energie. All rights reserved

		Ethernet status IC = 1, 0-0:94.43.142.255	
Info17	G3-Hybrid Configuration backup	Objects applied in ACE SM GCP - all are backup G3-PLC MAC layer counters, IC=90, 0-0:29.0.0.254 G3-PLC MAC setup, IC=91, 0-0:29.1.0.254 G3-PLC MAC 6LoWPAN adaption layer setup IC=92, 0-0:29.2.0.254 G3-PCL MAC Hybrid RF layer counters IC=160, 0-0:29.3.0.254 G3-PLC MAC Hybrid RF MAC setup IC = 161, 0-0:29.4.0.254 G3-PLC Hybrid 6LoWPAN adaption layer setup IC = 162, 0-0:29.5.0.254 Additional Objects TBC	
Info18	TCP/IP Configuration backup	backup objects. TCP-UDP setup, IC=41, 0-0:25.0.0.254 IPv4 setup, IC=42, 0-0:25.1.0.254 IPv6 setup, IC=48, 0-0:25.7.0.254 PPP setup, IC=44, 0-0:25.3.0.254	

6.23.7. Common terms and definitions

Common terms and definitions	
Term	***Definition***
Auto_answer	IC = 28. Version 0 of the Auto answer class models how the device handles incoming calls to request the connection of the modem. In version 2, new capabilities are added to manage wake-up requests that may be in the form of a wake-up call or a wake-up message e.g. an (empty) SMS message. After a successful wake-up request, the device connects to the network.
G3_PLC_Classes	These are: G3-PLC MAC layer counters, IC=90, G3-PLC MAC setup, IC=91, G3-PLC MAC 6LoWPAN adaption layer setup IC=92, G3-PCL MAC Hybrid RF layer counters IC=160, G3-PLC MAC Hybrid RF MAC setup IC = 161, G3-PLC Hybrid 6LoWPAN adaption layer setup IC = 162,
GSM_Diagnostic	IC = 47. The cellular network is undergoing constant changes in terms of registration status, signal quality, etc. It is necessary to monitor and log the relevant parameters in order to obtain

© Copyright 2026 Oesterreichs Energie. All rights reserved

	diagnostic information that allows identifying communication problems in the network. An instance of the “GSM diagnostic” class stores parameters of the GSM/GPRS, UMTS, CDMA or LTE network necessary for analysing the operation of the network. A GSM diagnostic “Profile generic” object is also available to capture the attributes of the GSM diagnostic object, see DLMS UA 1000-1 Ed 17 Part 1:2025, 6.5.
IPv4_setup	IC = 42. This IC allows modelling the setup of the IPv4 layer, handling all information related to the IP Address settings associated to a given device and to a lower layer connection on which these settings are used. There shall be an instance of this IC in a device for each different network interface implemented. For example, if a device has two interfaces (using the TCP-UDP/IPv4 profile on both of them), there shall be two instances of the IPv4 setup IC in that device: one for each of these interfaces.
IPv6_setup	IC = 48. The IPv6 setup IC allows modelling the setup of the IPv6 layer, handling all information related to the IPv6 address settings associated to a given device and to a lower layer connection on which these settings are used.
Modem_configuration	IC = 27. This IC allows modelling the configuration and initialisation of modems used for data transfer from/to a device. Several modems can be configured.
PPP_setup	IC = 44. This IC allows modelling the setup of interfaces using the PPP protocol, by handling all information related to PPP settings associated to a given physical device and to a lower layer connection on which these settings are used. There shall be an instance of this IC for each network interface of a physical device.
TCP-UDP_setup	IC = 41. Instances of the IC TCP-UDP setup allow modelling the setup of the TCP or UDP sub-layer of the COSEM TCP or UDP based transport layer of a TCP-UDP/IP based communication profile or the UDP sub-layer of the DLMS/COSEM CoAP transport layer of a DLMS/COSEM CoAP based communication profile.
P2P	Point to point. Note that this usually references cellular- based public network radio systems (GSM).
PLC	Power Line Carrier. Note that this is a generic term, and covers G3-PLC and G3-Hybrid (which applies power line carrier and radio technologies).

© Copyright 2026 Oesterreichs Energie. All rights reserved

Hub/Gateway	This is a neighbourhood network device, and may be a basic Gateway or a Dualmode-Gateway.
Dualmode-Gateway	A gateway with advanced features, for example meter reading or firmware image distribution.

6.24. Use Case Oe-02 – Calibration and maintenance

6.24.1. Description of the use case

6.24.1.1. Name of use case

Use case identification		
ID	***Area(s)/Domain(s)/Zone(s)***	***Name of use case***
	Austria	Oe-UC-02 Calibration & maintenance

6.24.1.2. Scope and objectives of use case

Scope and objectives of use case	
Scope	This covers the situation where the meter requires testing in the laboratory.
Objective(s)	Verification completed: The state of the meter's calibration is known.
Related business case(s)	

6.24.1.3. Narrative of Use Case

Narrative of use case
Short description
Placement of the meter into a test/calibration mode, recording of energy used during the test phase, and returning the meter to normal operation.
Complete description
The meter is to be capable of a change of operation to support calibration using the optical port. In this mode, the meter will: 1) indicate on the display that it is in a test/calibration mode 2) be capable of permitting a LED to change its function to deliver an alternate pulse rate and indicate an alternative parameter (e.g. a second LED selected to pulse for A- at 1 pulse per Wh), and also change the duration of LED illumination per pulse. 3) be capable of indicating consumption at a higher resolution than normal 4) stay in calibration mode during a power outage 5) automatically exit the calibration mode after 24 hours or at a predetermined future time. <u>Summary of use case</u> • **<u>Oe02-S1 Calibration mode start</u>** <u>Description</u>: The Meter enters the Calibration Mode. • **<u>Oe02-S2 Calibration mode operations</u>** <u>Description</u>: The meter's calibration is tested. The LED configuration will be changed during this phase to facilitate the tests being undertaken. Records are collected by the meter during the calibration mode

© Copyright 2026 Oesterreichs Energie. All rights reserved

- **Oe02-S3 End of calibration mode**
  Description: The meter ends calibration mode either as a result of an instruction from the Test Engineer or as a result of the timer.

6.24.1.4. Key performance indicators (KPI)

Key performance indicators			
ID	***Name***	***Description***	***Reference to mentioned use case objectives***
1	Verification completion	XX% of verifications are completed within the allotted time.	Verification completed

6.24.1.5. Use case conditions

Use case conditions	
Assumptions	
Prerequisites	
1	Requirement to validate calibration: The Test Engineer has a work instruction to verify the calibration of the meter.

6.24.1.6. Further information to the use case for classification/mapping

Classification information
Relation to other use cases
<<BUC>> Extensions
Level of depth
Some object modelling
Prioritisation
Mandatory
Generic, regional or national relation
Austria. This UC has been drafted to meet the national legislation of Austria, but may be applied in other countries.
Nature of the use case
SUC
Further keywords for classification

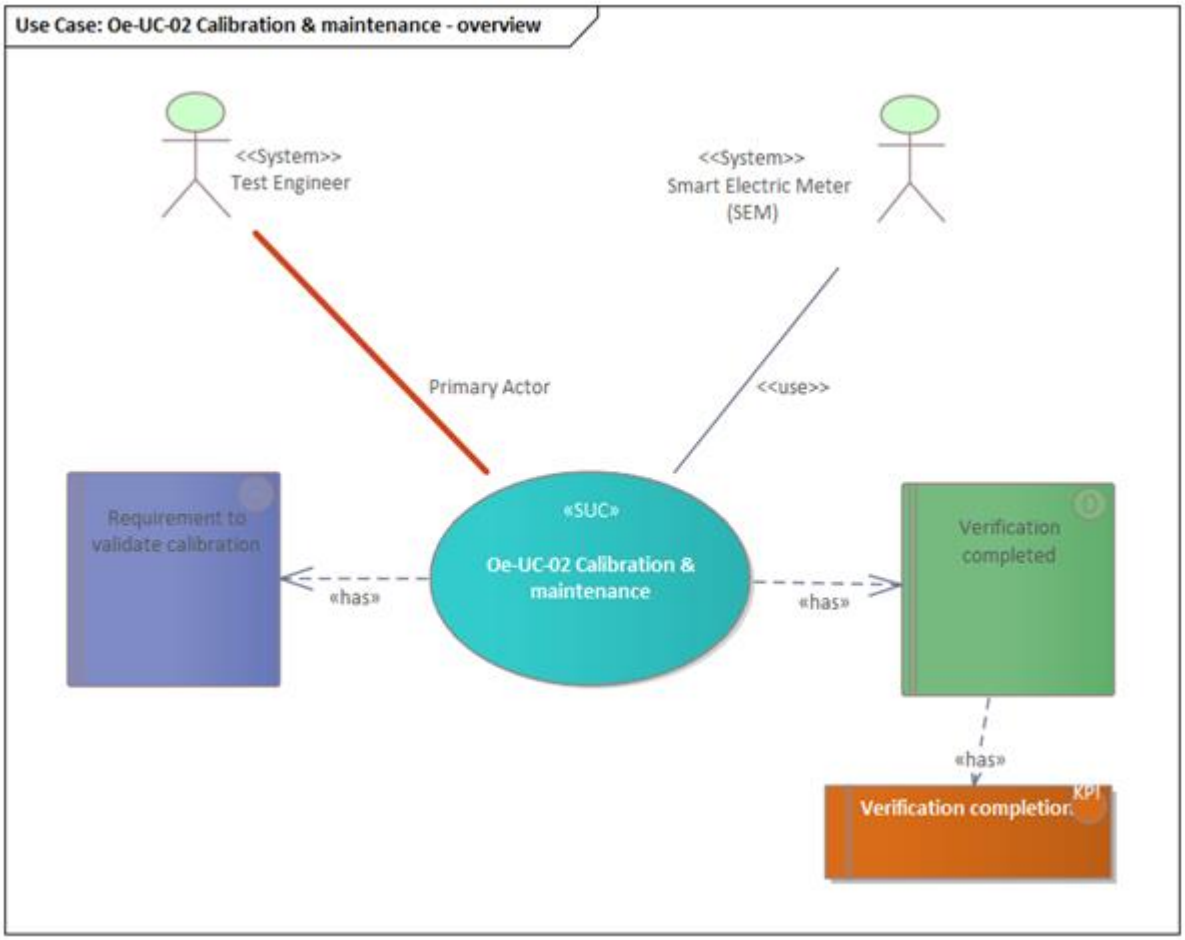
6.24.1.7. General remarks

General remarks
LED Operations: In normal operation, a LED will indicate active energy at a rate that is printed on the meter (for example, 800 pulses per kWh, 1 pulse per Wh). This rate and function is configurable for the LED, and the display may be able to show the current setting. This functionality must be listed in the BEV Calibration Certificate.

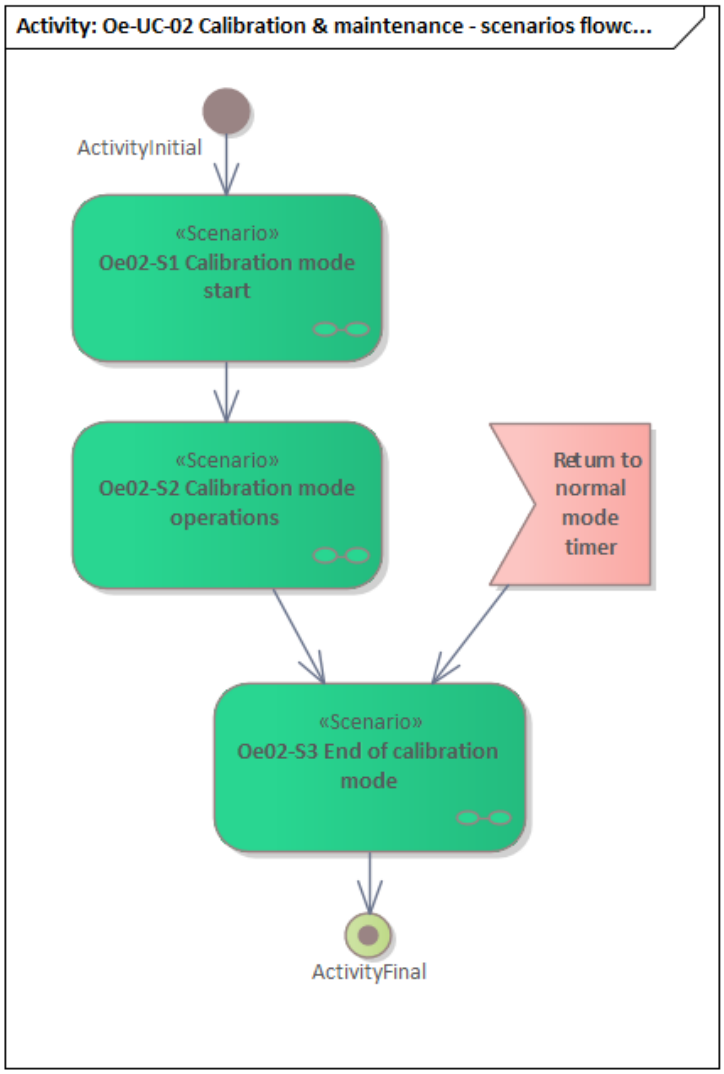
© Copyright 2026 Oesterreichs Energie. All rights reserved

6.24.2. Diagrams of use case

Diagram(s) of use case



© Copyright 2026 Oesterreichs Energie. All rights reserved



6.24.3. Technical details

6.24.3.1. Actors

Actors			
Grouping (e.g. domains, zones)		***Group description***	
Actor name	***Actor type***	***Actor description***	***Further information specific to this use case***
Smart Electric Meter (SEM)	System	Smart Meter is an AC Electricity Meter with additional functions.	The meter is the instrument under test
Test Engineer	System	An operator who works in a calibration laboratory setting to verify the accuracy (and possibly other features) of meters, both as initial acceptance from the manufacturer and during the lifetime of the meter.	

© Copyright 2026 Oesterreichs Energie. All rights reserved

6.24.3.2. References

References						
No.	***Reference Type***	***Reference***	***Status***	***Impact on use case***	***Originator / organisation***	***Link***
1	Type Approval	BEV Calibration Certificate	Per meter type	Controls what may be adjusted temporarily to improve speed of testing.	BEV	

6.24.4. Step by step analysis of use case

6.24.4.1. Overview of scenarios

Scenario conditions						
No.	***Scenario name***	***Scenario description***	***Primary actor***	***Triggering event***	***Pre-condition***	***Post-condition***
1	Oe02-S1 Calibration mode start	The Meter enters the Calibration Mode.	Test Engineer		Test Engineer equipped for task: The test engineer has the tools required. Security credentials: The test engineer has access to the security credentials	Calibration mode: The meter is functioning in calibration mode.
2	Oe02-S2 Calibration mode operations	The meter's calibration is tested. The LED configuration will be changed during this phase to facilitate the tests being undertaken. Records are collected by the meter during the calibration mode	Smart Electric Meter (SEM)		Oe02 S1 Completed correctly: The meter entered calibration mode correctly	Registers record correctly: The register (s) activated for calibration mode increment according to the consumption taking place.
3	Oe02-S3 End of calibration mode	The meter ends calibration mode either as a result of an instruction from the Test Engineer or as a	Test Engineer	Return to normal mode timer	Meter in calibration mode: The meter is operating in the calibration	Meter in normal operation: register (s) captured as required. display setting &

© Copyright 2026 Oesterreichs Energie. All rights reserved

		result of the timer.			mode, with non-standard displays.	LED configuration returned to normal calibration mode end event recorded.

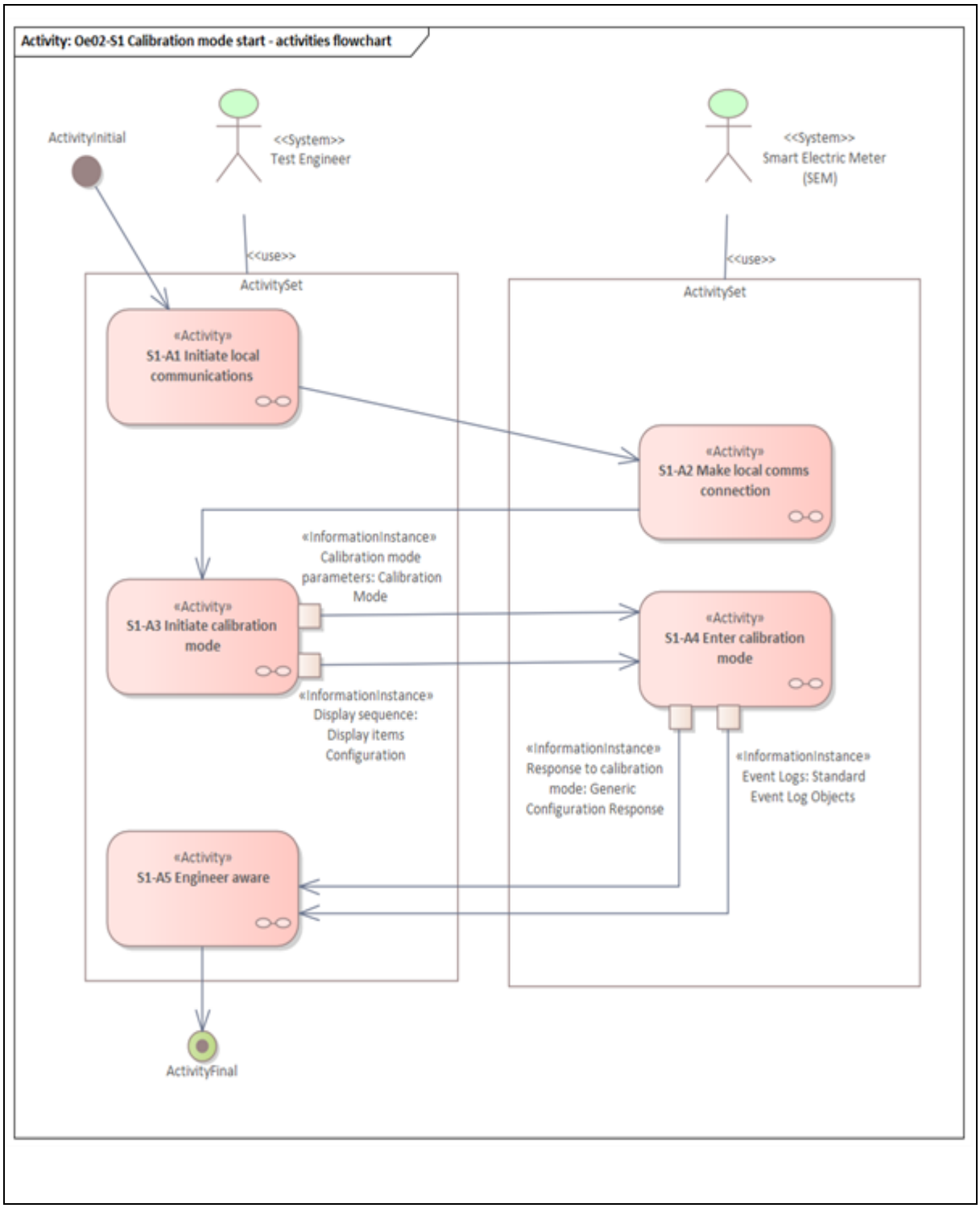
6.24.4.2. Steps - Scenarios

6.24.4.2.1. Oe02-S1 Calibration mode start

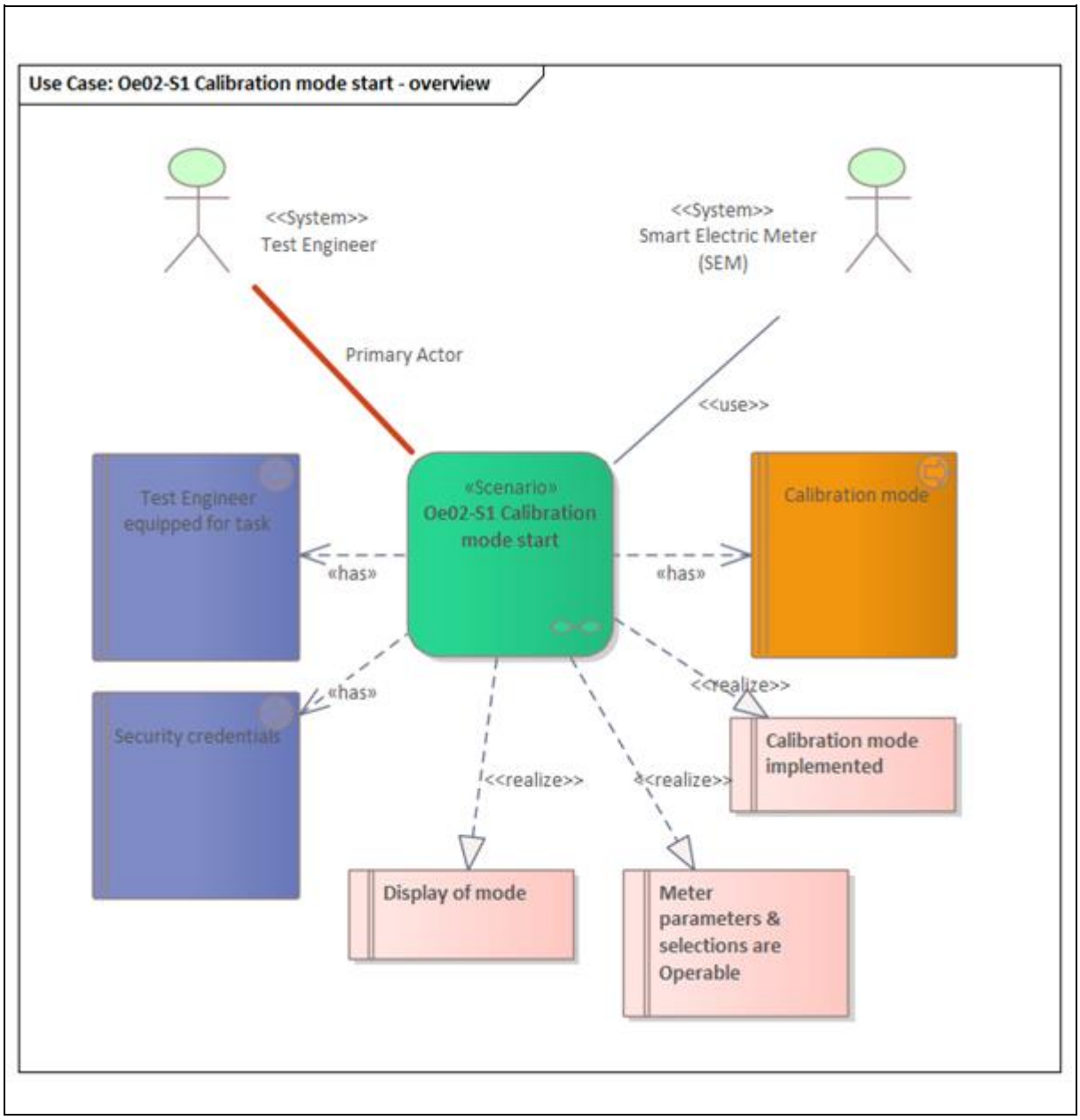
The Meter enters the Calibration Mode.

Requirement list (refer to "Requirement" section for more information)	
Requirement R-ID	***Requirement name***
Req1	Calibration mode implemented
Req2	Meter parameters & selections are Operable
Req3	Display of mode

© Copyright 2026 Oesterreichs Energie. All rights reserved



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	Oe02-S1 Calibration mode start							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
1.1		S1-A1 Initiate local communications	Create an HDLC connection, Establish the AA		Test Engineer			
1.2		S1-A2 Make local comms connection	Establish the AA Record the local communications Event(s)		Smart Electric Meter (SEM)			

© Copyright 2026 Oesterreichs Energie. All rights reserved

			(ToDo - References to UC19 Information instances)					
1.3		S1-A3 Initiate calibration mode	Set Calibration Mode to ON. Record Calibration Mode Start event Set required display parameters (See UC 18) Configure LED parameters Set test exit time		Test Engineer	Smart Electric Meter (SEM)	Info1-Calibration Mode, Info2-Display items Configuration	
1.4		S1-A4 Enter calibration mode	The meter performs the sequence of instructions and enters calibration mode		Smart Electric Meter (SEM)	Test Engineer	Info3-Standard Event Log Objects, Info4-Generic Configuration Response	
1.5		S1-A5 Engineer aware	The engineer is aware that the meter is in calibration mode		Test Engineer			

- 1.3. S1-A3 Initiate calibration mode

Information Overview: Oe02-S1 Calibration mode start/S1-A3 Initiate calibration mode

Set Calibration Mode to ON. Record Calibration Mode Start event Set required display parameters (See UC 18) Configure LED parameters Set test exit time

Information sent:

Information object	*Instance name*	*Instance description*
Calibration Mode	Calibration mode parameters	See detailed list
Display items Configuration	Display sequence	Temporary display sequence values

- 1.4. S1-A4 Enter calibration mode

Information Overview: Oe02-S1 Calibration mode start/S1-A4 Enter calibration mode

The meter performs the sequence of instructions and enters calibration mode

Information sent:

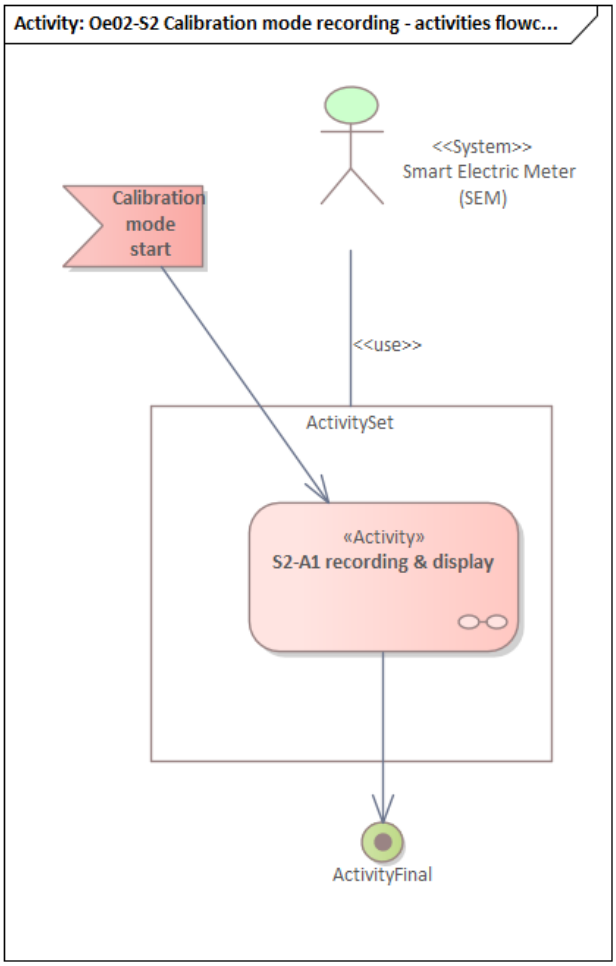
Information object	*Instance name*	*Instance description*
Standard Event Log Objects	Event Logs	
Generic Configuration Response	Response to calibration mode	

6.24.4.2.2. Oe02-S2 Calibration mode operations

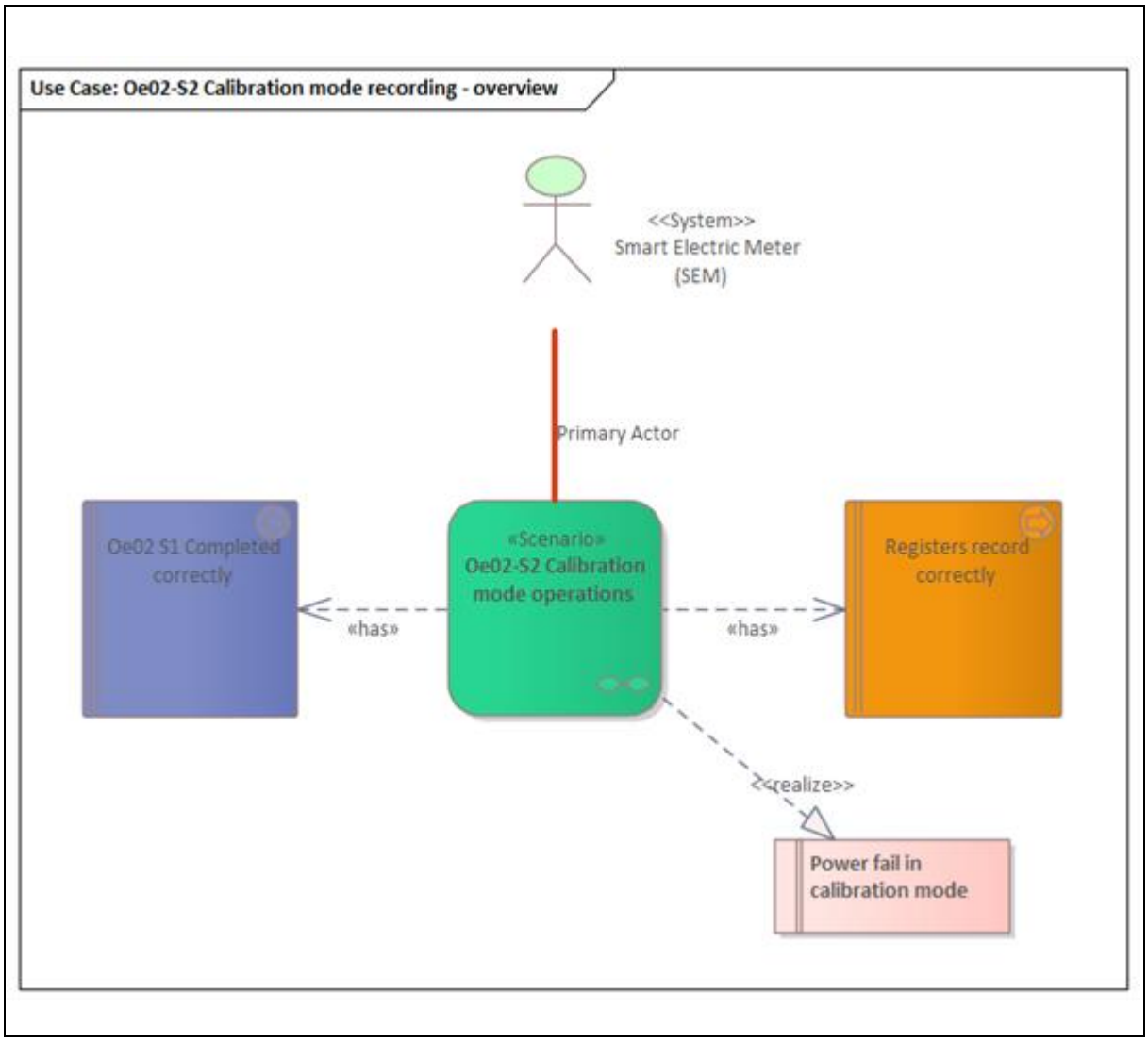
© Copyright 2026 Oesterreichs Energie. All rights reserved

The meter's calibration is tested.
The LED configuration will be changed during this phase to facilitate the tests being undertaken.
Records are collected by the meter during the calibration mode

Requirement list (refer to "Requirement" section for more information)	
Requirement R-ID	***Requirement name***
Req4	Power fail in calibration mode



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	Oe02-S2 Calibration mode operations							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
2.1		S2-A1 recording & display	The meter displays values according to the special display configuration. The LED s adopt the pulse conditions for calibration. For clarity, all other meter activities (Event logging, consumption recording, interval		Smart Electric Meter (SEM)			

© Copyright 2026 Oesterreichs Energie. All rights reserved

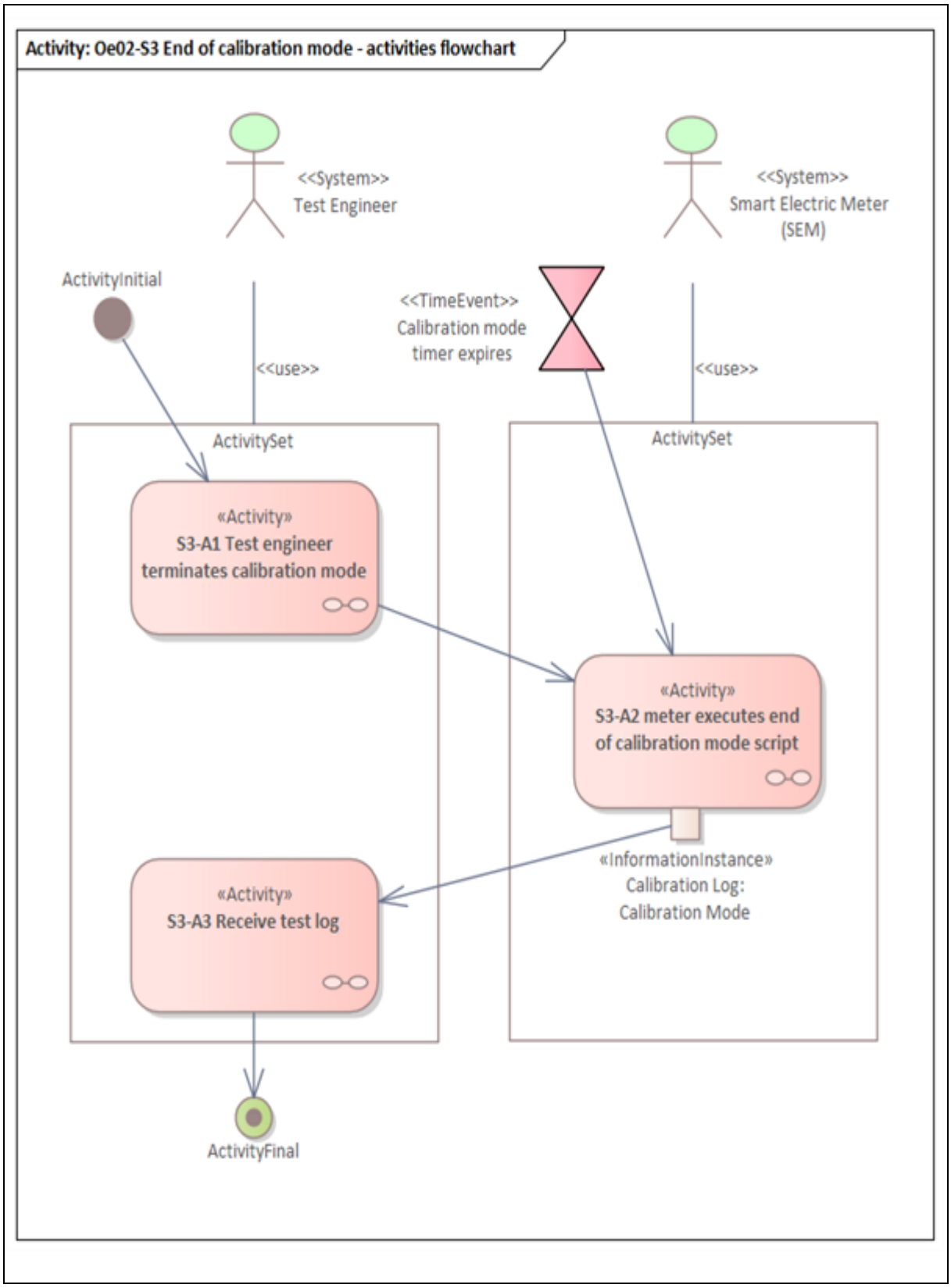
			logging etc) continue as normal.					

6.24.4.2.3. Oe02-S3 End of calibration mode

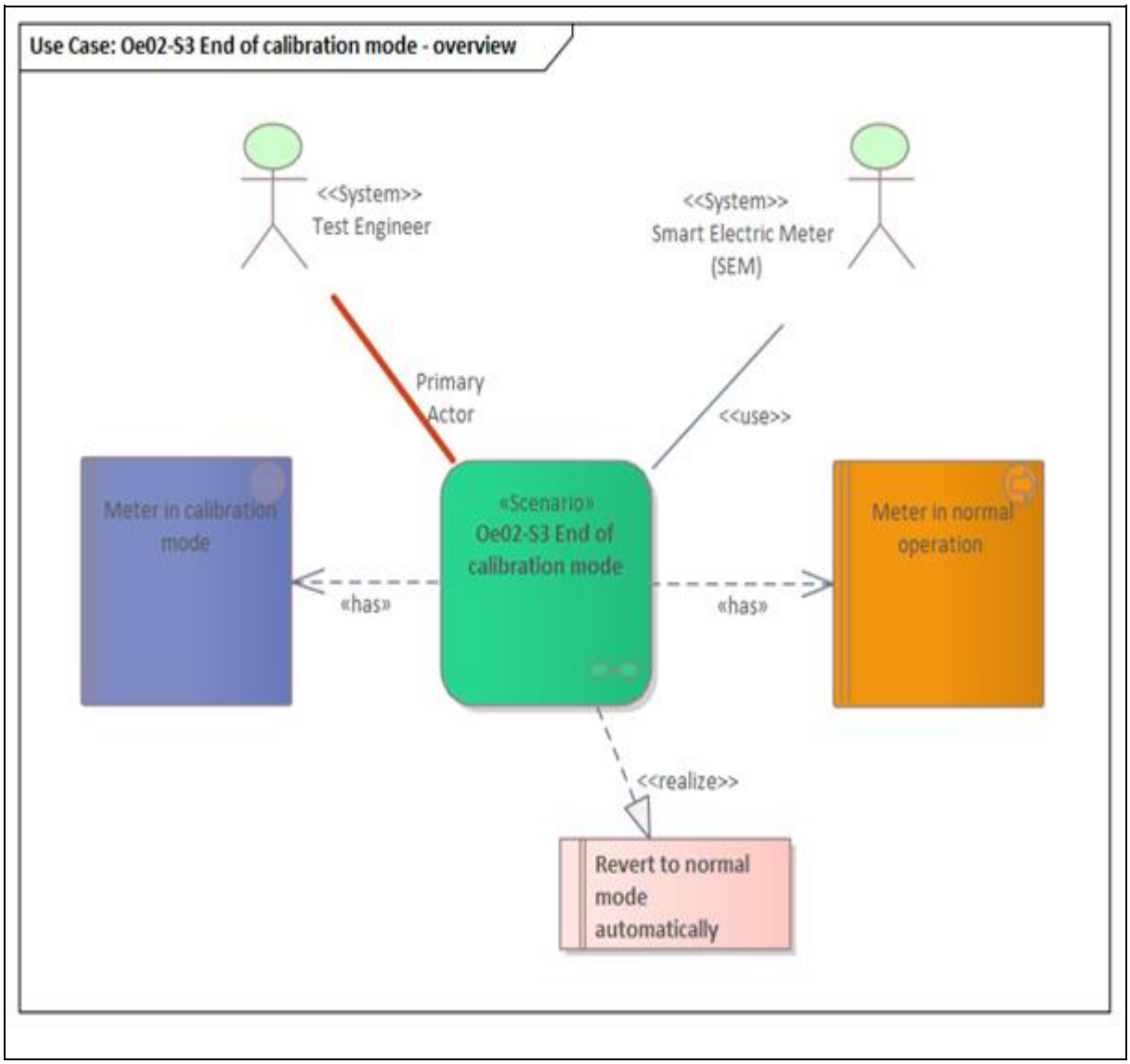
The meter ends calibration mode either as a result of an instruction from the Test Engineer or as a result of the timer.

Requirement list (refer to "Requirement" section for more information)	
Requirement R-ID	***Requirement name***
Req5	Revert to normal mode automatically

© Copyright 2026 Oesterreichs Energie. All rights reserved



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	Oe02-S3 End of calibration mode							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
3.1		S3-A1 Test engineer terminates calibration mode	Command(s) is/are sent from the Test Engineer to end the calibration mode. This includes executing the script and requesting the test log.		Test Engineer			

© Copyright 2026 Oesterreichs Energie. All rights reserved

3.2		S3-A2 meter executes end of calibration mode script	Script does the following steps 1) clear the test mode boolean 2) record the end of calibration mode event in the event log 3) return the display sequence to the default value 4) reset the LED configuration to default 5) cancel the calibration mode timer Note that if the test engineer has not collected the data, then the logs can be retrieved from the HES.		Smart Electric Meter (SEM)	Test Engineer	Info1-Calibration Mode	
3.3		S3-A3 Receive test log	The Test Engineer receives the log. The Test engineer will also record test results and deliver the report.		Test Engineer			

- 3.2. S3-A2 meter executes end of calibration mode script

Information Overview: Oe02-S3 End of calibration mode/S3-A2 meter executes end of calibration mode script

Script does the following steps
1) clear the test mode boolean
2) record the end of calibration mode event in the event log
3) return the display sequence to the default value
4) reset the LED configuration to default
5) cancel the calibration mode timer

Note that if the test engineer has not collected the data, then the logs can be retrieved from the HES.

Information sent:

Information object	*Instance name*	*Instance description*
Calibration Mode	Calibration Log	send the calibration log to the test engineer as a response to the command(s) issued.

6.24.5. Information exchanged

Information exchanged			
Information exchanged, ID	*Name of information*	*Description of information exchanged*	*Requirement, R-IDs*

© Copyright 2026 Oesterreichs Energie. All rights reserved

Info1	Calibration Mode	Calibration Mode Start Event Calibration Mode End Event Display Resolution increase LED register (the item for the LED to respond to) identification LED resolution (cycles per unit) adjustment LED pulse duration (milliseconds ON time) adjustment LED mode of operation (active, reactive, indication of start of LP1 period) Test exit Script Test exit schedule	
Info2	Display items Configuration	The instance below allows the configuration of data shown on the meter display where the attribute “capture_objects” defines attributes (non exhaustive) which are shown on the meter display. Object Name = General display readout (auto-scroll) IC = 7 Logical Name = 0-0:21.0.1.255 Description = List of the data to be available on the meter display in auto-scroll mode Object Name = alternate display readout (manual scroll) IC = 7 Logical Name = 0-0:21.0.2.255 Description = List of the data to be available on the meter display in manual scroll mode.	
Info3	Standard Event Log Objects	Class 7 - Standard Event Log 0-0:99.98.0.255 Class 1 - Event Object - Standard Event Log 0-0:96.11.0.255	
Info4	Generic Configuration Response	This will be one or more responses to SET or ACTION commands used to deliver a full or partial configuration of the Meter. OBIS codes are dependent on the Commands.	

6.24.6. Requirements (optional)

Requirements (optional)		
Categories ID	***Category name for requirements***	***Category description***

© Copyright 2026 Oesterreichs Energie. All rights reserved

Requirement R-ID	*Requirement name*	*Requirement description*
Req1	Calibration mode implemented	The meter must have a calibration mode implemented for efficient testing/calibration. and an event is recorded.
Req2	Meter parameters & selections are Operable	The functions supported by the calibration mode must be able to be activated and deactivated individually. These are: • Increasing the decimal places on the display, • Increasing the LED pulse constant, • Active/reactive switching of the LED, • Switching the LED pulse length.
Req3	Display of mode	The status of the calibration mode must be recognisable on the display.
Req4	Power fail in calibration mode	The meter is not allowed to deactivate the calibration mode in the event of a power failure.
Req5	Revert to normal mode automatically	If the calibration mode is not switched off by command, it must be deactivated automatically after 24 hours (timeout).

6.24.7. Common terms and definitions

Common terms and definitions	
Term	*Definition*
Profile_generic	IC = 7. This IC provides a generalized concept allowing to store, sort and access data groups or data series, called *capture objects*. Capture objects are appropriate attributes or elements of (an) attribute(s) of COSEM objects. The capture objects are collected periodically or occasionally. A profile has a *buffer* to store the captured data. To retrieve only a part of the buffer, either a value range or an entry range may be specified, asking to retrieve all entries that fall within the range specified. The list of *capture objects* defines the values to be stored in the *buffer* (using auto capture or the method *capture*). The list is defined statically to ensure homogenous buffer entries (all entries have the same size and structure). If the list of capture objects is modified, the *buffer* is cleared. If the buffer is captured by other “Profile generic” objects, their *buffer* is cleared as well, to guarantee the homogeneity of their *buffer* entries. The *buffer* may be defined as sorted by one of the *capture objects*, e.g. the clock, or the entries are stacked in a “last in first out” order.

© Copyright 2026 Oesterreichs Energie. All rights reserved

	For example, it is very easy to build a “maximum demand register” with a one entry deep sorted profile capturing and sorted by a “Demand register” *last_average_value* attribute. It is just as simple to define a profile retaining the three largest values of some period.
Register	IC = 3. This interface class can be used to represent any measured quantity, and has both the measured value and the scale and unit of measure available. Common uses include energy registers.
Demand_register	IC = 5. Register specific for demand monitoring.
LED	Light Emitting Diode. Used to indicate consumption and/or reactive.

6.25. Use Case Oe-03 – Communications module management

6.25.1. Description of the use case

6.25.1.1. Name of use case

Use case identification		
ID	***Area(s)/Domain(s)/Zone(s)***	***Name of use case***
	Austria	Oe-UC-03 Communications Module Management

6.25.1.2. Scope and objectives of use case

Scope and objectives of use case	
Scope	Generic control of change of communications module without removing the meter. Note that the scope does not include comms modules with their own COSEM servers and identities.
Objective(s)	Communications established: Communications in accordance with DSO practice are fully operational.
Related business case(s)	

6.25.1.3. Narrative of Use Case

Narrative of use case
Short description
Field exchange of communications module.
Complete description
A technician visits site and follows a process to exchange a communications module. This is in response to several possible circumstances: -Module failure - the module has a technical fault that can be resolved by module exchange -Network update - the module is not capable of upgrade to meet the requirements of a network change (e.g. 4G sunsetting) -Network change - the DSO wishes to use the meter on network that is not compatible with the existing module, for example, use a meter that was on G3-PLC to P2P or G3-Hybrid. In any of these circumstances, the processes will vary.

© Copyright 2026 Oesterreichs Energie. All rights reserved

Summary of use case

- **Oe-UC-03-S1 - Preconditioning of the meter**
  Description: If there is a change to the network technology, then it is possible that a new firmware version is needed for the meters affected. It is likely that a change of communications parameters is required, see Oe-UC-01.
- **Oe-UC03-S2 Module replacement**
  Description: The technician attends site and replaces the module.

6.25.1.4. Key performance indicators (KPI)

Key performance indicators			
ID	***Name***	***Description***	***Reference to mentioned use case objectives***
1	Communications in place	(ToDo) KPIs may vary depending on the purpose of the module exchange.	Communications established

6.25.1.5. Use case conditions

Use case conditions	
Assumptions	
1	Module transparency: The communications module is a key element of the network. However, at the application layer level it is transparent - settings and configuration of the module are carried out using Oe-UC01 which interacts with the meter and communications module as a single entity. Note that there may also be versions of communications modules that include data items related to communications, and these may have their own COSEM clients, and be managed as separate devices by the HES, but these are not included in the ACE SM GCP or in the Austria annex. Implementation of the communications module is therefore manufacturer specific.
2	Workforce Management system: For changing the module, the workforce managment system might be mandatory (e.g. if no communcation via WAN possible). Otherwise it might not possible to change the communication parameters.
Prerequisites	
1	Tested process: The module exchange - especially with respect to network change occurrences - has been thoroughly tested in non-production and pre-production environments.

6.25.1.6. Further information to the use case for classification/mapping

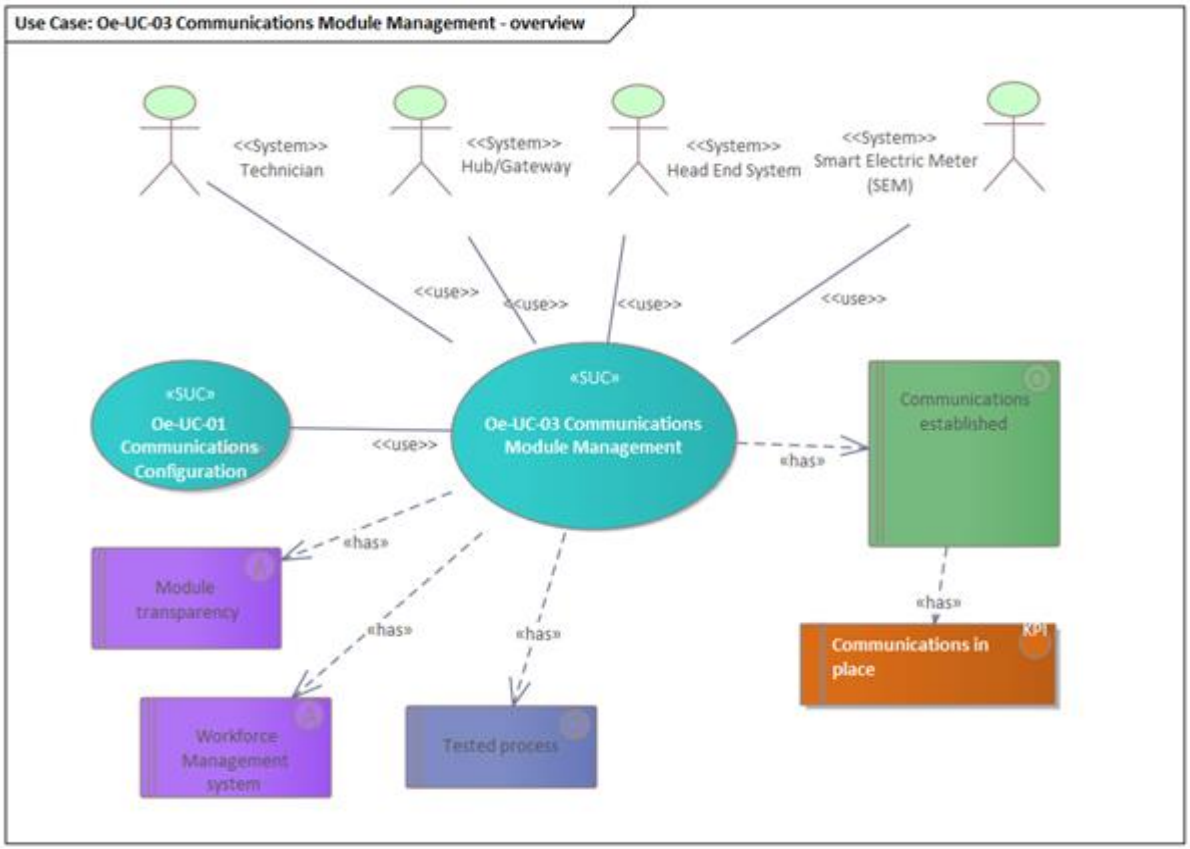
Classification information
Relation to other use cases
<<BUC>> Extensions <<SUC>> Oe-UC-01 Communications Configuration
Level of depth
high level first pass
Prioritisation
Mandatory
Generic, regional or national relation
Austria
Nature of the use case

© Copyright 2026 Oesterreichs Energie. All rights reserved

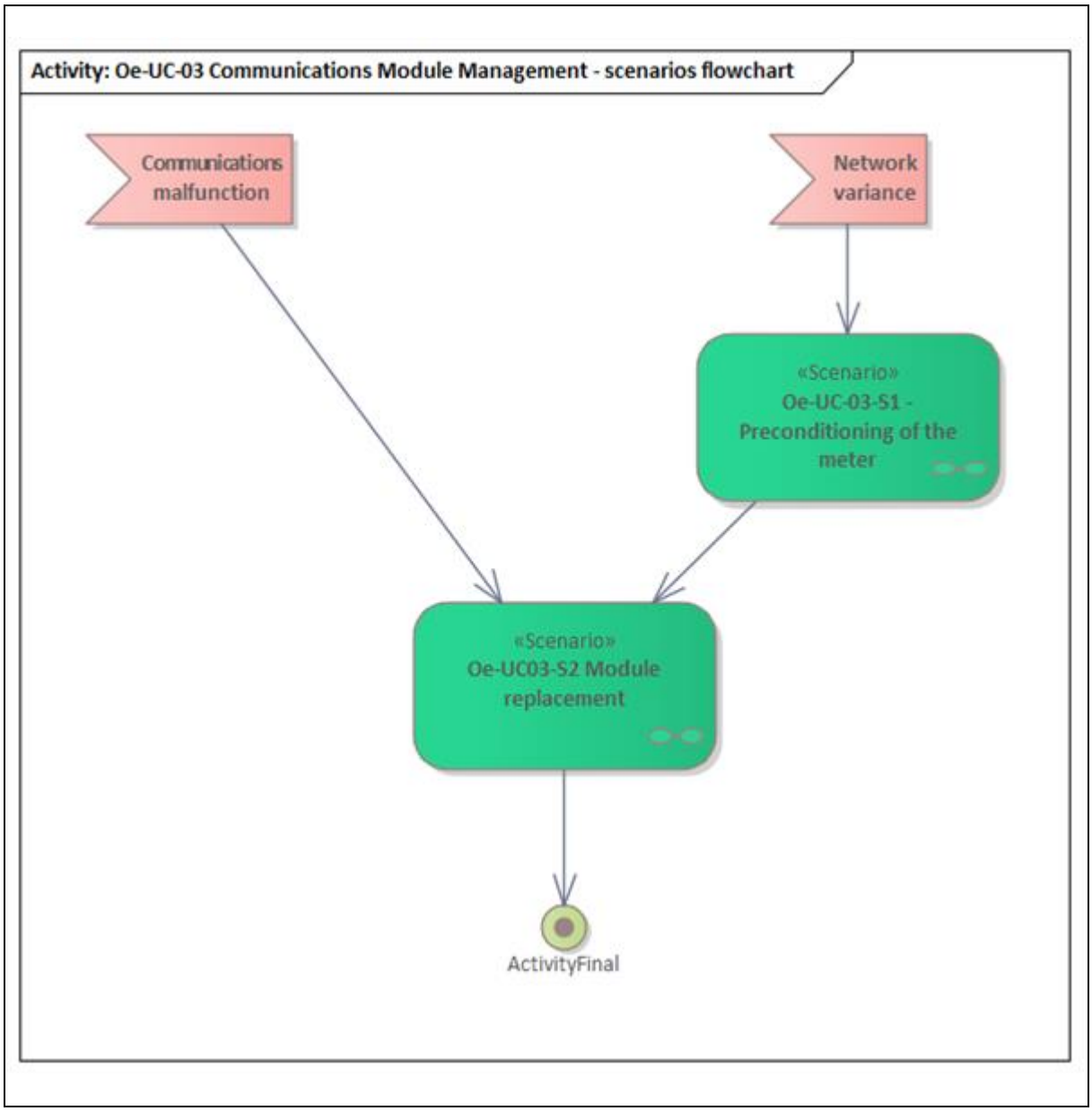
SUC
Further keywords for classification

6.25.2. Diagrams of use case

Diagram(s) of use case



© Copyright 2026 Oesterreichs Energie. All rights reserved



6.25.3. Technical details

6.25.3.1. Actors

Actors			
Grouping (e.g. domains, zones)		***Group description***	
Actor name	***Actor type***	***Actor description***	***Further information specific to this use case***
Technician	System	This person performs tasks with meters in the field, but is not necessarily qualified to do electrical works.	
Head End System	System	Head End System offers services to collect metering data and also to deliver configuration and other commands to the meters. It usually	

© Copyright 2026 Oesterreichs Energie. All rights reserved

		interacts with other business systems to deliver the meter data and other services to other business units and to wider industry.	
Smart Electric Meter (SEM)	System	Smart Meter is an AC Electricity Meter with additional functions.	
Hub/Gateway	System	Hub/Gateway is an intermediate device that is interposed between the Smart Meter and the HES. It may be a simple relay device or have intelligence to read meters and perform other functions directly.	

6.25.3.2. References

References						
No.	***Reference Type***	***Reference***	***Status***	***Impact on use case***	***Originator / organisation***	***Link***
1		Austria annex to the ACE SM GCP	Required		OeE	

6.25.4. Step by step analysis of use case

6.25.4.1. Overview of scenarios

Scenario conditions						
No.	***Scenario name***	***Scenario description***	***Primary actor***	***Triggering event***	***Pre-condition***	***Post-condition***
1	Oe-UC-03-S1 - Preconditioning of the meter	If there is a change to the network technology, then it is possible that a new firmware version is needed for the meters affected. It is likely that a change of communications parameters is required, see Oe-UC-01.	Head End System, Technician	Network variance: Either the network is becoming unavailable (e.g. 4G sunsetting) or there is a need to change the communications network to an alternative technology (e.g. P2P to PLC or vice-versa).	Meter is contactable: Communications can be established with the meter.	Meter ready for module exchange: Meter has firmware and configuration ready for the new module.
2	Oe-UC03-S2 Module replacement	The technician attends site and replaces the module.	Technician	Communications malfunction: Communications has worked	Technician has equipment: Technician will need replacement	Meter communications established with HES: The meter has

© Copyright 2026 Oesterreichs Energie. All rights reserved

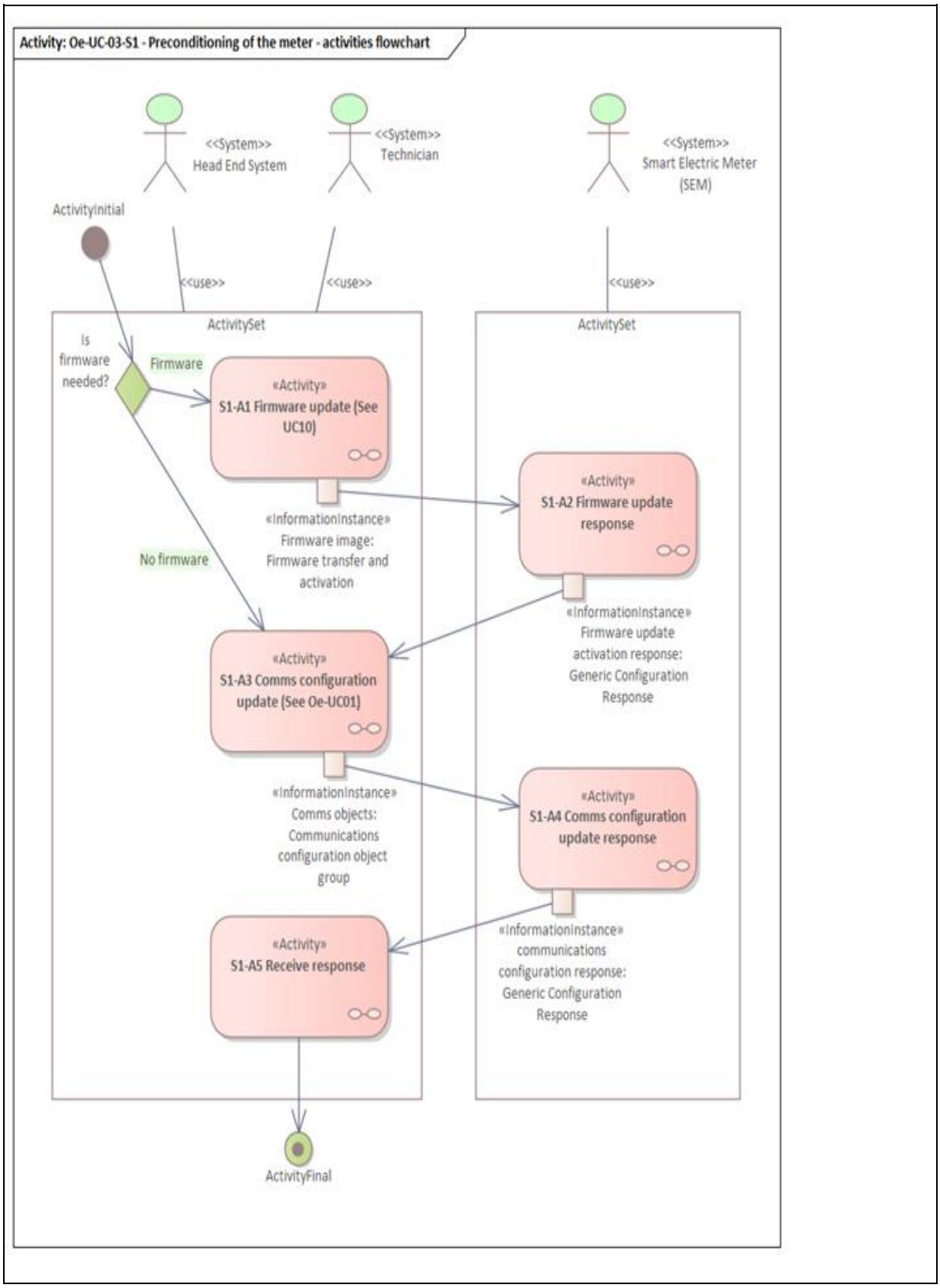
				but is now not working.	module and other tools and equipment. Technician qualified: Technician has suitable qualifications and has documented process for the exchange.	sent a datanotification (Push on Connectivity) to the HES, and received a response.

6.25.4.2. Steps - Scenarios

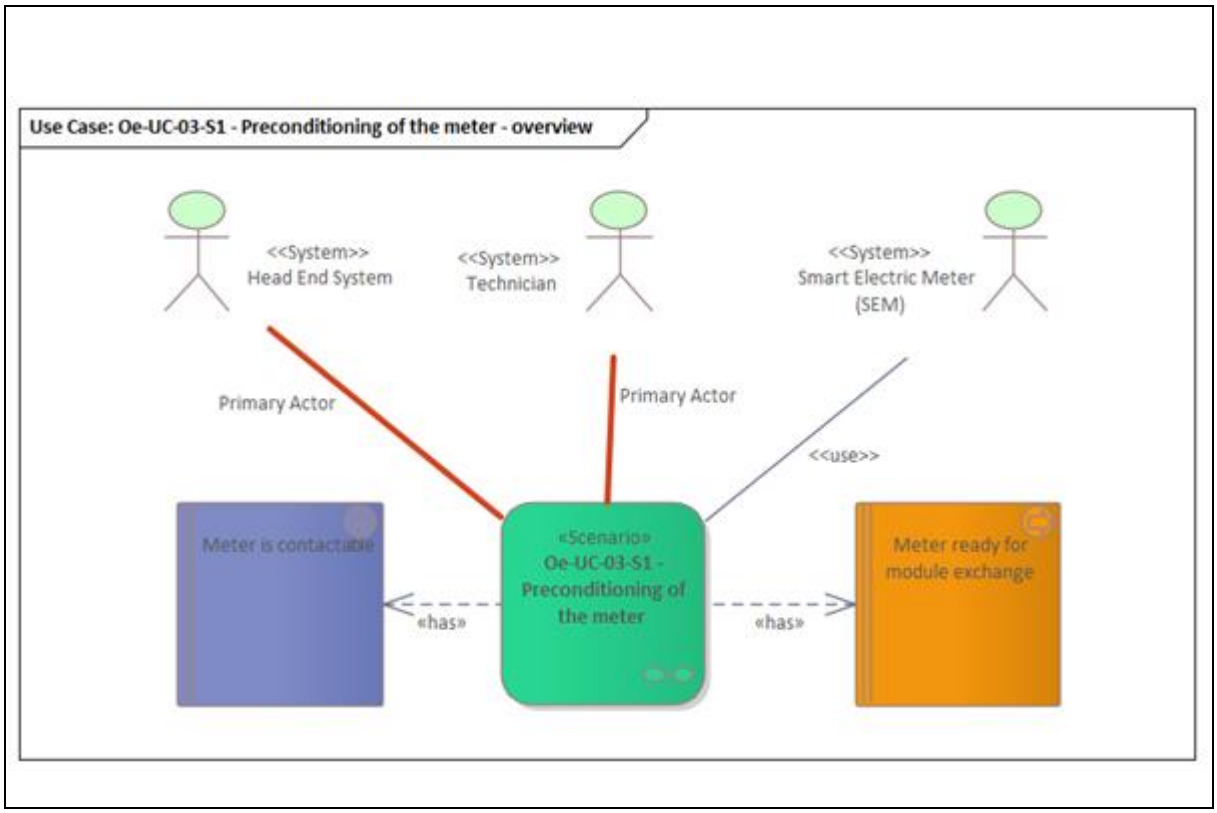
6.25.4.2.1. Oe-UC-03-S1 - Preconditioning of the meter

If there is a change to the network technology, then it is possible that a new firmware version is needed for the meters affected.
It is likely that a change of communications parameters is required, see Oe-UC-01.

© Copyright 2026 Oesterreichs Energie. All rights reserved



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	Oe-UC-03-S1 - Preconditioning of the meter							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
1.1		S1-A1 Firmware update (See UC10)	The firmware is updated in the meter		Head End System, Technician	Smart Electric Meter (SEM)	Info1-Firmware transfer and activation	
1.2		S1-A2 Firmware update response			Smart Electric Meter (SEM)	Head End System, Technician	Info2-Generic Configuration Response	
1.3		S1-A3 Comms configuration update (See Oe-UC01)	New communications configuration parameters are applied to the meter.		Head End System, Technician	Smart Electric Meter (SEM)	Info3-Communications configuration object group	
1.4		S1-A4 Comms configuration update response			Smart Electric Meter (SEM)	Head End System, Technician	Info2-Generic Configuration Response	

© Copyright 2026 Oesterreichs Energie. All rights reserved

1.5		S1-A5 Receive response	The HES receives the response, stores needed data and updates other systems as required.		Head End System, Technician			

- 1.1. S1-A1 Firmware update (See UC10)

  Information Overview: Oe-UC-03-S1 - Preconditioning of the meter/S1-A1 Firmware update (See UC10)

  The firmware is updated in the meter

  Information sent:

Information object	*Instance name*	*Instance description*
Firmware transfer and activation	Firmware image	firmware image and activation process as per UC10.

- 1.2. S1-A2 Firmware update response

  Information Overview: Oe-UC-03-S1 - Preconditioning of the meter/S1-A2 Firmware update response

  Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	Firmware update activation response	Response to the activation command.

- 1.3. S1-A3 Comms configuration update (See Oe-UC01)

  Information Overview: Oe-UC-03-S1 - Preconditioning of the meter/S1-A3 Comms configuration update (See Oe-UC01)

  New communications configuration parameters are applied to the meter.

  Information sent:

Information object	*Instance name*	*Instance description*
Communications configuration object group	Comms objects	For detail, see UC Oe-01

- 1.4. S1-A4 Comms configuration update response

  Information Overview: Oe-UC-03-S1 - Preconditioning of the meter/S1-A4 Comms configuration update response

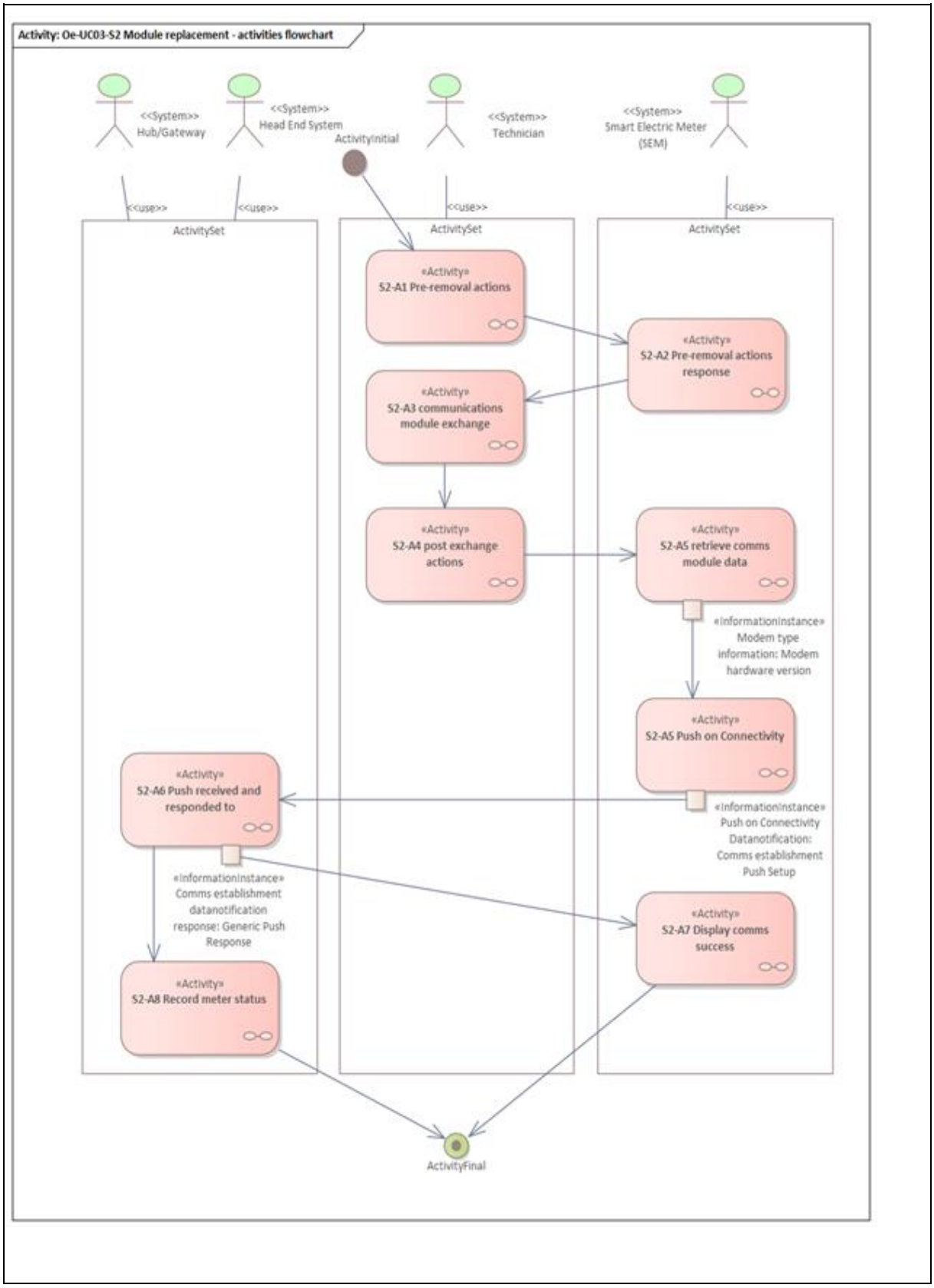
  Information sent:

Information object	*Instance name*	*Instance description*
Generic Configuration Response	communications configuration response	Responses to the communications commands.

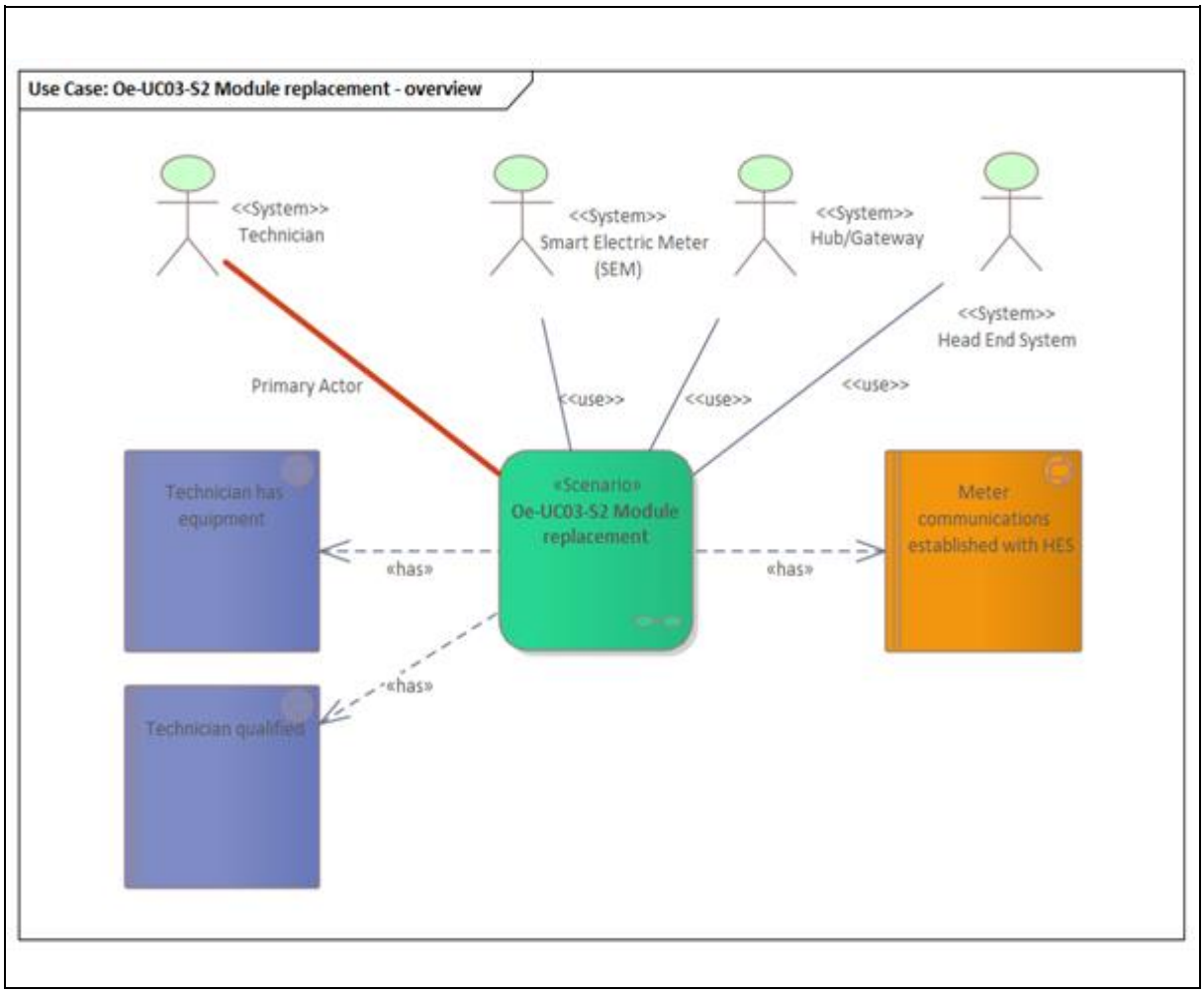
6.25.4.2.2. Oe-UC03-S2 Module replacement

© Copyright 2026 Oesterreichs Energie. All rights reserved

The technician attends site and replaces the module.



© Copyright 2026 Oesterreichs Energie. All rights reserved



Scenario step by step analysis

Scenario								
Scenario name	Oe-UC03-S2 Module replacement							
Step No	***Event***	***Name of process/activity***	***Description of process/activity***	***Service***	***Information producer (actor)***	***Information receiver (actor)***	***Information exchanged (IDs)***	***Requirement, R-IDs***
2.1		S2-A1 Pre-removal actions	The steps to be carried out will depend on the DSO and the module change. Could include - Download readings, change communications settings Depending on the communication module: - set address for HES push		Technician			

© Copyright 2026 Oesterreichs Energie. All rights reserved

			Meter reading Events					
2.2		S2-A2 Pre-removal actions response			Smart Electric Meter (SEM)			
2.3		S2-A3 communications module exchange	The installed communications module is removed and replaced with the new module. This may require a number of steps depending on the old and new modules.		Technician			
2.4		S2-A4 post exchange actions	This is likely to include: Stimulate the meter to send the push on communications as needed Record the exchange information. This is likely to take the form of data entry in a work force management application, and can include the communications parameters for the device once the module is installed. If the IP address is static with the comms module replaced, then it would be possible, but if there are no communications with a DHCP, then there may not be data like an IP address to collect. Note that PLC module changes could include need to configure the tone map,		Technician			

© Copyright 2026 Oesterreichs Energie. All rights reserved

			tone mask, and other related items.					
2.5		S2-A5 Push on Connectivity	Note that this is described in Oe-UC-01.		Smart Electric Meter (SEM)	Head End System, Hub/Gateway	Info4-Comms establishment Push Setup	
2.6		S2-A5 retrieve comms module data	The SEM retrieves the hardware identifier from the module, and stores it within the object model		Smart Electric Meter (SEM)	Smart Electric Meter (SEM)	Info5-Modem hardware version	
2.7		S2-A6 Push received and responded to	The HES sends the datanotification response		Head End System, Hub/Gateway	Smart Electric Meter (SEM)	Info6-Generic Push Response	
2.8		S2-A7 Display comms success	As needed, indicate that communications to the HES or possibly a gateway is established on the meter display.		Smart Electric Meter (SEM)			
2.9		S2-A8 Record meter status	Record that the meter communications is established. Notify other systems as necessary.		Head End System, Hub/Gateway			

- 2.5. S2-A5 Push on Connectivity

  Information Overview: Oe-UC03-S2 Module replacement/S2-A5 Push on Connectivity

  Note that this is described in Oe-UC-01.

  Information sent:

Information object	*Instance name*	*Instance description*
Comms establishment Push Setup	Push on Connectivity Datanotification	Push on connectivity data notification defined using the push setup on connectivity object.

- 2.6. S2-A5 retrieve comms module data

  Information Overview: Oe-UC03-S2 Module replacement/S2-A5 retrieve comms module data

  The SEM retrieves the hardware identifier from the module, and stores it within the object model

  Information sent:

Information object	*Instance name*	*Instance description*
Modem hardware version	Modem type information	The hardware version of the Modem.

- 2.7. S2-A6 Push received and responded to

© Copyright 2026 Oesterreichs Energie. All rights reserved

Information Overview: Oe-UC03-S2 Module replacement/S2-A6 Push received and responded to

The HES sends the datanotification response

Information sent:

Information object	*Instance name*	*Instance description*
Generic Push Response	Comms establishment datanotification response	Acknowledgement of successful comms registration.

6.25.5. Information exchanged

Information exchanged			
Information exchanged, ID	*Name of information*	*Description of information exchanged*	*Requirement, R-IDs*
Info1	Firmware transfer and activation	Instances of the following COSEM Interface classes: Image transfer (class_id: 18) Single action schedule (class_id: 22) Script table (class_id 9) Data (class_id 1) and the following COSEM Objects: Image transfer 0-0:44.0.0.255 Image transfer activation scheduler 0-0:15.0.2.255 Predefined Scripts - Image activation 0-0:10.0.107.255 Active firmware identifier 1-0:0.2.0.255 Active firmware signature 1-0:0.2.8.255 Active firmware identifier 1 1-1:0.2.0.255 Active firmware signature 1 1-1:0.2.8.255 Active firmware identifier 2 1-2:0.2.0.255 Active firmware signature 2 1-2:0.2.8.255	
Info2	Generic Configuration Response	This will be one or more responses to SET or ACTION commands used to deliver a full or partial configuration of the Meter. OBIS codes are dependent on the Commands.	
Info3	Communications configuration object group	See the object model for the full list of affected objects for preset.	

© Copyright 2026 Oesterreichs Energie. All rights reserved

Info4	Comms establishment Push Setup	Push setup - On connectivity. IC = 40, 0-0:25.9.0.255	
Info5	Modem hardware version	OBIS 0-0:96.1.4.255, class 1, attribute 2.	
Info6	Generic Push Response	This may depend on the lower layers employed. It may be an Application layer response from the cosem Client, or it may be a lower layer acknowledgement of datagram delivery.	

6.25.6. Common terms and definitions

Common terms and definitions	
Term	***Definition***
communications_module	A device that provides wide area communications linkage for a meter.
Hub/Gateway	This is a neighbourhood network device, and may be a basic Gateway or a Dualmode-Gateway.
Dualmode-Gateway	A gateway with advanced features, for example meter reading or firmware image distribution.
push_setup	IC = 40. The Push setup IC contains a list of references to COSEM object attributes to be pushed. It also contains the push destination and method as well as the communication time windows and the handling of retries. For a full explanation, see Blue Book 17 part 2 clause 4.4.8.2.

7. Configuration of protection of the Service (optical) interface.

ACE SM GCP is extended with respect to delivery of protection of the service interface. DLMS/COSEM supports a specific Communication port protection Interface Class, (class_id = 124) and this is intended to provide an intermediate option from completely disabled or fully enabled port.

This is intended to disable the port for increasing periods of time after a threshold of failed communication attempts.

Instances of this Interface Class have:

1) control of the protection mode – in that a port can be unlocked, locked on failed attempts, and locked.
2) A number of allowed failed attempts.
3) An initial lockout time
4) A steepness factor that controls the increase in lockout time after extended failure of attempts.
5) A maximum lockout time
6) A protection status that indicates the current state of the port.
7) A counter of failed attempts since the last successful login (or remote reset)

© Copyright 2026 Oesterreichs Energie. All rights reserved

8) A counter of total failed attempts.

A full description of the IC is in Blue Book Part 2.

An instance of this object is included in the object model, and default values are included in the object model.

A DSO can use the UC14 extension to configure:

1) Protection mode (attribute 2) to lock, unlock, or control the port using the parameters;

- Number of failed attempts (attribute 3);

2) Initial lockout time (attribute 4) measured in seconds;
3) Steepness factor (attribute 5); and
4) Maximum lockout time (attribute 6) also measured in seconds.

And, when changing these parameters, the DSO can also execute the reset method as preferred.

The DSO can use Use Case 3 to read out information about the status of the Object, any of the values above can be read out, and also:

1) Port reference (attribute 7) which is programmed to the OBIS code for the port;

- Protection status (attribute 8) which reports an enum: if the port is unlocked (0), temporarily locked (1), or locked (2);

2) Failed attempts (attribute 9) which indicates the number of failed attempts since the last reset; and
3) Cumulative failed attempts (attribute 10) which indicates the total number of failed attempts.

The OBIS code for this object is 0-0:44.2.0.255.

The default values chosen in the Object Model will:

1) Allow 5 erroneous attempts to connect.
2) Then lock the port for 60 seconds
3) Further erroneous attempts (after the end of the lock period) will cause escalating lock times.
4) The maximum lock time is 24 hours

© Copyright 2026 Oesterreichs Energie. All rights reserved

Oesterreichs Energie Companion Standard
Smart Meter 2.0

D.2_OE_CS_Implementation_Guide_G3-PLC_und_G3-Hybrid

Version 1.0

31.03.2026

Revision History

Version	Change	Datum	Autor
1.0	Initial Release	31.03.2026	Oesterreichs Energie

Content

A. Introduction – Definition 4

B. G3-PLC Communication Module 5

B.1 Coupling setup for PLC signal measurement 5

B.2 Signal strength measurements 5

B.3 Reception Input Impedance 6

B.4 Notching support 6

C. Physical and Data Link Layers 6

C.1 Physical Layer 6

C.2 RF Physical Layer 7

C.3 Implementation requirements 7

C.4 MAC layer – Frame Counter Handling 7

D. Initialization and Bootstrapping 8

E. Timeout and Keep-Alive mechanisms 12

F. DLMS/COSEM Communication Profiles and Services 13

F.1 UDP/IP Profile 13

F.2 G3 Interface Setup 14

F.3 G3 Interface Setup – Pending/Backup 15

F.4 G3 Network Management 15

A. Introduction – Definition

The aim of this document is to provide a uniform definition of the functions and parameters required for the PLC and RF communication infrastructure to ensure the interoperability of all smart meters and head-end systems.

It is a complementary document to the ITU-T G.9901 and G.9903 standards, describing the physical and data link layers.

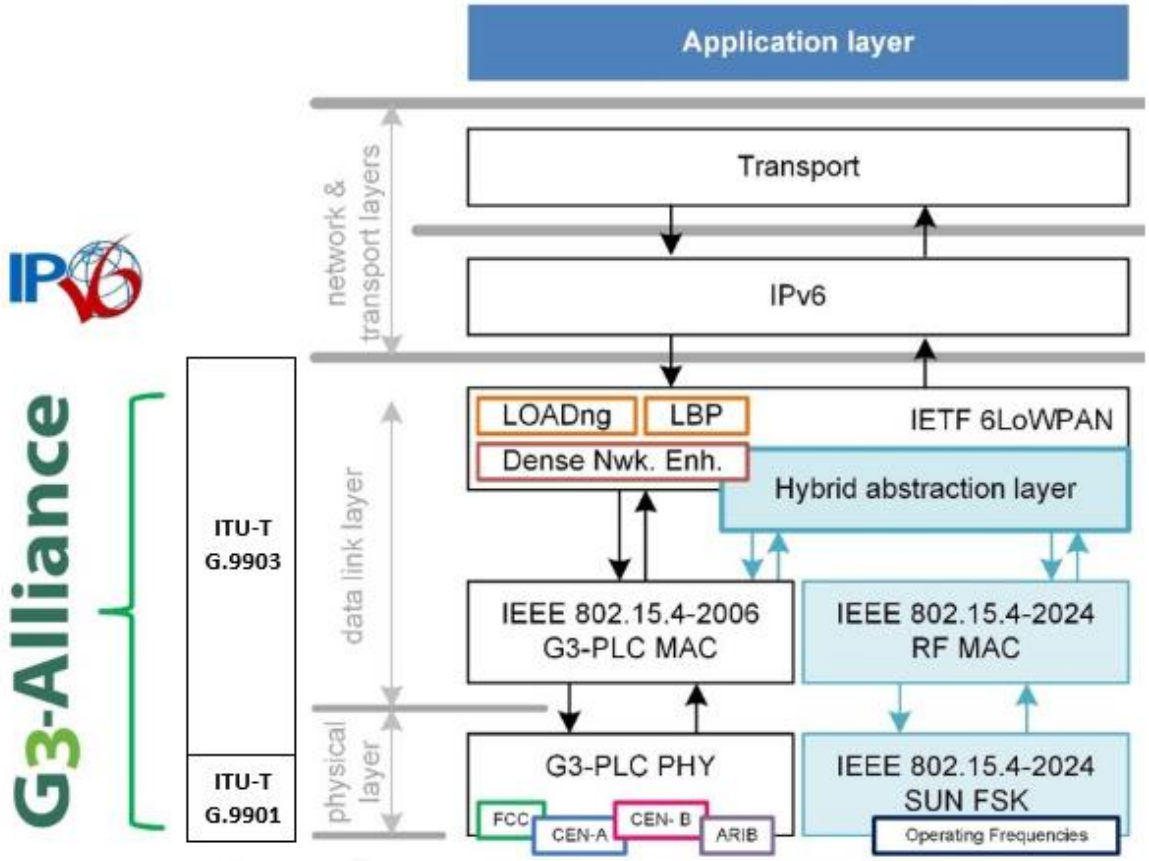


Figure 1: G3-Hybrid based metering profile.

The following topics are defined here:

- Supported network technologies
- Specific counter functions
- Additions to the D.1_OE_CS_Objektmodel.xlsx
- Additional specific event, alarm, and troubleshooting procedures

For functions that are already documented, reference is made only to the relevant documents. For example, ITU-T G.9901, ITU-T G.9903, etc.

B. G3-PLC Communication Module

B.1 Coupling setup for PLC signal measurement

Two coupling setups are used for PLC signal measurement, following G3 Alliance Certification program document - Performance test suite for G3 device certification:

- A CISPR 16-1 LISN, as referenced by CISPR16-1: Ed2.1 §5.1.2 (50 Ω/50 µH + 5 Ω artificial mains V-network)
- A modified CISPR 16-1 LISN resulting in a 2-Ohms impedance following ÖVE/ÖNORM EN 50065-1 and ETSI TS 103 909 V1.1.1 (2012-12).

B.2 Signal strength measurements

Communication modules working in the CENELEC-A band shall conform to the definition in ITU-T G.9901 concerning the output specification relating to the 3 kHz – 148,5 kHz band.

Modules working in the FCC band shall conform to the definition in ITU-T G.9901 concerning the output specification relating to the 148,5 kHz – 535 kHz band.

Conformance with EN 50065-1

G3 PLC modules must meet the requirements of EN 50065-1 regarding transmitter output voltage and interference limits.

Signal strength measurement

Signal strength measurement follows the procedure defined in Performance test suite for G3 device certification §3.1 and §3.2, which rely on the methods defined in and measure the amplitude of a G3 frame FCH and payload fields, for each carrier, in dBµV.

The resulting signal strength is defined as the amplitude of the carrier with the lowest signal level in the whole frequency band.

The signal strength of Smart Meters must be above the target defined in the following table:

Table 1: Signal strength of Smart Meters

Description	**Targets**			
Type of PLC injection	Single phase injection		3-phases injection	
Operating PLC band	CEN-A	FCC	CEN-A	FCC
Minimum signal level that must be injected on a 2-Ohms LISN by the device. Correspond to PHY_001_SIGNAL_LEVEL value on a G3 performance certificate.	≥ 100 dBµV	≥ 104 dBµV	≥ 100 dBµV	≥ 104 dBµV
Minimum signal level that must be injected on a CISPR16-1 LISN by the device. Correspond to PHY_002_SIGNAL_LEVEL value on a G3 performance certificate.	≥ 101 dBµV	≥ 105 dBµV	≥ 101 dBµV	≥ 105 dBµV

The signal strength for Dualmode-Gateways should be 3 - 5 dBµV above the target defined in that table.

Additional requirements:

- For both single-phase and three-phase transmitters, no single carrier may have an average amplitude level outside the range of ±5 dB with respect to the average amplitude of all subcarriers (at the same transmit power).
- The previously mentioned amplitude levels must still be observed when using notched subcarrier frequencies.

B.3 Reception Input Impedance

Couplers and analogue front-end components for the communication section must ensure an input impedance of over 50 ohms in the frequency range [35 kHz – 500 kHz] measured at network level during reception operation.

B.4 Notching support

The communication module must support tone-masking (i.e. disabling of individual PLC carriers), using the mechanism defined in G3 Alliance Specifications.

When suppressing four adjacent subcarrier frequencies, the attenuation relative to the normal transmit level must be at least 13 dB. (see chapter B.3 in ITU-T G.9901).

Suppressing the subcarrier frequencies must not negatively affect the signal level of frequencies that are not suppressed.

The disabled ("notched") subcarrier frequencies must be modifiable both locally and remotely, through COSEM object “G3-PLC MAC setup” object, “mac_tone_mask” attribute.

C. Physical and Data Link Layers

G3 communication is based on the following recommendations of the International Telecommunication Union (ITU):

- Recommendation ITU-T G.9901 (2017) Amd.1 (04/2023). Narrowband orthogonal frequency division multiplexing power line communication transceivers – Power spectral density specification Amendment 1
- Recommendation ITU-T G.9903 (2017) Corrigendum 1 + Amendment 2 (03/23). Narrowband orthogonal frequency division multiplexing power line communication transceivers for G3-PLC networks Amendment 2

Certification from G3 Alliance is also requested to ensure the compliance to these versions and verify the signal level requirements detailed in previous chapter.

C.1 Physical Layer

The frequency bands used by G3-PLC or G3-Hybrid are specified in ITU-T G.9901, and the operating description is given in ITU-T G.9903.

Frequency bandplan and physical parameters

A PLC device must support both PLC bands. Switching from CENELEC-A to FCC must be possible during operation through COSEM object “PLCG3_Bandplan” without updating the firmware.

The communication module input filter must adapt to the operating PLC band, so that a PLC signal from outside of the operating band is blocked.

A wide-frequency filter allowing simultaneous operation in both CENELEC-A and FCC band is not allowed, as this can allow interference between PLC bands (ex. suboptimal reception gain or receiver saturation).

C.2 RF Physical Layer

The RF physical layer is defined in ITU-T G.9903, based on the SUN (Smart Utility Network) FSK profile specified in IEEE 802.15.4-2020.

The physical layer must support at least the 863MHz band (863,1 MHz to 869,9 MHz) in mode #1, with optional support for mode #2.

Default configuration for RF physical layer for Smart Meters and Dualmode-Gateways:

Table 2: Default configuration for RF physical layers

Frequency band:	866 MHz band in mode #1 channel 29 (correspond to the 868,0 MHz channel)
Max. Transmit Power:	25 mW (= 14 dBm)
Duty Cycle:	2,5% (ETSI EN 300 220-2 v3.2.1 allows for 100s Tx time per 1h per 200 kHz spectrum)
Minimum pause time:	100 ms (macMinInterTxInterval_RF parameter)

C.3 Implementation requirements

Requirements for Smart Meter

- Broadcast Log Table shall allow at least 20 entries
- Neighbour Table shall allow at least 1.200 entries
- POS Table shall allow at least 1.200 entries
- Routing Table shall allow at least 1.200 entries

Requirements for Dualmode-Gateway

- Device Table shall allow at least 1.200 entries
- Neighbour Table shall allow at least 1.200 entries
- POS Table shall allow at least 1.200 entries
- Routing Table shall allow at least 1.200 entries
- Broadcast Log Table shall allow at least 20 entries
- Group Table shall allow at least 16 entries
- Context Information Table shall allow 16 entries

In case the Table is full and the node must store a new entry, the entry corresponding to the shortest valid time is removed.

C.4 MAC layer – Frame Counter Handling

The MAC layer frame counter must not be reset when receiving a new GMK key (during the bootstrapping or rekeying process). Resetting the frame counter can cause communication problems if a device bootstraps alternately in two PLC networks (e.g., due to crosstalk).

C.4.1 Key Management Overview

During manufacturing a Smart Meter is provisioned with a unique PSK key and a unique PSK-KEK key, generated from a cryptographically secure random generator.

The keys are securely uploaded to the information system on Smart Meter delivery. The keys are delivered to the DSO via a secure shipment file process.

The PSK and PSK-KEK keys can be replaced by writing to the PLCG3_PSK and PLCG3_PSK_KEK COSEM objects respectively. The new key is wrapped by the AES-256 key wrap algorithm, using the current PSK-KEK as the wrapping key.

The PAN coordinator manages the PAN's GMK key and provides it to the devices during bootstrapping. The GMK key remains the same after a PAN coordinator reboot.

The PAN coordinator also acts as an EAP authentication server to the devices. To perform the EAP-PSK bootstrapping exchanges with the devices, the PAN coordinator downloads the device's PSK key from the information system.

C.4.2 GMK Re-keying operation

To perform a GMK key change, the following operations are performed by the PAN coordinator:

- A new GMK must be generated at least every 90 days or when the PAN coordinator has sent 1.000.000 frames using the current GMK.
- Generation phase: The PAN coordinator generates a new GMK key and chooses an identifier (KeyId-new), which is different from the identifier of the current GMK. GMK key identifier values can only be set to 0 or 1.
- Distribution phase: The PAN coordinator carries out an EAP-PSK authentication procedure with every device of the PAN to distribute the new GMK.
- This procedure starts with an EAP-PSK message 1, follows the normal EAP-PSK message exchanges and concludes with an EAP-Success message.
- After key distribution, a device can receive frames using either the current GMK or the new GMK and send frames using the current GMK.
- Activation phase: The PAN coordinator activates the new GMK by sending an LBP ACCEPTED message embedding a GMK-Activation parameter to each device of the PAN. Devices acknowledge the message with an LBP JOINING message embedding a Parameter-result.
- After key activation, a device sends frames using the new GMK.
- Once the EAP server has completed the GMK activation with all peers, it sends an LBP ACCEPTED message with a GMK-remove parameter to each peer, to ensure deletion of the old GMK key from the network.
- After key removal, only the new GMK must be used for frame reception and transmission.

D. Initialization and Bootstrapping

On startup, PAN Devices (Smart Meter) shall initialize their G3 modems and carry out a registration procedure, which is controlled by the device application layer (see "G3 guideline - Upper layer integration" chapter 3).

To join a G3 PLC or G3 Hybrid network, the device must execute the following steps:

(0) Initialise the G3 modem: configure the device EUI-64 (if needed), initialise G3 parameters, restore the frame-counters and LOADng sequence-number values.

(1) Discover surrounding G3 networks and G3 neighbouring devices by calling ADPM-DISCOVERY.request,

(2) Choose which neighbouring device to contact to join the selected G3 network,

(3) Execute a bootstrap procedure by calling ADPM-NETWORK-JOIN.request, with the target neighbouring device acting as a bootstrapping relay toward the PAN-Coordinator.

Cumulative and random delays are applied before retrying a discovery (1) or bootstrap (3) step, to avoid network congestion if a lot of devices are bootstrapping at the same time (for example following a power outage).

The registration procedure is detailed below:

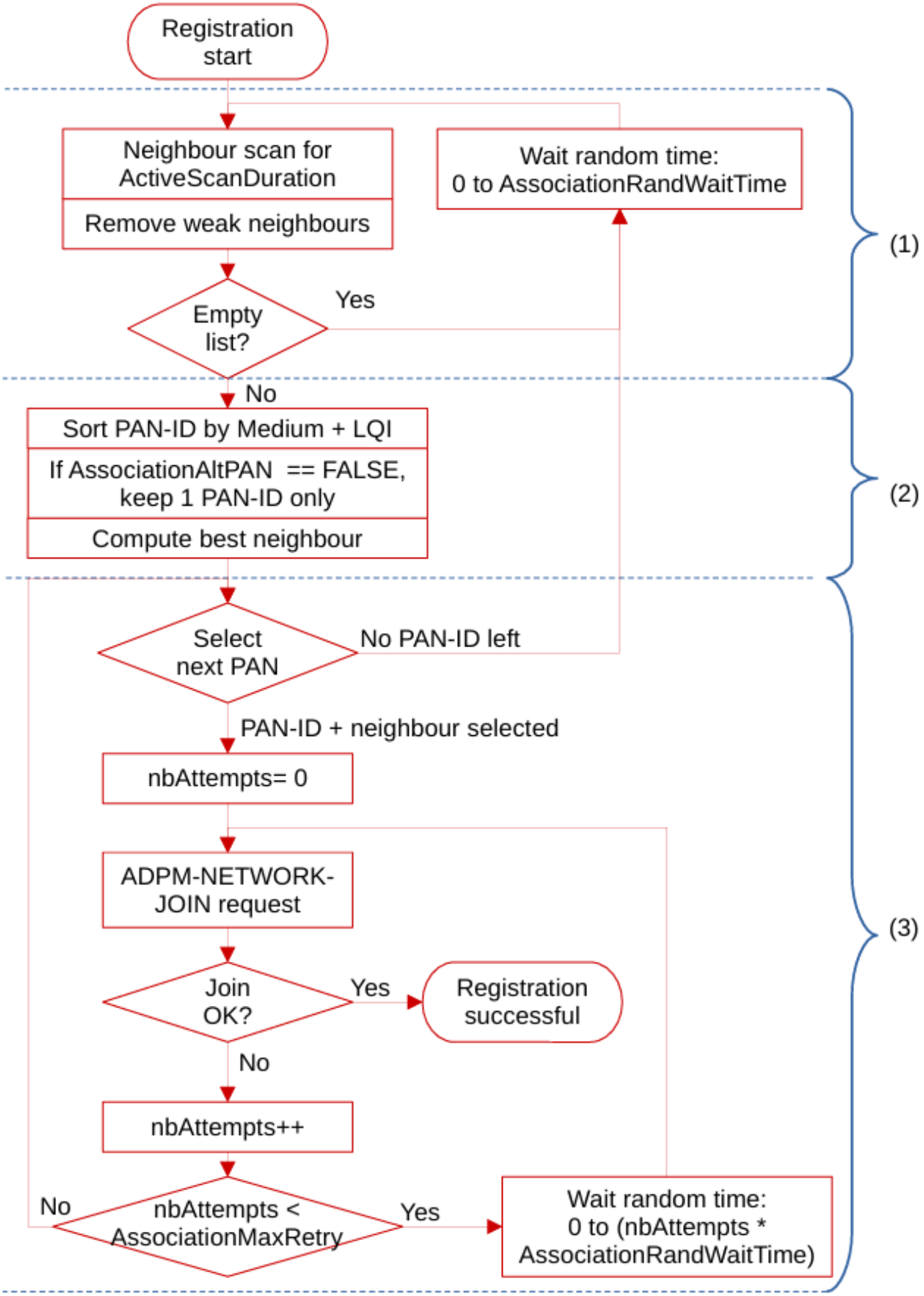


Figure 3: Device registration procedure

Step 1: Neighbour discovery

On power-up, reboot or reset, a PAN Device executes a neighbour discovery using ADPM-DISCOVERY.request() for a duration of ActiveScanDuration seconds.

This provides a list of neighbouring G3 devices, with the following information for each neighbour:

- PAN-ID (16 bits): G3 network identifier
- Short address (16 bits): neighbour MAC address
- RC_COORD (16 bits): route cost between the neighbour and its PAN Coordinator
- LQI (8 bits): Link Quality Indicator measured between the neighbour and the PAN Device
- Media Type (PLC or RF): the medium the neighbour was detected on
- A G3 Hybrid neighbour can be detected on both PLC and RF. In this case, 2 entries will be present in the list with different MediaType and LQI values

Entries with bad Link Quality indicator are removed from the list:

- If MediaType = PLC and LQI < JoinLQIThreshold_PLC, the entry is removed
- If MediaType = RF and LQI < JoinLQIThreshold_RF, the entry is removed

If the neighbour discovery returns an empty list, the meter waits a random time between 0 and AssociationRandWaitTime seconds before executing another neighbour discovery.

Step 2: Selection of G3 network to join

The selection of the network(s) to join is done in two steps:

1. Ranking G3 networks: The goal is to prioritise joining a G3 network accessible by PLC with good signal, reducing the risk of selecting a PLC network only accessible by signal crosstalk or a distant RF network (without PLC connexion).
2. Selecting the best G3 neighbour: The goal is to select the neighbour providing the best network connectivity toward its PAN-Coordinator, using the route-cost formula.

First, computes an ordered list of network PAN-IDs (better first):

- Using neighbour discovery entries with MediaType = PLC, sort by decreasing LQI (higher LQI value is better) to create an ordered list of PAN-IDs
- If no entry with MediaType = PLC exists, use the entries with MediaType = RF and sort by decreasing LQI to create the list of PAN-IDs
- If AssociationAltPAN is set to FALSE, only keep the first PAN-ID of the list. This limits the registration attempts to a single network for each procedure.

Second, determine the best neighbour to contact for each selected PAN, using the route-cost formula (lower is better). For each neighbour discovery entry:

- If the entry PAN-ID is not in the network PAN-ID list, skip this entry.
- Compute RC_NEIGHBOUR = route-cost between the meter and the neighbour, using the measured LQI and the route-cost formula corresponding to the MediaType value
- Compute RC_TOTAL = RC_COORD + RC_NEIGHBOUR
- For each PAN-ID in the network PAN-ID list, select the neighbour entry with the lower RC_TOTAL value

The result of this selection algorithm is a list of neighbour devices, one for each discovered G3 network, ordered with the best network first.

Step 3: Bootstrap procedure

For each entry in the list from step 2, following the list ordering:

1. Set a variable nbAttempts = 0
2. The meter tries to join the PAN by calling ADPM-NETWORK-JOIN, targeting the selected neighbour device as a bootstrapping relay
3. If the ADPM-NETWORK-JOIN fails, increment nbAttempts by 1:
    a. If nbAttempts < AssociationMaxRetry, wait a random time between 0 and (nbAttempts * AssociationRandWaitTime) seconds, then retry ADPM-NETWORK-JOIN on the same PAN-ID + neighbour
    b. Otherwise set nbAttempts = 0 and try the next entry in the list

If no bootstrap succeeded after trying all the PAN-ID in the list, the meter waits a random time between 0 and AssociationRandWaitTime seconds before executing another neighbour discovery

Once the bootstrap is completed successfully, if the attribute adpDefaultCoordRouteEnabled is set to TRUE, then a route discovery with the unicast RREQ flag set to TRUE is issued by the PAN Device to install the route to the PAN Coordinator.

The COSEM object ADPLBPAssociationSetup (0-0:94.43.14.255) contains the parameters defined in this chapter:

Table 3: Initialization and bootstrapping parameters

Parameter	Description
ActiveScanDuration	This attribute specifies the duration in seconds of the active scan. It is recommended that this attribute is greater than mac_beacon_randomization_window_length.
AssociationMaxRetry	This attribute indicates the maximum number of associations retries carried out for one PAN.
AssociationRandWaitTime	This attribute indicates the waiting window time step in minutes between two associations retries for the same PAN.
AssociationAltPAN	This attribute indicates whether the device tries to join an alternate PAN after reaching Association_max_retry retries.
JoinLQIThreshold	This attribute specifies the LQI threshold value to be used for LBA and PAN selection.

E. Timeout and Keep-Alive mechanisms

A G3 timeout is defined that disconnect a PAN Device if it has not been individually addressed by the PAN Coordinator in PLCG3TimeOut minutes.

Any Path Discovery messages (6loWPAN layer), ICMP Echo Request or ICMP Echo Reply (IPv6 layer) or unicast DLMS/COSEM APDU sent by the PAN Coordinator in unicast to this PAN Device shall reset the timeout.

If PLCG3TimeOut is set to 0, this G3 timeout mechanism is disabled.

A complementary Keep-Alive mechanism allows the PAN Device to maintain the device's association with the PAN Coordinator autonomously.

When the G3 timeout reaches KeepAliveStartTime minutes since the last reset, the PAN Device starts sending ICMP Echo requests intended for the PAN coordinator every KeepAliveSendPeriod minutes.

The Keep-Alive mechanism can be disabled by setting KeepAliveEnable to FALSE.

The following table provides a description of the parameters defined in this chapter:
The COSEM objects PLCG3TimeOut (0-0:94.43.10.255) and PLCG3KeepAlive (0-0:94.43.11.255) contains the parameters defined in this chapter:

Table 4: Timeout and KeepAlive parameters

Parameter	Description
PLCG3TimeOut	This data defines the time, in minutes, after which a meter that has not been individually addressed (meaning the meter has not received any Path Discovery message, ICMP ping, nor unicast DLMS APDU) returns to the non-associated state and loses its PAN coordinator. A value equal to 0 is equivalent to cancel the use of the related time-out-not-addressed counter.
KeepAliveEnable	This parameter indicates whether the keep alive mechanism is enabled or not.
KeepAliveStartTime	This parameter indicates the time in minutes to wait before starting the periodic emission of ICMP Echo requests.
KeepAliveSendPeriod	This parameter indicates the time in minutes between two successive keep alive ICMP Echo requests.

F. DLMS/COSEM Communication Profiles and Services

F.1 UDP/IP Profile

The DLMS COSEM application connects to the TCP/IP or UDP/IP layer using and additional sublayer called the DLMS/COSEM wrapper.

The UDP/IP channel is configured and managed via the following COSEM objects:

Table 5: UDP/IP objects

Object / Attribute Name	Class	Ver.	OBIS code
TCP-UDP setup	41	0	0-0:25.0.0.255
IPv6 setup	48	0	0-0:25.7.0.255

The UDP client port number used by the “COSEM Client Application Layer” shall be set between 61617 (0xF0B1) and 61631 (0xF0BF).

The UDP server port number used by the “COSEM Server Application Layer” shall be set to 61616 (0xF0B0).

The following table summarizes the valid UDP port numbers for the DLMS/COSEM metering application:

Table 6: UDP port numbers for DLMS COSEM metering application

Application	Server UDP ports Ports applying for packets emitted by the server to the client		Client UDP ports Ports applying for packets emitted by the client to the server	
	Source	Destination	Source	Destination
DLMS/COSEM	61616	61617 - 61629	61617 - 61629	61616

All but Data-Notification Service				
DLMS/COSEM Data-Notification Service	61616	61631	N/A	N/A

Other port numbers are reserved for future services

F.2 G3 Interface Setup

The G3 channel is configured and managed via the following COSEM objects:

Table 7: G3 channel configuration objects

Object / Attribute Name	Class	Ver.	OBIS code
MAC address setup	43	0	0-0:25.2.0.255
G3-PLC MAC layer counters	90	1	0-0:29.0.0.255
G3-PLC MAC setup	91	4	0-0:29.1.0.255
G3-PLC 6LoWPAN adaptation layer setup	92	4	0-0:29.2.0.255
G3-PLC MAC Hybrid RF MAC layer counters	160	0	0-0:29.3.0.255
G3-PLC MAC Hybrid RF MAC setup	161	1	0-0:29.4.0.255
G3-PLC Hybrid 6LoWPAN adaptation layer setup	162	1	0-0:29.5.0.255

MAC address setup

The MAC address setup holds the EUI-64 address of the PLC G3 Modem.

G3-PLC MAC layer counters

This object stores the counters relating to exchanges between PHY and MAC. The purpose of these counters is to provide statistical information for maintenance. When a counter reaches its maximum value (0xFFFFFFFF), it is automatically reset.

G3-PLC MAC setup

This object holds the necessary parameters to set up the MAC IEEE 802.15.4 sub-layer and provides access to information settings and tables that might be necessary for the network management.

G3-PLC 6LoWPAN adaptation layer setup

This object holds the necessary parameters to set up the 6LoWPAN adaptation sub-layer and provides access to information settings and tables that might be necessary for the network management.

The attribute adp_routing_configuration contained in the G3-PLC 6LoWPAN adaptation layer setup defines all parameters associated with the routing mechanism described in ITU-T G.9903:2017, ITU-T G.9903 Amd. 1:2021, ITU-T G.9903 Cor. 1:2023, and ITU-T G.9903 Amd. 2:2023. These elements are specified in section 9.4.1.2 of this Recommendation.

G3-PLC MAC Hybrid RF MAC layer counters

This object stores the counters relating to exchanges between PHY and MAC. The purpose of these counters is to provide statistical information for maintenance. When a counter reaches its maximum value (0xFFFFFFFF), it is automatically reset.

G3-PLC MAC Hybrid RF MAC setup

This object holds the necessary parameters to set up the MAC IEEE 802.15.4 RF sub-layer and provides access to information settings and tables that might be necessary for the network management.

G3-PLC Hybrid 6LoWPAN adaptation layer setup

This object holds the necessary parameters to set up the G3-Hybriod 6LoWPAN adaptation sub-layer and provides access to information settings and tables that might be necessary for the network management. The attribute `adp_routing_configuration_RF` contained in the G3-PLC Hybrid RF 6LoWPAN adaptation layer setup defines all parameters associated with the routing mechanism described in ITU-T G.9903:2017, ITU-T G.9903 Amd. 1:2021, ITU-T G.9903 Cor. 1:2023, and ITU-T G.9903 Amd. 2:2023. The elements are specified in section H.8.1 of this Recommendation.

F.3 G3 Interface Setup – Pending/Backup

The G3 interface objects (G3-PLC MAC setup, G3-PLC 6LoWPAN, G3-PLC MAC Hybrid setup, G3-PLC Hybrid 6LoWPAN) are delivered with the default values listed in this document or with values specified by the network operator.

To optimize the PLC network, the objects can be modified remotely or locally.

Changes to or backups of the PLC communication parameters are configured and managed via the following COSEM objects:

Table 8: DLMS COSEM objects for PLC communication

Object / Attribute Name	Class	Ver.	OBIS code
G3-PLC MAC setup – pending	91	4	0-1:29.1.0.255
G3-PLC MAC setup – backup	91	4	0-2:29.1.0.255
G3-PLC MAC 6LoWPAN adaptation layer setup - pending	92	4	0-1:29.2.0.255
G3-PLC MAC 6LoWPAN adaptation layer setup - backup	92	4	0-2:29.2.0.255
G3-PLC MAC Hybrid RF MAC setup - pending	161	1	0-1:29.4.0.255
G3-PLC MAC Hybrid RF MAC setup - backup	161	1	0-2:29.4.0.255
G3-PLC Hybrid 6LoWPAN adaptation layer setup - pending	162	1	0-1:29.5.0.255
G3-PLC Hybrid 6LoWPAN adaptation layer setup - backup	162	1	0-2:29.5.0.255

F.4 G3 Network Management

The G3 PLC network requires some specific functions for establishing and maintaining connections to the PAN device.

These parameters are not described in the IDIS specification but are important for fine-tuning and maintaining the G3 PLC network.

The G3 network is configured and managed using the following COSEM objects:

Table 9: DLMS COSEM objects for G3 network configuration

Object / Attribute Name	Class	Ver.	OBIS code
Auto connect	29	2	0-0:2.1.0.255
PLCG3_Security Setup – to hold G3-PLC key and KEK	1	0	0-0:94.43.133.255
MacDeviceTable	1	0	0-0:94.43.13.255
MacDeviceTable_RF	1	0	0-0:94.43.14.255
MacCoherentTransmission	1	0	0-0:94.43.12.255
macSNRdBUseDiff8PSK	1	0	0-0:94.43.13.255
InitiatorElectricalPhase	1	0	0-0:96.62.0.255
DeltaElectricalPhase	1	0	0-0:96.62.1.255
AlternatePANId	1	0	0-0:94.43.55.255
AlternatePANIdLog	7	1	0-0:94.43.9.255
PAN connection status	1	0	0-0:94.43.131.255
PAN connection status profile	7	1	0-0:94.43.132.255
PLCG3_Bandplan	1	0	0-0:94.43.128.255

Auto connect

The network connectivity of the meter is controlled by the auto connect object.

The following auto connect mode is supported:

- (101) The meter is permanently connected to the IP network and can be reached by the HES via its known IP address

PLCG3_Security Setup – to hold G3-PLC key and KEK

This object allows changing the PSK (128 bits / 16 octets) and PSK Key Encryption Key (128 bits / 16 octets) of the meter.

The new PSK is wrapped by the AES-128 key wrap algorithm, using the dedicated PSK KEK as the wrapping key. On writing, the wrapped PSK integrity is validated. If the integrity check fails, the write access is refused and the PSK is not modified

The new PSK_KEK is wrapped by the AES-128 key wrap algorithm, using the current PSK_KEK as the wrapping key. On writing, the wrapped PSK_KEK integrity is validated. If the integrity check fails, the write access is refused and the PSK_KEK is not modified.

Reading the object value is not allowed.

After the successful change of the PSK (confirmation to the DLMS client), the meter returns to the non-associated state and re-starts its joining process for the reconnection to the PAN coordinator.

MacDeviceTable

This object describes a table of Device-Descriptor entries, for frames received over PLC.

MacDeviceTable_RF

This object describes a table of Device-Descriptor entries, for frames received over RF.

MacCoherentTransmission

This object indicates the coherent modulation scheme to set in the tone map response.

macSNRdBUseDiff8PSK

This object indicates the number of dB with respect to the macSNRdBD8PSK threshold to force the tone map algorithm to ask for differential scheme - part of mac coherent transmission

InitiatorElectricalPhase

This object indicates the phase number to which the client system is connected.

DeltaElectricalPhase

This object indicates the phase difference between the client system's connecting phase and the meter's connecting phase.

AlternatePANid

This object stores the detected PANid for capturing into the AlternatePANIdLog

The data contains the alternate PAN Id that has been indicated by the MLME-COMM-STATUS.indication with Status = ALTERNATE_PANID_DETECTION received from the PLC MAC layer.

Only G3 neighbouring networks detected by PLC crosstalk are captured by this object.

Detection of G3 neighbouring networks over radio is normal during G3 operation, so they should not be logged.

AlternatePANid log

This object logs the « alternate PAN Id » detected by the meter.

Everytime the MLME-COMM-STATUS.indication primitive is called with Status = ALTERNATE_PANID_DETECTION, the meter checks if there is already an entry with the same PAN-ID in the buffer:

- If it is the case, this entry is updated with the current date & time and moved to the end of the buffer (i.e. it becomes the latest element of the array).
- If not, a new entry is added with the alternate PAN-Id value and the current date and time.

When the buffer is full, the oldest entry is deleted to allow the storage of a new entry.

PAN connection status

This object contains the network status information for the connection of the end device to the PAN coordinator.

The connection status information is based on the:

- Routing table entry of the ‘PAN coordinator’ and
- Neighbour table entry of the ‘Next Hop’

If an entry is missing or not valid, the valid_time (routing entry) or neighbour_valid_time (neighbor entry) fields is set to 0, the values for other fields are undefined.

PAN connection status profile

This object allows monitoring the network status for the connection of the end device to the PAN coordinator by recoding the PAN connection status in a regular interval.

PLCG3_Bandplan

This object allows the identification of the current bandplan in use.

The supported bandplans are:
0 = Only CENELEC-A band
3 = Only FCC band

Switching between CENELC-A and FCC band must be possible by configuration change.

This object shall be declared as readable and writable and allows changing the current bandplan in use.

Oesterreichs Energie Companion Standard
Smart Meter 2.0

D.3_OE_CS_Implementation_Guide_Mobilfunk

Version 1.0

31.03.2026

Inhaltsverzeichnis

A. Einleitung 5

A.1 Ziel und Zweck des Dokuments 5

A.2 Normative Referenzen 5

B. Beschreibung WAN Interface – G1 5

C. Technische Spezifikation 6

C.1 Schnittstelle Kommunikationsmodul – Zähler und Modularität 6

C.2 Unterstützte Kommunikationstechnologien und Mobilfunkstandards 6

C.3 Unterstützung Coverage Enhancement Levels/Mode 7

C.4 Unterstützte Frequenzbänder 7

C.5 Interne Antenne 8

C.6 Externer Antennenanschluss 8

C.7 Automatische Umschaltung externe Antenne 8

C.8 Dual SIM 9

C.9 Powerclass 9

C.10 Empfindlichkeit des Geräts 9

C.11 Unterstützung Control Plane-Optimierung für NB-IoT 9

C.12 Unterstützung IP-Protokollstapel für User Plane CIoT Optimierung 9

C.13 Vermeidung von unnötiger Signalisierungslast 9

C.14 Verwendung von Zufallsalgorithmus beim Verbindungsaufbau 10

C.15 Unterstützung eUICC Anforderungen 10

D. Modem related Object 10

D.1 PHY Randomization 10

D.2 Auto connect 11

D.3 MAC address setup 11

D.4 GPRS modem setup 11

D.5 GSM diagnostic 11

D.6 LTE monitoring 13

D.7 Pegeltabellen und –referenzen 15

D.8 Network Information 18

D.9 Periodic Ping Configuration 19

D.10 Average RTT 18

D.11 Number Packets Received 18

D.12 Network Condition Profile 18

D.13 Telecom CATM-NBIOT switch threshold 19

D.14 Telecom CAT-M switch threshold 19

D.15 Inter Radio Access Network Technology (IRAT) – Timer 19

E. Communication related EVENTS 20

E.1 Communication Events 19

E.2 Mobile Radio Attach Event Codes 20

E.3 Mobile Radio Attach Event Codes Log 21

E.4 PDP Context Error 21

E.5 PDP Context Error Log 22

F. Firmware Upgrade Mobile Radio modems 22

F.1 Firmware related Events 22

G. Mobile Radio Communications parameter 22

Versionsverlauf

Version	Bezeichnung	Datum	Autor
1.0	Initiales Release	31.03.2026	OE Companion Standard AG Kommunikation

A. Einleitung

A.1 Ziel und Zweck des Dokuments

Ziel dieses Dokuments ist die Sicherstellung der Interoperabilität der Smart Meter 2.0 mit Mobilfunkmodul und den Zentralen Systemen der Netzbetreiber.

Dazu werden in diesem Dokument folgende Aspekte definiert

- Zu unterstützende Mobilfunktechnologien
- Notwendige Zählerfunktionen
- Erläuterungen zum Objektmodell Siehe Dokument „D.1_OE_CS_Objektmodell.xlxs“
- Zu überwachende Events und Alarme

Detaillierte Beschreibungen der in diesem Dokument gesammelten Funktionen sind in den jeweils genannten Dokumenten zu finden. Eine vollständige Liste der referenzierten Dokumente findet sich in „A.1_OE_CS_Gesetze_Normen_und_Standards.pdf“.

A.2 Normative Referenzen

Eine Auflistung sämtlicher gesetzlicher Vorgaben, Standards und Normen ist im Dokument „A.1_ OE_CS_Gesetze_Normen_und_Standards.pdf“ zu finden.

B. Beschreibung WAN Interface – G1

Das Mobilfunk Kommunikationsmodul dient als Verbindung zwischen dem Smart Meter und den Zentralen Systemen, indem es einen IP-basierten Kommunikationspfad über die G1- Schnittstelle zur Verfügung stellt. Netzwerkseitig ist das Kommunikationsmodul für eine stabile und verlässliche Verbindung zu den Zentralen Systemen zuständig.

Die folgende *Abbildung 1: Grundbausteine des Smart Meters* zeigt eine schematische Darstellung der grundlegenden Zählerfunktionen und dient einer besseren Übersicht über die oben beschriebene Schnittstelle G1. Die aktuelle und gültige Version ist dem Dokument „B.3_ Anhang_Schnittstellen_Details.pdf“ zu entnehmen.

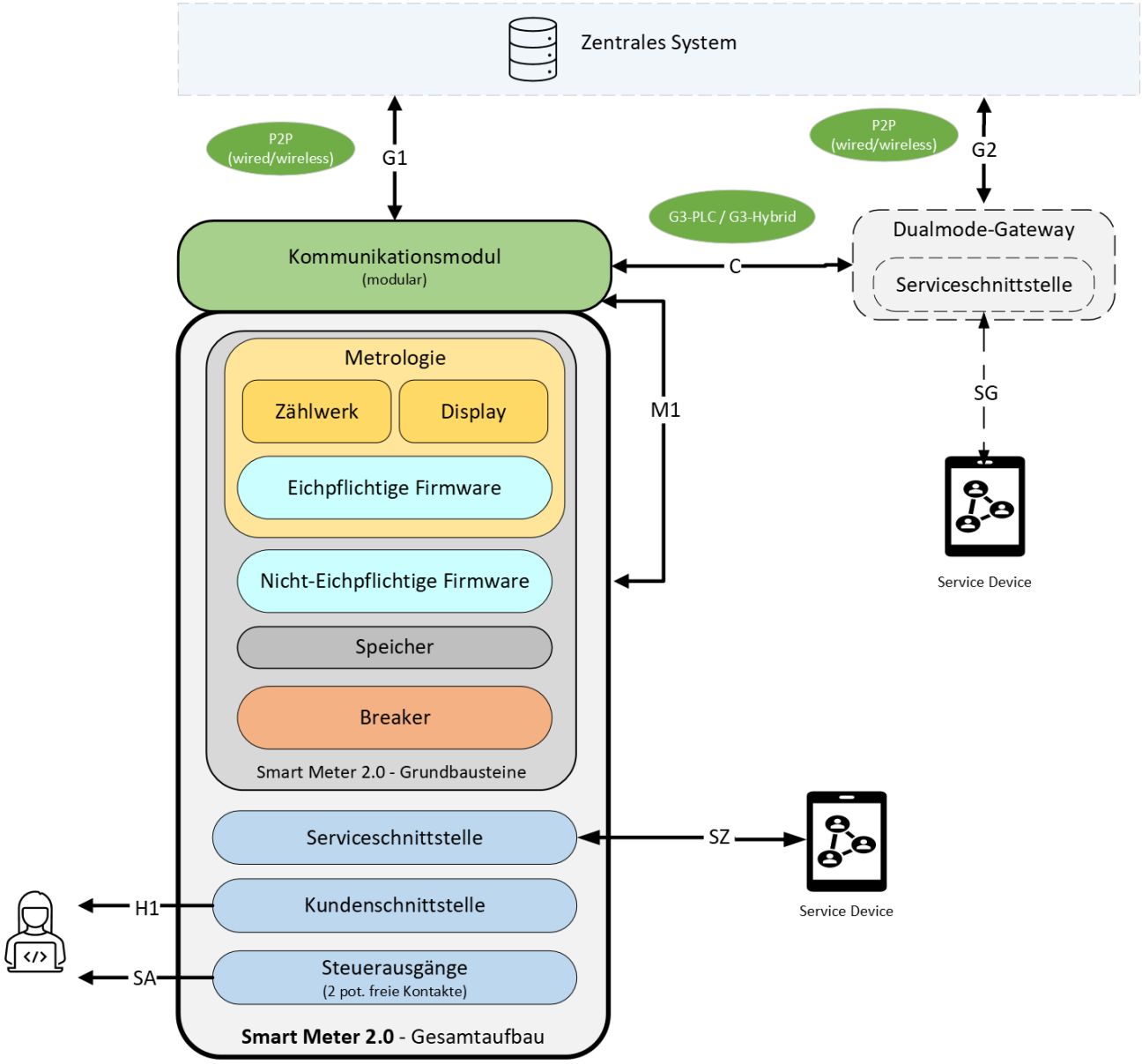


Abbildung 1: Grundbausteine des Smart Meters

C. Technische Spezifikation

C.1 Schnittstelle Kommunikationsmodul – Zähler und Modularität

Der Kommunikationsteil für Mobilfunk muss modular ausgeführt sein. Eine genaue Beschreibung der Funktionalität befindet sich im Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“.

C.2 Unterstützte Kommunikationstechnologien und Mobilfunkstandards

Das Mobilfunkmodul muss die Mobilfunktechnologien entsprechend dem Dokument „B.3_ Anhang_Schnittstellen_Details.pdf“ unterstützen.

Mindestanforderung ist die Unterstützung der folgenden Technologien:

- LTE-M (UE Cat.M1)

- LTE NB-IoT (UE Cat.NB2)
- LTE (UE Cat.1bis)
- LTE (UE CAT.1)

Zukünftige Technologien:

- LTE-M (UE Cat.M2) muss unterstützt werden, sobald ausreichend Verfügbarkeit gegeben ist.

Die Unterstützung mehrerer Technologien in einem Modul ist zulässig.

Die Übertragungstechnologien müssen 3GPP konform umgesetzt werden. Mindestanforderung ist die Umsetzung von 3GPP Release 14. Funktionen, die eine andere Mindestrelease erfordern sind bei Bedarf in den folgenden Beschreibungen enthalten. Auf jeden Fall muss der Hersteller für jede Funktion die von ihm implementierte Release angeben.

C.3 Unterstützung Coverage Enhancement Levels/Mode

Das Kommunikationsmodul muss alle definierten Level zur Verbesserung der Abdeckung sowohl für LTE Cat-M als auch für NB-IoT-Technologien unterstützen. Die Umsetzung muss laut 3GPP TS 36.331, TS 36.306, TS 36.321 und mindestens Release 14 konform ausgeführt werden.

- für LTE-M (UE Cat.M1) :
  CE Mode A
  CE Mode B (optional)
- für NB-IoT: CE Levels 0, 1 und 2

C.4 Unterstützte Frequenzbänder

Es müssen Module zur Verfügung gestellt werden, die zumindest die folgenden Frequenzbänder unterstützen:

LTE Band	NR- Band	Frequenz
72		450 MHz
28	n28	700 MHz
20	n20	800 MHz
8	n8	900 MHz
3	n3	1800 MHz
1	n1	2100 MHz

C.5 Interne Antenne

Das Modul muss über eine interne Antenne verfügen, welche eine Anpassung für die geforderten Frequenzbänder hat. Die interne Antennenanpassung muss für die geforderten Frequenzbänder einen VSWR kleiner 2 besitzen. Die interne Antenne muss so verbaut sein, dass sie gegen Manipulation geschützt ist.

Die Effizienz der integrierten Antenne muss für den Uplink-Bereich jedes geforderten Frequenzbandes zumindest 40% betragen.

LTE Band	Antennen Effizienz in %	Antennen Effizienz in dB	Uplink Frequenz
72	>= 40	>= -4	451,3 - 455,74 MHz
28	>= 40	>= -4	694 - 738 MHz
20	>= 40	>= -4	832 - 862 MHz
8	>= 40	>= -4	880 - 915 MHz
3	>= 40	>= -4	1710 - 1785 MHz
1	>= 40	>= -4	1920 - 1980 MHz

C.6 Externer Antennenanschluss

Der Anschluss einer externen Antenne muss möglich sein. Dazu sind Standardbuchsen (z.B. SMA-F oder MCX-F vorzusehen. Die Antenne muss ohne zusätzliche Komponenten, wie zum Beispiel einem Antennenkoppler, anschließbar sein.

C.7 Automatische Umschaltung externe Antenne

Das Kommunikationsmodul muss den Anschluss einer externen Antenne eigenständig erkennen und automatisch auf den externen Anschluss umschalten, ohne dass der Auftraggeber eine Parameteränderung durchführen muss. Falls die externe Antenne wieder entfernt wird, muss dies ebenso vom Kommunikationsmodul eigenständig erkannt und wieder auf die interne Antenne umgeschaltet werden, ohne dass der Auftraggeber eine Parameteränderung durchführen muss.

Die HF- Eigenschaften zwischen internen und externen Antennenanschluss müssen mindestens den Parametern der unten angeführten Tabelle entsprechen.

Parameter	Values			Unit	Notes
	Min.	Typ.	Max		
Insertion Loss					
	-	-	0,5	**dB**	451- 960 MHz
	-	-	0,5	**dB**	1710 – 2170 MHz
Return Loss					
	20	-	-	**dB**	451- 960 MHz
	15	-	-	**dB**	1710 – 2170 MHz
Isolation					

Interne zu Externe Antenne	35	40	-	**dB**	451- 960 MHz
	30	35	-	**dB**	1710 – 2170 MHz

C.8 Dual SIM

Das Kommunikationsmodul muss die Möglichkeit bieten eine austauschbare SIM-Karte (2FF) und/oder eine verlötete eSIM-Karte aufzunehmen.

Es muss sichergestellt werden, dass die SIM Karte nur durch Befugte getauscht werden kann.

Das Kommunikationsmodul muss UICC und eUICC SIM-Karten unterstützen.

C.9 Powerclass

Die RF-Ausgangsleistung des Kommunikationsmoduls muss der Power Class 3 (gemäß ETSI TS 36.101) entsprechen. Für LTE-M im Band 72 muss zusätzlich die Power Class 2 (gemäß ETSI TS 36.101) unterstützt werden.

Technologie	Band 72	sonstige Bänder
LTE	+23dBm	+23dBm
LTE-M	+26dBm	+23dBm
NB-IoT	+23dBm	+23dBm

C.10 Empfindlichkeit des Geräts

Das Kommunikationsmodul muss in der Lage sein, eine Verbindung mit einer definierten Mindestsignalstärke (gemäß 3GPP TS 36.101) aufzubauen. Um eine ausreichende Abdeckung zu erreichen, muss die tatsächliche Empfindlichkeit des Zählers (als Ganzes) mindestens die folgenden Anforderungen erfüllen:

LTE-M: RSRP mindestens -115 dBm

NB-IoT: NRSRP mindestens -125 dBm

LTE Cat1bis: RSRP mindestens -105 dBm

Diese Werte stellen die unterste garantierte Empfangsschwelle dar, bei der das Gerät noch eine Verbindung aufbauen und die in 3GPP TS 36.101 spezifizierte Performance (z. B. BLER ≤ 10 %) einhalten muss.

C.11 Unterstützung Control Plane-Optimierung für NB-IoT

Das Kommunikationsmodul muss die Control Plane CIoT-Optimierungen entsprechend 3GPP TS 24.301 (ab Rel. 13) unterstützen.

C.12 Unterstützung IP-Protokollstapel für User Plane CIoT Optimierung

Das Kommunikationsmodul muss User Plane CIoT-Optimierungen gemäß 3GPP TS 24.301 (ab Rel. 13) unterstützen.

C.13 Vermeidung von unnötiger Signalisierungslast

Das Kommunikationsmodul darf keine unnötige Signalisierungslast durch falsche Behandlung von Netzrückweisungsursachen verursachen, um die Betriebsfähigkeit wiederzuerlangen, da es weiter zu einer Netzüberlastung beitragen und die Dienstverfügbarkeit auch für Smart-Meter-Zwecke verringern würde. Dazu müssen die jeweils aktuellen best practice Konzepte der GSMA laut “TS.34 IoT Device Connection Efficiency Guidelines” eingehalten und umgesetzt werden zusätzlich zu den Anforderungen aus 3GPP TS 24.301.

C.14 Verwendung von Zufallsalgorithmus beim Verbindungsaufbau

Der Zähler muss in der Lage sein, sich nach Kommunikationsproblemen automatisch zu erholen, indem er einen Zufallsalgorithmus verwendet, um die PDN-Verbindung wiederherzustellen. Um zu verhindern, dass viele getrennte Zähler gleichzeitig eine PDN-Verbindung wiederherstellen, müssen die jeweils aktuellen best practice Konzepte der GSMA laut “TS.34 IoT Device Connection Efficiency Guidelines” eingehalten und umgesetzt werden.

C.15 Unterstützung eUICC Anforderungen

Der Zähler muss alle Anforderungen der GSMA SGP.31 und GSMA SGP.32 Spezifikationen erfüllen.

D. Modem related Objects

D.1 PHY randomization

Um die Überlastung von Mobilfunknetzen durch gleichzeitiges Anmelden vieler Zähler (zum Beispiel nach einem Stromausfall) zu verhindern, muss ein Anmeldungsmechanismus entsprechend “GSMA TS.34 - IoT Device Connection Efficiency Guidelines” genutzt werden. Ein beispielhafter Anmeldemechanismus ist in diesem Dokument beschrieben und in einem Flow-Diagramm dargestellt. Der konkrete Mechanismus muss von jedem Hersteller mittels Flow- Diagramm dargestellt und zur Verfügung gestellt werden. Der Anmeldemechanismus muss mit den in der folgenden Tabelle dargestellten Werten über das Objekt “PHY randomization” einstellbar sein.

Parameter name Datentyp	**Erklärung**
randomisation_start_window double-long-unsigned	In Sekunden. Ein Zeitfenster von 0 bedeutet keine Randomisierung. Der Anmeldeprozess startet sofort. Der Zähler wählt zufällig einen Zeitpunkt innerhalb des Zeitfensters. Innerhalb eines Zeitfensters wird ein Anmeldeversuch unternommen. Min. 1, Max. 65535
multiplication_factor long-unsigned	Im Falle einer nicht erfolgreichen WAN Registrierung wird ein neues Zeitfenster durch multiplikation mit diesem Wert errechnet. Min. 1, Max. 7
number_of_retries long-unsigned	Gibt die Anzahl der Anmeldeversuche an. Jeder Anmeldeversuch hat ein um “multiplication_factor” vervielfachtes “randomisation_start_window“. Wenn diese Anzahl erreicht wurde, wird das Modem neu gestartet und der gesamte Anmeldeprozess startet erneut.

	Min. 1, Max. 7
direct_attach_at_power_on_flag Boolean	Wenn diese Flag gesetzt (Wert = 1) ist, verbindet sich das Kommunikationsmodul sofort mit dem Mobilfunknetz. 0: Not Set 1: Set

Der Smart Meter muss in der Lage sein zu erkennen, dass das Kommunikationsmodul aufgrund von netzbedingten Problemen oder unterbrochener Verbindungen beeinträchtigt ist und die erforderlichen Schritte unternehmen, um den Normalbetrieb ohne Eingreifen des Zentralen Systems wiederherzustellen. Dies erfolgt über einen implementierten Modem-Reset-Mechanismus, der dem Ausschalten und erneutem Einschalten der Stromversorgung des Kommunikationsmoduls entspricht. Der Smart Meter überwacht ständig den RSSI-Wert, den Netzwerkregistrierungsstatus und den PDP-Kontext. Sobald ein Problem erkannt wird, schaltet das Messgerät das Modem aus und startet die Warteprozedur namens PHY-Randomisierung. Während dieser Prozedur wartet das Messgerät eine zufällige Zeitspanne, bevor es das Modem wieder einschaltet und erneut eine Verbindung zum Netzwerk herstellt. Die PHY-Randomisierung- Prozedur kann die Wahrscheinlichkeit einer Netzüberlastung erheblich verringern, insbesondere im Falle eines großflächigen Netzausfalls, wenn Tausende von Modems gleichzeitig versuchen, sich wieder mit dem Netzwerk zu verbinden.

D.2 Auto connect

Zur Konfiguration des Verbindungsverhaltens des Mobilfunkmoduls muss die Klasse “Auto connect” entsprechend DLMS Blue Book konform umgesetzt werden. Die Attribute sind im DLMS Blue Book beschrieben.

D.3 GPRS modem setup

Um Grundlegende Verbindungsparamter einstellen zu können muss die Objektklasse “GPRS modem setup” entsprechend DLMS Blue Book konform umgesetzt werden. Die Attribute und Methoden sind im DLMS Blue Book beschrieben.

D.4 GSM diagnostic

Zur Analyse von Mobilfunkinformationen muss das Objekt “GSM diagnostics” gemäß DLMS Blue Book umgesetzt werden. Die folgende Tabelle fasst die wesentlichen Attribute entsprechend DLMS Blue Book zusammen.

Attribut	Beschreibung	Mögliche Werte
status	Indicates the registration status of the modem.	(0) not registered, (1) registered, home network, (2) not registered, but MT is currently searching a new operator to register to, (3) registration denied, (4) unknown, (5) registered, roaming, (6)... (255) reserved

cs_attachment	Indicates the current circuit switched status.	enum: (0) inactive, (1) incoming call, (2) active, (3)...(255) reserved
ps_status		(0) inactive, (1) GPRS, (2) EDGE, (3) UMTS, (4) HSDPA, (5) LTE, (6) CDMA, (7) LTE Cat M1, (8) LTE Cat NB1, (9) LTE Cat NB2, (10)...(255) reserved

cell_info	Represents the cell information:
	
	cell_info_type ::= structure
	{
	cell_ID: double-long-unsigned,
	location_ID: long-unsigned,
	signal_quality: unsigned,
	ber: unsigned,
	mcc: long-unsigned,
	mnc: long-unsigned,
	channel_number: double-long-unsigned
	}
		cell_ID: Four-byte cell ID in hexadecimal format;
		
		location_ID: Two-byte location area code (LAC) in the case of GSM networks or Tracking Area Code (TAC) in the case of UMTS, CDMA or LTE networks in hexadecimal format (e.g. "00C3" equals 195 in decimal);
		
		signal_quality: Represents the signal quality:
		(0) –113 dBm or less,
		(1) –111 dBm,
		(2...30) –109…-53 dBm,
		(31) –51 or greater,
		(99) not known or not detectable
		
		ber: Bit Error Rate (BER) measurement in percent:
		(0…7) as RXQUAL_n values specified in ETSI GSM 05.08:1996, 8.2.4
		(99) not known or not detectable.

		mcc: Mobile Country Code of the serving network, as defined in ITU-T E.212 (05.2008) SERIES E; **mnc**: Mobile Network Code of the serving network, as defined in ITU-T E.212 (05.2008) SERIES E; **channel_number:** Represents the absolute radio-frequency channel number (ARFCN or EARFCN for LTE network).

D.5 LTE monitoring

Für erweitertes Monitoring von LTE-Netzen muss dieses Objekt entsprechend DLMS Blue Book, umgesetzt werden. Wesentliche Attribute sind hier entsprechend DLMS Blue Book angeführt und weiterführende Dokumente referenziert.

Attribut	Beschreibung	Mögliche Werte
LTE_network_parameters	Represents the network parameters for the LTE network LTE_network_parameters_type ::= structure { T3402: long-unsigned, T3412: long-unsigned, T3412ext2: double-long-unsigned, T3324 long-unsigned, TeDRX double-long unsigned, TPTW long-unsigned, qRxlevMin: integer, qRxlevMinCE-r13: integer,	- T3402 timer in seconds, used on PLMN selection procedure and sent by the network to the modem. Refer to 3GPP TS 24.301 V13.4.0 (2016-01) for details. - T3412 timer in seconds, used to manage the periodic tracking area updating procedure and sent by the network to the modem. Refer to 3GPP TS 24.301 V13.4.0 (2016-01) for details. -T3412ext2 timer in seconds (extended periodic tracking area update timer). Refer to 3GPP TS 24.301 V13.4.0 (2016-01) and

	qRxlevMinCE1-r13 integer }	3GPP TS 24.008 V13.7.0 (2016-10) for details. - T3324 timer in seconds (Power saving mode active timer). Refer to 3GPP TS 24.301 V13.4.0 (2016-01) and 3GPP TS 24.008 V13.7.0 (2016-10) for details. - TeDRX timer (Extended Idle mode DRX cycle timer). Refer to 3GPP TS 24.301 V13.4.0 (2016-01) and 3GPP TS 24.008 V13.7.0 (2016-10) for details. The double-long unsigned value shall be multiplied by 0,01 to get the real value in seconds. E.g. 512 represents 5,12 seconds - TPTW timer (Extended Idle mode DRX paging time window). Refer to 3GPP TS 24.301 V13.4.0 (2016-01) and 3GPP TS 24.008 V13.7.0 (2016-10) for details. The long unsigned value shall be multiplied by 0,01 to get the real value in seconds. E.g. 512 represents 5,12 seconds - qRxlevMin the minimum required Rx level in the cell in dBm as defined in 3GPP TS 36.304 V13.8.0 (2018-01). qRxlevMinCE-r13 the minimum required Rx level in enhanced coverage CE Mode A, LTE Cat M1. For this mode a value from -70…-22 in steps of 1 is required.

		NOTE 1 This field is not used in case of LTE Cat NB1 or NB2. - qRxlevMinCE1-r13 the minimum required Rx level in enhanced coverage CE Mode B, LTE Cat M1. For this mode a value from -78…-22 in steps of 1.

LTE_quality_of_service	Represents the quality of service of the LTE network
	
	The convertion tables for Signal strength etc. origin from the mentioned 3GPP documents. For further details refer to them.
	
	LTE_QoS_type ::= structure
	
	{
	(N)RSRQ: integer,
	(N)RSRP: integer,
	SNR: integer,
	Coverage Enhancement: enum
	}
		Die Umrechnungstabellen für (N)RSRSQ, (N)RSRP und SNR finden sich im nächsten Absatz und den folgenden Seiten

Im Mobilfunk kommen unterschiedliche Messwerte zur Beurteilung der Signalqualität zum Einsatz. Im Folgenden werden diese Werte kurz beschrieben und auf die jeweiligen Grundlagen in den Mobilfunkstandards referenziert. Der Zähler und das Kommunikationsmodul müssen diese Werte entsprechend den Mobilfunkstandards erfassen und auslesbar in den Objekten zur Verfügung stellen.

Die mit dem “LTE_quality_of_service” erfassten Werte müssen den nachfolgenden Beschreibungen entsprechend in Abhängigkeit des ps_status korrekt erfasst werden.

D.5.1 (N)RSRQ Signalqualität

(N)RSRQ repräsentiert die Signalqualität wie in 3GPP TS 36.133 definiert. Die korrekte Zuordnung zur jeweiligen Tabelle erfolgt durch den Parameter *ps_status* aus dem Objekt *GSM diagnostic.*

Für LTE Cat M1 (*ps_status* = *7*), ist eine Range von -30 bis 46 notwendig um den RSRQ darzustellen. Detailliertere Informationen sind in 3GPP TS 36.133 zu finden.

Für LTE Cat NB1 und LTE Cat NB2 (*ps_status= 8 oder 9*) ist eine Range von -30 bis 46 notwendig um den NRSRQ abzubilden. Detailliertere Informationen sind in 3GPP TS 36.133 zu finden.

Integer-Wert	Entsprechender dB- Wert

(-30)	-34 dB,
(-29)	-33,5 dB,
(-28)..(-1)	-33 dB ... -19,5 dB,
(0)	-19,5 dB or less,
(1)	-19 dB,
(2)...(31)	-18,5 dB ... -4 dB,
(32)	-3.5 dB,
(33)	-3 dB,
(34)	-3 dB or less,
(35)	-2.5 dB,
(36)	-2 dB,
(37)...(45)	-1.5 dB ...+2.5 dB,
(46)	2.5 dB or better,
(99)	not known or not detectable,
other values	reserved

D.5.2 (N)RSRP Signalpegel

(N)RSRP ist der Signalpegel entsprechend 3GPP TS 36.133. Die korrekte Zuordnung zur jeweiligen Tabelle erfolgt durch den Parameter *ps_status* aus dem Objekt *GSM diagnostic.*

Für ps_status = 7 (LTE Cat M1) ist ein Wertebereich von -17 bis 97 ist notwendig um den RSRP entsprechend 3GPP TS 36.133 darzustellen.

Integer-Wert	Entsprechender dB- Wert
(-17)	-156 dBm,
(-16)	-155 dBm,
(-15)..(-1)	-154 dBm .. -140 dBm,
(0)	-140 dBm or less,
(1)	-139 dB,
(2)	-138 dBm,
(3)..(96)	-137 dBm .. -44 dBm,
(97)	-44 dBm or better,
(127)	not known or not detectable,
other values	reserved

HINWEIS: Abhängig von der Verwendung von Coverage-Enhancement-Modi wird ein gemeldeter Wert von (0) verwendet oder nicht (bei Geräten, die keine CE-Modi verwenden, werden die Werte (-17..-1) nicht verwendet). Ein gemeldeter Wert von (0) bedeutet in diesem Fall ein RSRP < -140 dBm.

Für ps_status = 8 oder 9 (LTE Cat NB1 oder NB2) ist ein Wertebereich von 0 bis 113 ist notwendig um den RSRP entsprechend 3GPP TS 36.133 darzustellen.

Integer-Wert	Entsprechender dB- Wert
(0)	-156 dBm,
(1)	-155 dBm,
(2)	-154 dBm

(3)..(112)	-153 dBm .. -44 dBm,
(113)	-44 dBm or better,
(127)	not known or not detectable,
other values	reserved

D.5.3 SNR Signal-Noise-Ration

Signal-Noise-Ration (= Signal-Rausch-Verhältnis) wird im Bereich von -20 dB bis 50 dB entsprechend 3GPP TS 36.101 dargestellt.

D.5.4 Coverage- Enhancement Modus

Coverage-Enhancement-Modus A oder B im Fall von LTE Cat M1, CE-Level 0, 1 oder 2 im Fall von LTE Cat NB1/NB2. Detailierte Beschreibungen befinden sich in 3GPP TS 36.331, 3GPP TS 36.321 und 3GPP TS 36.312

enum	LTE Cat M1	NB-IoT
(0)	CE Mode A	CE Level 0
(1)	CE Mode B	CE Level 1
(2)	(not used)	CE Level 2
other values	reserved	

D.6 Network Information

Zur Fehleranalyse in Mobilfunknetzen ist eine Objektklasse notwendig, welche bisher nicht im DLMS Blue Book erfasste Netzinfomationen erfasst. Eine genaue Klassenbeschreibung ist “D.1_OE_CS_Objektmodell.xlxs” zu entnehmen. Die zu erfassenden Informationen sind im Folgenden tabellarisch dargestellt:

Attribut	Beschreibung
IMSI	*International Mobile Subscriber Identity* – Eindeutige Kennung des Mobilfunkteilnehmers auf der SIM, vom Netz zur Identifikation verwendet.
IMEI	*International Mobile Equipment Identity* – Eindeutige Seriennummer eines Mobilgeräts (Hardware-ID).
MSISDN	*Mobile Station International Subscriber Directory Number* – Die eigentliche Rufnummer, unter der der Teilnehmer erreichbar ist.
ICCID	*Integrated Circuit Card Identifier* – Seriennummer der SIM-Karte selbst.
PCI	*Physical Cell ID* – Identifikationsnummer einer LTE/NR-Funkzelle zur Unterscheidung am Funkinterface.
EARFCN	*E-UTRA Absolute Radio Frequency Channel Number* – Nummer zur eindeutigen Identifikation des Frequenzkanals in LTE.
TAC	*Tracking Area Code* – Kennung eines geografischen Bereichs im Mobilfunknetz, in dem sich ein Gerät aufhalten kann, ohne sich neu registrieren zu müssen.

D.7 Network Condition Profile

Dieses Profil wird benötigt, um die Netzwerkqualität über einen bestimmten Zeitraum zu erfassen und so Probleme am Mobilfunknetz besser eingrenzen zu können.
Aufbau und Inhalt dieser Objektklasse sind im Dokument “D.1_OE_CS_Objektmodell.xlxs” detailliert beschrieben.

D.8 Periodic Ping Configuration

Durch die Konfiguration dieses Objekts muss ein regelmäßiger Ping an ein Zielsystem ermöglicht werden. Wenn der Smart Meter keine Ping Antwort erhält, muss das Event „ping_response_not_received“ ausgelöst werden.

D.9 Telecom CATM-NBIOT switch threshold

Wenn LTE NB-IoT als bevorzugte Technologie konfiguriert ist, wechselt das Modul automatisch zu Cat-M, wenn es für 5 Minuten unter dem konfigurierten RSRP-Schwellenwert bleibt.

D.10 Telecom CAT-M switch threshold

Wenn LTE Cat-M als bevorzugte Technologie konfiguriert ist, wechselt das Modul automatisch zu NB-IoT, wenn es für 5 Minuten unter dem konfigurierten RSRP-Schwellenwert bleibt.

D.11 Inter Radio Access Network Technology (IRAT) – Timer

Timer für den Wechsel von einer Technologie mit niedriger Priorität zu einer Technologie mit hoher Priorität. Wenn das Modul mit der RAT (Radio Access Technology) niedriger Priorität verbunden ist, versucht das Modul nach Ablauf des hier konfigurierten Timers zur RAT mit höherer Priorität zu wechseln.

E. Communication related Events

Die im Objektmodell definierten Kommunikationsevents müssen am Smart Meter erfasst werden. Eine vollständige Liste befindet sich in “D.1_OE_CS_Objektmodell.xlsx” im Arbeitsblatt Events. Für eine gezielte Fehlersuche muss der Smart Meter zusätzlich Netzwerk Attach-rejects und PDP Kontextfehler entsprechend den hier beschriebenen Objekten erfassen und abspeichern.

E.1 Mobile radio attach-reject code

Bei der Anmeldung an einem Mobilfunknetz kann es zu Fehlern kommen. Diese Fehler werden durch einen network attach reject-code vom Netzwerk begründet. Eine vollständige Liste der reject- causes sind in 3GPP TS 24.301 vom Kommunikationsmodul und dem Smart Meter erfasst und im Log E.2 “Mobile radio attach-code log” gespeichert werden. Wenn der Smart Meter einen attach-reject erhält muss das Event “241 P2P MNO Error” ausgelöst werden.

Folgende Event Codes müssen jedenfalls erfasst werden:

Reject-Cause	Beschreibung (Englisch)	Beschreibung (Deutsch)
2	IMSI unknown in HSS	IMSI im HSS unbekannt
3	Illegal UE	Illegales Endgerät
5	IMEI not accepted	IMEI nicht akzeptiert
6	Illegal ME	Illegales Mobilfunkgerät
7	EPS services not allowed	EPS-Dienste nicht erlaubt
8	EPS services and non-EPS services not allowed	EPS- und Nicht-EPS-Dienste nicht erlaubt
9	UE identity cannot be derived by the network	UE-Identität kann vom Netz nicht abgeleitet werden
10	Implicitly detached	Implizit getrennt (Detach)
11	PLMN not allowed	PLMN nicht erlaubt
12	Tracking area not allowed	Tracking Area nicht erlaubt
13	Roaming not allowed in this tracking area	Roaming in dieser Tracking Area nicht erlaubt
14	EPS services not allowed in this PLMN	EPS-Dienste in diesem PLMN nicht erlaubt
15	No suitable cells in tracking area	Keine geeigneten Zellen in der Tracking Area
17	Network failure	Netzwerkausfall
19	ESM failure	ESM-Fehler (Sitzungsmanagement-Fehler)
20	MAC failure	MAC-Fehler (vom UE an das Netz gesendet, Auth-Fehler)
21	Synch failure	Synch-Fehler (vom UE an das Netz gesendet, Auth-Fehler)
22	Congestion	Überlastung

23	UE security capability mismatch	Sicherheitsfähigkeits-Mismatch des UE
24	Security mode rejected, unspecified	Sicherheitsmodus abgelehnt, nicht spezifiziert
25	Not authorized for this CSG	Für diese CSG nicht autorisiert
39	CS domain not available	CS-Domäne nicht verfügbar
40	Permanent rejection	Permanente Ablehnung

E.2 Mobile radio attach-reject code Log

Radio attach-reject codes müssen in diesem Log- Objekt für einen konfigurierbaren Zeitraum gespeichert und auslesbar sein.

E.3 PDP context error code

Beim Aufbau des PDP Kontexts werden Fehler in diesem Objekt erfasst:
Die folgenden Fehlermeldungen müssen dabei erfasst werden und das Communication Event *147 "PDP context destroyed"* oder *148 "PDP context failure"* ausgelöst werden.

PS internal cause		Comm Event
1	Invalid connection identifier	148
2	Invalid NSAPI	148
3	Invalid Primary NSAPI	148
4	Invalid field	148
5	SNDCP failure	148
6	RAB setup failure	148
7	No GPRS context	148
8	PDP establish timeout	147
9	PDP activate timeout	147
10	PDP modify timeout	147
11	PDP inactive max timeout	147
12	PDP lowerlayer error	147
13	PDP duplicate	148
14	Access technology change	147
15	PDP unknown reason	148
PS network cause		
16	LLC or SNDCP failure	148
17	Insufficient resources	148
18	Missing or unknown APN	148

19	Unknown PDP address or PDP type	148
20	User Aauthentication failed	148
21	Activation rejected by GGSN	148
22	Activation rejected, unspecified	148
23	Service option not supported	148
24	Requested service option not subscribed	148
25	Service option temporarily out of order	147
26	NSAPI already used (not sent)	148
27	Regular deactivation	147
28	QoS not accepted	147
29	Network failure	147
30	Reactivation required	147
31	Feature not supported	148
32	Semantic error in the TFT operation	148
33	Syntactical error in the TFT operation	148
34	Unknown PDP context	148
35	PDP context without TFT already activated	148
36	Semantic errors in packet filter	147
37	Syntactical errors in packet filter	147
38	Invalid transaction identifier	148
39	Semantically incorrect message	148
40	Invalid mandatory information	147
41	Message non-existent/not implemented	148
42	Message type not compatible with state	148
43	IE non-existent/not implemented	148
44	Conditional IE error	148
45	Message not compatible with state	148
46	Protocol error, unspecified	148

E.4 PDP context error event log

PDP Kontext Errors müssen in diesem Log- Objekt für einen konfigurierbaren Zeitraum gespeichert und auslesbar sein.

Oesterreichs Energie Companion Standard
Smart Meter 2.0

D.4_OE_CS_Implementation_Guide_Ethernet

Version 1.0

31.3.2026

Inhaltsverzeichnis

A. Einführung 2

A.1 Scope 3

A.2 Revisionshistorie 3

A.3 Normative Referenzen 3

B. Beschreibung WAN Interface – G1 4

C. Technische Spezifikation 4

C.1 Ethernet Schnittstelle 4

C.2 Unterstützte Protokolle 4

C.3 Physikalischer Zugriffsschutz 4

C.4 Watchdog Mechanismen 4

D. Communication module related Object 4

D.1 Generelle Anmerkungen 5

D.2 Ethernet configuration 5

D.3 Ethernet Filter 5

D.4 Ethernet Status 5

D.5 Ethernet diagnostic 5

E. Communication related EVENTS 5

E.1 Communication Events 5

A. Einführung

A.1 Scope

Ziel dieses Dokuments ist die Sicherstellung der Interoperabilität des Smart Meter 2.0 mit Ethernet Modul mit den Zentralen Systemen der Netzbetreiber.

Dazu werden in diesem Dokument folgende Aspekte definiert

- Physikalische Anforderungen Ethernet Schnittstelle
- Notwendige Zählerfunktionen
- Erläuterungen zum Objektmodell „D.1_OE_CS_Objektmodel.xlsx“
- Zu überwachende Events und Alarme

A.2 Revisionshistorie

Version	Revisions	Date	Author
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

A.3 Normative Referenzen

Eine Auflistung sämtlicher gesetzlicher Vorgaben, Standards und Normen ist im Dokument „A.1_OE_CS_Gesetze_Normen_und_Standards.pdf“ zu finden.

B. Beschreibung WAN Interface – G1

Das Ethernet Kommunikationsmodul dient als Verbindung zwischen dem Zähler und den Zentralen Systemen, indem es einen IP-basierten Kommunikationspfad über die G1- Schnittstelle zur Verfügung stellt. Netzwerkseitig ist das Modul für eine stabile und verlässliche Verbindung zu den Zentralen Systemen zuständig. Die aktuelle und gültige Version ist dem Dokument „B.3. Anhang_Schnittstellen_Details.pdf“ zu entnehmen.

C. Technische Spezifikation

C.1 Ethernet Schnittstelle

Die Ethernet Schnittstelle muss nach IEE 802.3 ausgeführt werden. Die Ethernet Schnittstelle stellt eine WAN-Verbindung über IP (Internet Protocol) zum Zentralen System zur Verfügung.

Die Kommunikations-Schnittstelle muss mindestens folgende grundlegende Eigenschaften unterstützen:

- Übertragungsgeschwindigkeit: Fast Ethernet(10/100 Mbit)
- Auto-Negotiation bzw. fixierte Geschwindigkeitseinstellungen
- Duplex Verfahren: Full-Duplex und Half Duplex
- Physikalische Ausführung: RJ-45 mit Auto MDI-X (Automatic medium-dependent interface crossover)
- Status LED:
  - Mindestens eine LED zur Anzeige des Betriebszustandes (LINK ON, TX/RX Aktivität)
- VLAN Tagging nach IEEE 802.1Q
- DHCP

C.2 Unterstützte Protokolle

Die Vollständige Liste aller Protokolle ist dem Dokument „B.3_Anhang_Schnittstellen_Details.pdf“ zu entnehmen.

C.3 Physikalischer Zugriffsschutz

Das Kommunikationsmodul und die Schnittstelle müssen so ausgeführt werden das unbefugten Personen der Zugang zur Schnittstelle verwehrt bleibt. Die Abdeckung des RJ45-Ethernet Anschlusses muss konstruktiv so ausgeführt sein, dass sie auch bei eingestecktem Ethernet Kabel vollständig verschließbar ist. Darüber hinaus muss die Abdeckung in diesem Zustand eine Plombierung ermöglichen, sodass ein unbefugtes Öffnen eindeutig erkennbar ist.

C.4 Watchdog Mechanismen

Der Zähler und das Kommunikationsmodul müssen mehrere Watchdog-Mechanismen unterstützen, um sicherzustellen, dass kurative Maßnahmen eingeleitet werden, falls Probleme auf der Geräte- oder Netzwerkseite auftreten und die Kommunikation zwischen Zentralem System und Zähler unterbrochen ist. Dafür müssen mehrere unterschiedliche Watchdog-Timer unterstützt werden, welche je nach Anwendungsfall, nach definierten Zeiten ohne Kommunikation zum Zentralem System einen Neustart (reboot) oder andere kurative Maßnahmen des Kommunikationsmodul auslöst.

Die Anforderungen sind dem Dokument „H.2_OE_CS_Annex.pdf“ zu entnehmen.

D. Communication module related Object

D.1 Generelle Anmerkungen

Alle Objekte in diesem Kapitel sind im Oesterreichs Energie SmartMeter 2.0 Companion Standard unter „D.1_OE_CS_Objektmodel.xlsx“ vollständig beschrieben und dokumentiert. Dieses Kapitel dient für zusätzliche Anmerkungen oder Erläuterungen.

D.2 Ethernet configuration

Dieses Objekt dient der Konfiguration des Ethernetmoduls. Die folgenden Parameter müssen anpassbar sein:

- MTU: 1280
- Speed: 10M/100M/Autoneg
- Duplex: FullDuplex/HalfDuplex/Auto
- VLANID: 1
- Status LED: ON/OFF
- Ethernet: Enable/Disable (only possible with local Client)

D.3 Ethernet Filter

Folgende Filteroptionen müssen konfigurierbar sein:

- Ethernet Filter options:
  - Drop multicast: ON/OFF
  - Drop broadcast: ON/OFF
  - Drop DHCP requests: ON/OFF
  - Drop ARP: ON/OFF
- ACL (Access Class List)
  - MAC address filter list
  - IP Range filter list

D.4 Ethernet Status

Für Diagnosezwecke müssen die folgenden Parameter erfasst und über dieses Objekt auslesbar sein.

- Speed
- Duplex
- Ethernet

D.5 Ethernet diagnostic

- TX traffic in bytes
- RX traffic in bytes
- Paket statistics

E. Communication related EVENTS

E.1 Communication Events

Die folgenden Kommunikationsevents müssen am Zähler erfasst werden:
Eine vollständige Liste befindet sich im Anhang des Hauptdokuments unter „D. Implementierungsstandards/D1. Objektmodel.xlsx“, Tabellenblatt „Generic Events“.

Ethernet Related Communication events		
Number	Name	Description
	LINK UP	Ethernet Link Status UP
	LINK DOWN	Ethernet Link Status DOWN

Oesterreichs Energie Companion Standard
Smart Meter 2.0

E.1_OE_CS_Lastenheft_SM_Direktmessung

Version 1.0

31.03.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Einleitung 5

B. Zulassung 5

B.1 Eichrecht 5

C. Smart Meter 6

C.1 Generelle Anforderungen 6

C.2 Allgemeine konstruktive Anforderungen 7

C.2.1 Gehäuse allgemein 7

C.2.2 Klemmenblock 8

C.2.3 Zählerkontaktstifte 10

C.2.4 Klemmendeckel 11

C.2.5 Typenschild 13

C.2.6 Seriennummer 14

C.2.7 Anforderungen an EMV, Isolationsfestigkeit; Luft- und Kriechstrecke 14

C.2.8 Resistenz gegen Oberschwingungsströme 16

C.2.9 Schutzklasse 16

C.2.10 Beständigkeit gegen Hitze und Feuer 16

C.2.11 Klimatische Bedingungen und Temperaturbereich 16

C.2.12 Eigenverbrauch 17

C.2.13 Zulassung, Eichung, Nacheichung 17

C.2.14 Messtechnik, Anschluss 20

C.2.15 Funktionsüberwachung (Smart Meter Selbsttest), Watchdog 21

C.3 Technische Ausführung 21

C.3.1 Nennströme 21

C.3.2 Messgrößen 22

C.3.3 Speichertiefe 22
C.3.4 Opt-Out Funktion 22
C.3.5 Softwarearchitektur der Smart Meter 22
C.3.6 Anzeigen am Smart Meter 23
C.3.7 Uhren- und Kalenderfunktion 24
C.3.8 Breaker 25
C.3.9 Steuerausgänge 26
C.3.10 Schnittstelle Kommunikationsmodul - Zähler 26
C.3.11 Events/Alarme 26
C.4 Dokumentation 27

A. Einleitung

Das nachfolgende Dokument beschreibt die wesentlichen technischen Anforderungen an direkt messende Smart Meter mit 1 und 3 phasigen Anschluss für den österreichischen Markt.

B. Zulassung

Der Smart Meter sowie alle Zusatzmodule müssen, die für den Betrieb in Österreich erforderlichen Zulassungen und Zertifizierungen besitzen. Es sind die dafür erforderlichen Dokumente dem Auftraggeber zeitnah zur Verfügung zu stellen.

B.1 Eichrecht

In Österreich müssen Smart Meter beim Einsatz im rechtsgeschäftlichen Verkehr geeicht sein. Die Smart Meter unterliegen sowohl der europäischen Messgeräterichtlinie für die Eichung der Wirkenergie als auch dem österreichischen Maß- und Eichgesetz für die nationale Eichung der Blindenergie, Leistungsmaximum und des Lastprofils. Dazu benötigt der Smart Meter neben einer MID-Zulassung auch eine nationale Zulassung durch das österreichische Bundesamt für Eich- und Vermessungswesen (1160 Wien, Arltgasse 35; http://www.metrologie.at). Die nationale Eichung ist nur in einer durch das BEV ermächtigten Eichstelle möglich.

Die österreichischen Eichvorschriften für Elektrizitätszähler, elektrische Tarifgeräte und Zusatzeinrichtungen bieten zwei Möglichkeiten für die nationale Eichung. Lückenlose eichtechnische Prüfung aller Messgeräte (Einzelüberprüfung) oder als statistische Prüfung (Kontrolle) eines Loses an Messgeräten.

Des Weiteren besteht die Möglichkeit der Anerkennung geeichter Smart Meter aus dem Ausland. Der Hersteller hat die Möglichkeit, im Zuge eines Antrags, „nicht in Österreich geeichte Smart Meter“ von der Behörde anerkennen zu lassen. Die Anerkennung erfolgt per Bescheid, sofern das Messgerät den österreichischen Anforderungen entspricht. Die dafür erforderlichen Rahmenbedingungen sind direkt zwischen dem Anbieter und den Behörden (Bundesministerium für Wirtschaft, Energie und Tourismus sowie dem Bundesamt für Eich- und Vermessungswesen) abzuklären. Sämtliche Verantwortungen zur Zulassung obliegen dem Lieferanten.

Die Smart Meter müssen geeicht ausgeliefert werden, so dass sie in Österreich im rechtsgeschäftlichen Verkehr eingesetzt werden können. Das Eichjahr der gelieferten Smart Meter muss dem Jahr der Lieferung entsprechen, ausgenommen sind die ersten 3 Monate des Kalenderjahres, hier ist als Eichjahr das letzte Kalenderjahr zulässig.

C. Smart Meter

Definition des Smart Meters: Physikalische Einheit von Zählwerk (eichpflichtige und nicht eichpflichtige Firmware), Display, Breaker, Kunden-, WAN- und Serviceschnittstelle.

Es werden 3 unterschiedliche Smart Meter Typen bei direkt angeschlossenem Smart Meter unterschieden.

Tabelle 1: Smart Meter Typen

Anschluss-Varianten	**Smart Meter 1ph**	**Smart Meter 3ph**	**Hochampere Smart Meter 3ph**
Nennströme	0,25 - 5(60) A	0,25 - 5(60) A	**0,25 - 5 oder 10(100) A**
U_{Nenn} bei Nenn-frequenz 50 Hz	**230 V**	**3x 230/400 V**	**3x 230/400 V**

C.1 Generelle Anforderungen

Die Smart Meter haben grundsätzlich den anzuwendenden Anforderungen gemäß Dokument "A.5_OE_CS_Gesetze_Normen_und_Standards.pdf" zu entsprechen.

Zusätzliche Anforderungen sind in diesem Dokument definiert.

Die Smart Meter müssen den Anforderungen der europäischen Messgeräterichtlinie MID sowie dem österreichischen Maß – und Eichgesetz (MEG) entsprechen sowie die österreichischen Eichvorschriften erfüllen.

Die Smart Meter und verfügbare Module müssen ohne eine weitere Überprüfung in Österreich einsetzbar sein. Sie müssen alle anwendbaren Gesetze sowie europäische und österreichische Normen erfüllen.

Bei Anforderungen in diesem Dokument, welche von Normen abweichen oder über diese hinausgehen, gilt jeweils die strengere Version.

Der Smart Meter muss auch die FNN (Forum Netztechnik/Netzbetrieb im VDE) Forderungen des „Leitfaden zur Bewertung der Zuverlässigkeit und Messbeständigkeit von Messsystemen" erfüllen.

Smart Meter mit 60 A Maximalstrom müssen mit 100,8 A für 2 Stunden ohne Schäden und Funktionseinschränkungen belastbar sein (HLS 63 A x1,6).

Smart Meter mit 100 A Maximalstrom müssen mit 128 A für 2 Stunden ohne Schäden und Funktionseinschränkungen belastbar sein (HLS 80 A x1,6).

C.2 Allgemeine konstruktive Anforderungen

Die Smart Meter müssen aufgrund ihrer konstruktiven Gestaltung und Herstellung so beschaffen sein, dass bei festgelegten Betriebs- und normalen Einsatzbedingungen keine Gefährdungen auftreten können. Insbesondere müssen sichergestellt sein:

- die Sicherheit von Personen gegen gefährliche Körperströme
- die Sicherheit von Personen gegen Auswirkungen erhöhter Temperatur
- die Sicherheit und Beständigkeit gegen Hitze und Feuer
- der Schutz des Gehäuses gegen das Eindringen von Festkörpern, Staub und Wasser (mindestens IP51)
- der Schutz von Personen gegen gesundheitsbeeinträchtigende Ereignisse (Dämpfe, scharfe Kanten, …).

Darüber hinaus müssen die Smart Meter einfachen mechanischen und elektrischen Manipulationsversuchen (Schnittstellen eingeschlossen) widerstehen.

Alle unter normalen Einsatzbedingungen der Korrosion ausgesetzten Teile müssen wirksam geschützt sein. Die Schutzschichten müssen so widerstandsfähig sein, dass sie bei den in der MID festgelegten Einsatzbedingungen nicht durch atmosphärische Einwirkungen beschädigt werden können.

Die Geräte sind so auszuführen, dass bei der Montage maximal 2 Werkzeuge benötigt werden. Für den Klemmenblock und Klemmendeckel ist Torx 20 zu verwenden. Sonderwerkzeuge sind explizit nicht erlaubt. Bei plombierbaren Schrauben muss die Position der Öffnung für den Plombendraht ersichtlich sein.

C.2.1 Gehäuse allgemein

Die Hauptmaße der Smart Meter sowie die Art und Anordnung der Befestigungselemente müssen folgenden Anforderungen entsprechen:

- Smart Meter 1ph: DIN 43857-1
- Smart Meter 3ph: DIN 43857-2

  Ausnahme beim Smart Meter 3ph: Der vertikale Lochabstand der Befestigungslaschen ist in der Norm mit 230 +-1 mm angegeben. Dieser Abstand darf von den Angaben in der Norm abweichen, aber nicht überschreiten.

Das Gehäuse muss so konstruiert und angeordnet sein, dass eine vorübergehende Deformation den zuverlässigen Betrieb des Smart Meters nicht beeinträchtigt (z.B. Verspannung bei der Montage darf zu keinem Geräteschaden führen).

Die grundsätzliche Art und Anordnung der Befestigungselemente haben der DIN 43857 zu entsprechen. Zur leichteren Montage des Smart Meters, ohne entfernen der Befestigungsschrauben des Klemmbretts, muss die obere Aufhängelasche über das Smart Meter Gehäuse inkl. montiertem Kommunikationsmodul hinausragen. Trotz dieser Vorgabe muss die Aufhängelasche möglichst kurz bleiben.

Das Gehäuse muss in der Weise plombierbar sein, dass die inneren Teile des Zählers erst nach Brechen der Plombe(n) oder des Gehäuses zugänglich sind. Mindestdurchmesser 3,0 mm für Plombierdraht. Eine Entfernung der Gehäusekappe darf ohne Benutzung eines Werkzeugs nicht möglich sein.

Die Kundenschnittstelle muss frei zugänglich sein (ohne Öffnung einer Plombe, …).

Es sind ein oder mehrere Modulschächte für die WAN-Schnittstellenmodule vorzusehen.

Der Modul- und Antennentausch ist elektrotechnisch laiensicher und ohne Abschaltung vorzusehen – Die Verbindung vom Zähler zum Modul ist ab 48 V berührungssicher auszuführen.

Es darf kein Zugang zum Kommunikationsmodul möglich sein, ohne die Plombierung des Moduldeckels zu öffnen. Es darf dabei auch keine Eichplombe bzw. Eichklebeetikette beschädigt oder entfernt werden.

Die Befestigungsschrauben des Moduldeckels sind vorzugsweise mit Torx Tx-20 Schrauben auszuführen, eine schraubenlose Verriegelung ist zulässig.

Das Gehäuse muss so ausgeführt werden, dass sämtliche Plombiermöglichkeiten als Plombe und als Klebeetikette sichergestellt werden können.

WAN-Schnittstellenmodule für Smart Meter 1ph + 3ph und Smart Meter Messwandler müssen die gleichen Abmessungen haben und funktional kompatibel für alle drei Varianten einsetzbar sein.

Bei Modulen für Funkkommunikation muss der Anschluss einer externen Antenne möglich sein. Eine Ausführung unterhalb des Klemmdeckels ist nicht zulässig. Gehäuse und Deckel sind aus wiederverwertbarem Isolierstoff (UV- Lichtbeständig, beständig gegen Lösungsmitteldämpfe) entsprechend Schutzklasse II auszuführen.

Um die Lagerung und das Handling zu vereinfachen, müssen die Geräte ohne Hilfsmittel – jedoch auch im plombierten Zustand sowie mit und ohne Verpackung – stapelbar sein. Diverse Gehäuseteile (Klemmdeckel, Modulabdeckungen, usw.) müssen auch als Zubehör einzeln bestellbar sein.

C.2.2 Klemmenblock

Der Klemmenblock bei Smart Meter 3ph bis 60 A hat den Abmessungen laut DIN 43857-2 und bei Smart Meter 1ph der DIN 43857-1 zu entsprechen und muss für den Einsatz von Smart Meter Anschlussklemmen (Steckleisten, Klemmleisten) gemäß OVE R21 geeignet sein.

Wenn die Klemmen in einem Klemmenblock oder in mehreren Klemmenblöcken angeordnet sind, müssen sie eine ausreichende Isolation und mechanische Festigkeit aufweisen. Um diese Forderung zu gewährleisten ist das für die Herstellung der Anschlussklemme(n) vorgesehene Isoliermaterial entsprechend zu prüfen.

Das Material des Klemmenblocks muss die Prüfungen nach ISO 75 für eine Temperatur von 135 °C und einen Druck von 1,8 MPa (Methode A) bestehen.

Einführungen in das Isolationsmaterial, die über die Klemmenbohrungen herausragen, müssen von ausreichender Größe sein, um auch die Isolierung der Leiter einführen zu können.

Die Befestigungsart der Leiter in den Klemmen muss ausreichenden und dauerhaften Kontakt gewährleisten. Es muss verhindert sein, dass sich die Leiter lockern oder übermäßig erwärmen können. Schraubverbindungen, die einen elektrischen Kontakt herstellen und Schrauben, die während der Lebensdauer des Smart Meters mehrfach angezogen und gelöst werden dürfen, müssen eine Gewindebuchse aus Metall haben.

Die Hauptklemmen sind als Buchsenklemmen mit zwei Klemmschrauben oder Rahmenklemmen durchgängig aus elektrisch leitfähigem Material zur Verwendung von Torx- Schraubendrehern (Größe Tx-20) auszuführen.

Für die Hauptklemmen ist eine Zentrierung für die Stifte und Drähte gefordert. Alle Schraubenklemmen müssen mit Sicherungen versehen sein, die ein Herausfallen von komplett gelösten Schrauben verhindern. Die Schrauben müssen dabei aber austauschbar sein.

Das minimale und maximale Anzugsdrehmoment für alle Schrauben ist bekannt zu geben.

Es sind auch neuartige Methoden (z.B. Klemmung) zur Montage der Leiter oder Stifte zulässig. Es obliegt dem jeweiligen Netzbetreiber die Langlebigkeit zu beurteilen und die Lieferung dieser Methode freizugeben.

Die Tiefe der Hauptklemme muss zur sicheren Montage min. 23 mm betragen. Der Klemmblock muss auch zur Aufnahme von Zählerstiften (siehe Dokument „H.1_OE_CS_Zählerstifte_und_Steckleisten.pdf“) oder Einzelleitern (mehrdrahtig bzw. feindrahtig mit Adernendhülse) geeignet sein.

Das Material des Klemmenblocks muss die Prüfungen nach ISO 75 für eine Temperatur von 135 °C und einen Druck von 1,8 MPa (Methode A) bestehen.

Die 100 A Variante muss ebenfalls die DIN-Maße der 60 A Variante einhalten, jedoch ist ein Klemmbereich von 4 mm² bis 35 mm² einzuhalten.

Schutzart mind. IP51

Die Bezeichnungen für die Hauptklemmen sind nach DIN 43856 anzubringen.

Die Korrosionsgefahr durch unterschiedliche Kontaktmaterialien ist durch die geeignete Auswahl dieser Werkstoffe zu minimieren.

Elektrische Verbindungen müssen so ausgelegt sein, dass der Kontaktdruck nicht durch das Material der Isolation geführt wird.

Anschlussklemmen mit unterschiedlichem Potential, die eng nebeneinander angeordnet sind, müssen gegen zufälliges Kurzschließen gesichert sein. Dieser Schutz kann durch isolierende Zwischenstücke erreicht werden.

C.2.3 Zählerkontaktstifte

Zählerkontaktstifte werden beigestellt oder vom Netzbetreiber gesondert definiert.

Bei Bestellung mit Kontaktstiften sind Smart Meter 3ph mit 7 bzw. Smart Meter 1ph mit 3 Kontaktstiften zu bestücken.

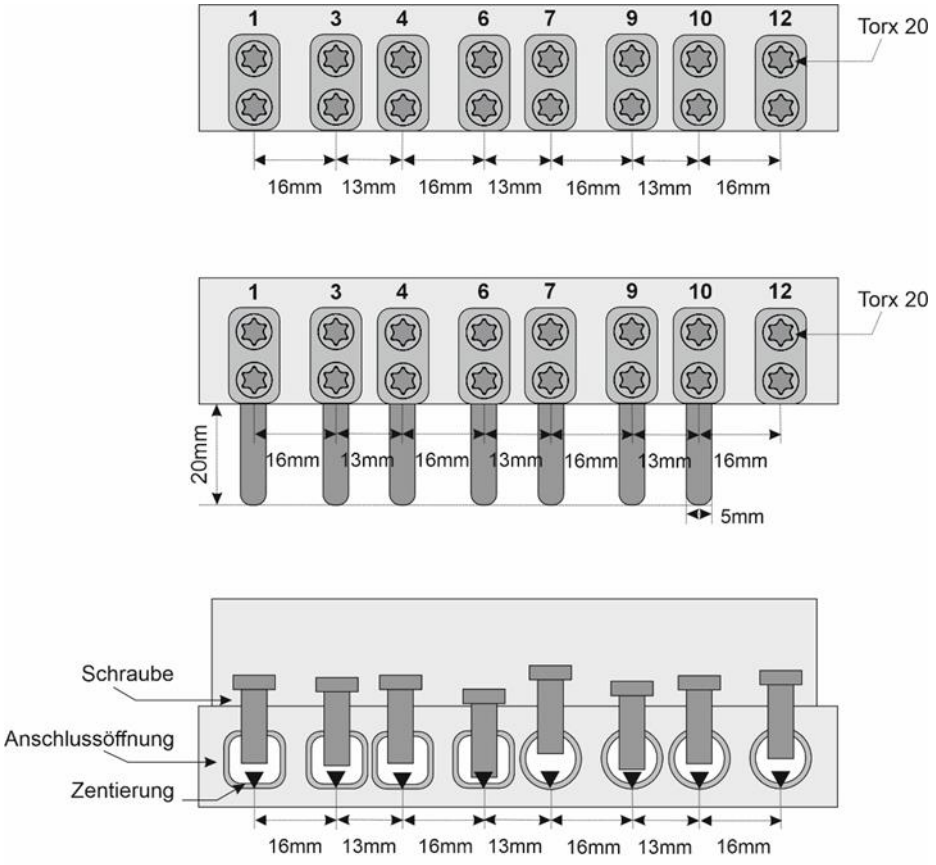


Abbildung 1: Smart Meter 3ph: Positionierung der Zählerstifte (Durchmesser 5 mm) mit festgezogenen Zählerklemmen

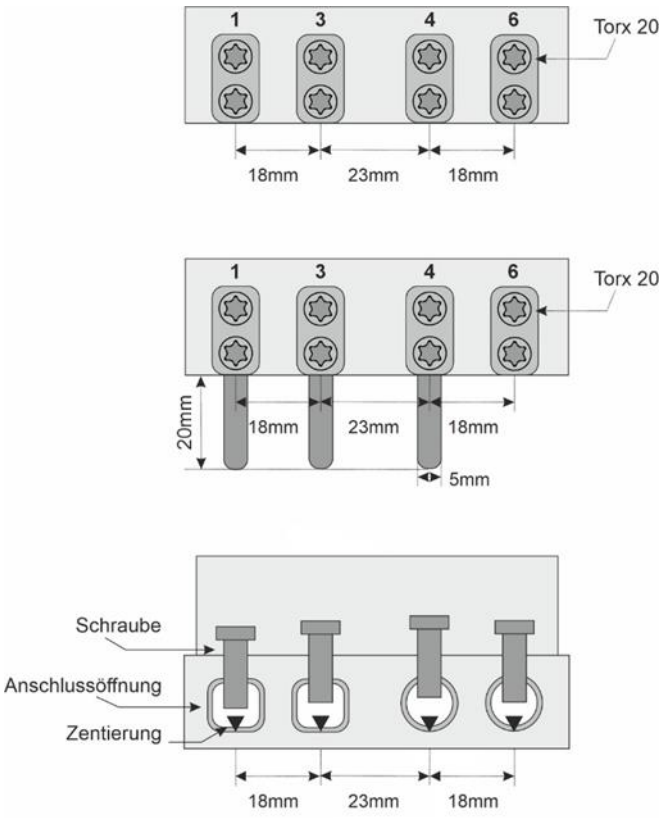


Abbildung 2: Smart Meter 1ph: Positionierung der Zählerstifte (Durchmesser 5 mm) mit festgezogenen Zählerklemmen

C.2.4 Klemmendeckel

Die Anschlussklemmen des Zählers müssen einen getrennten Klemmendeckel aufweisen, der unabhängig vom Gehäuse und dem Kommunikationsmodul plombiert werden kann. Der Klemmendeckel muss die Anschlussklemmen, die Befestigungsschrauben für die Leiter und über eine geeignete Länge auch externe Leiter und ihre Isolation, sowie alle Steuerausgänge abdecken.

Es darf kein Zugang zu den Klemmen möglich sein, ohne die Plombierung des Klemmendeckels zu öffnen. Die Befestigungsschrauben des Klemmendeckels sind mit Torx Tx-20 Schrauben auszuführen, eine schraubenlose Verriegelung des Klemmendeckels ist ebenso zulässig.

Die Plombiermöglichkeiten sind so auszuführen, dass eine einfache Plombierung möglich ist, Mindestdurchmesser 3,0 mm für Durchführung des Plombierdrahts.

Klemmendeckel sind aus wiederverwertbarem Isolierstoff entsprechend Schutzklasse II herzustellen.

Der Klemmendeckel muss aus einem undurchsichtigen Kunststoff gefertigt werden.

Schrauben müssen unverlierbar, aber trotzdem tauschbar im Klemmendeckel eingebracht sein (captive Screw). Weiters müssen die Schrauben für mehrmalige Verwendung geeignet sein. Bei der Auslieferung muss der Klemmendeckel bereits auf dem Smart Meter montiert sein.

Es ist gefordert ein Schaltbild für den Anschluss des Smart Meters im Klemmendeckel anzubringen. Dieses Schaltbild ist mit dem Auftraggeber abzustimmen.

Es sind verschiedene Längen von Klemmendeckel erforderlich:

Für Smart Meter 3ph gilt:

Freiraum zwischen Klemmenblock und Ende des Klemmendeckel (x): 60 mm, 70 mm, 85 mm,110 mm, ohne Freiraum (15 mm, unten geöffnet). Bei einer Ausführung von 85 mm und 110 mm wird die maximale Länge des Klemmdeckels gem. Norm DIN 43857-4 von 100 mm überschritten.

Der Klemmendeckel darf in seiner gesamten Länge die Mindesthöhe (y) von 45 mm nicht unterschreiten.

Zusätzlich wird eine **Spezialversion in 85 mm** Ausführung mit der Möglichkeit zur **Montage von Zusatzgeräten gemäß DIN 43857-5** benötigt, wobei die max. Länge gem. Norm (105 mm) überschritten werden kann.

Für Smart Meter 1ph gilt:

Freiraum zwischen Klemmenblock und Ende des Klemmendeckel (x): 45 mm, 65 mm, 80 mm, ohne Freiraum (15 mm, unten geöffnet).

Der Klemmendeckel darf in seiner gesamten Länge die Mindesthöhe (y) von 45 mm nicht unterschreiten.

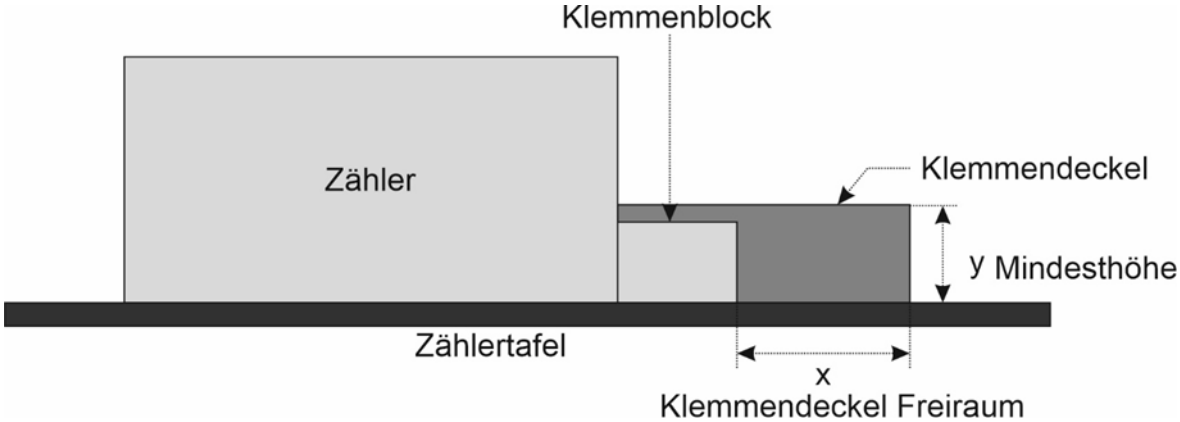


Abbildung 3: Definition der Abmessungen des Klemmdeckels

Der Smart Meter muss mit dem längsten Klemmendeckel auf der Zählerplatte für Verteilermontage (Typ A) laut Ö-Norm 8640 montiert werden können. Um eine Montage auf einer Normzählertafel bewerkstelligen zu können, dürfen die 230 mm Lochabstand für die Befestigung und die 340 mm Gesamtlänge auf keinen Fall überschritten werden.

Das Öffnen des Klemmendeckels muss ohne vorherige Öffnung anderer Gehäuseteile möglich sein.

C.2.5 Typenschild

Wenn der Smart Meter auf der Zählerbrett montiert ist, müssen das Typenschild und das nationale Eichsiegel von vorne vollständig lesbar sein.

Jeder Smart Meter muss folgende Aufschriften haben:

- alle durch die MID geforderten Aufschriften
- alle national geforderten Aufschriften
- alle aus Zulassungen und Bescheinigungen geforderten Aufschriften
- alle durch geltende Normen geforderten Aufschriften

Die nachfolgend angeführten Angaben stellen den Mindestumfang der Aufschriften dar, welche auf dem UV-beständigen Typenschild enthalten sein müssen. Sie müssen dauerhaft aufgebracht werden und deutlich und von außen lesbar sein.

- Name des Herstellers oder Firmenzeichen
- Typenbezeichnung und beide Zulassungszeichen: Von der MID-Zulassung ist die jeweilige Nummer des Zulassungsbescheides der Prüfstelle anzugeben.
- die Anzahl der Phasen und die Anzahl der Leiter, für die der Smart Meter vorgesehen ist (dreiphasig Vierleiter). Diese Angaben können auch in Form von graphischen Symbolen nach EN 62053-52 gemacht werden.
- die Seriennummer und das Herstellungsjahr.
- Nennspannung: Anzahl der Messsysteme und die Spannung an den Klemmen der Spannungspfade.
- Nennstrom (Bsp.: 0,25 – 5(60) A)
- Nennfrequenz: in Hertz
- Zählerkonstante z.B. in der Form: Imp. /kWh
- Genauigkeitsklasse
- Bemessungsstoßspannung
- Gebrauchskategorie (UC)
- Temperaturbereich lt. MID z.B.: 3k6 (-25 °C bis +55 °C)
- das Zeichen für Schutzisolierung
- Kennziffernschlüssel: Es sind alle relevanten Kennziffern am Typenschild zu beschreiben.
- Eigentumsvermerk, optional inkl. Logo
- CE – Zeichen mit MID-Eichjahr (Bsp. M26) und durchgeführte benannte Stelle
- Optional muss auf Wunsch des Netzbetreibers eine Schaltungsnummer zur eindeutigen Identifikation des zugehörigen Klemmenplans angebracht werden.
- Messperiode (tm=15min)
- Optisch lesbare Codes für Seriennummern (Barcodes oder QR-Codes) müssen in einer ausreichende Größe und kontrastreich ausgeführt werden, welche auch bei diffuser Beleuchtung gut lesbar sind.

Die Verwendung genormter Symbole nach EN 62053-52 auf dem Typenschild ist zulässig.

Die Ausgestaltung des Typenschilds ist jeweils individuell mit dem Netzbetreiber abzustimmen, insbesondere der maschinenlesbare Code. Es ist darauf zu achten, dass keine unerlaubten Aufschriften angebracht sind z.B. herstellerspezifische Seriennummern oder nicht normgerechte Schaltzeichen.

C.2.6 Seriennummer

Seriennummern für Smart Meter und Modul entsprechend COSEM logical device name lt. AC Electricity Smart Meter Generic Companion Profile, Punkt 6.2.2.

Smart Meter und Module müssen voneinander unabhängige Seriennummern/Barcodes aufweisen.

MMMTTTCCNNNNNNNN:

- MMM ist der Drei-Buchstaben-Code für Hersteller
- TTT ist der Gerätetyp
- CC ist der Funktionstyp
- NNNNNNNN ist die Fabrikationsseriennummer (8 Ziffern).

C.2.7 Anforderungen an EMV, Isolationsfestigkeit; Luft- und Kriechstrecke

C.2.7.1 Genormte Nennspannungen

Nennspannung: 230 V (L, N) bzw. 230/400 V (L1, L2, L3, N)

C.2.7.2 Toleranzbereich der Netzspannung

Das Netzteil mit der Nennspannung Un = 230 V, muss so ausgelegt sein, dass es lt. EN 50470-1 in folgenden Spannungsbereichen einwandfrei betrieben werden kann:

- normaler Betriebsbereich: 0,9 Un bis 1,10 Un
- erweiterter Betriebsbereich: 0,8 Un bis 1,15 Un

Im Zuge des Angebotes ist jene Mindestspannung anzugeben, bei welcher der Smart Meter zu messen beginnt.

C.2.7.3 Frequenz

Netzgeräte sind für eine Nennfrequenz von 50 Hz auszulegen. Sie müssen in einem Toleranzbereich von + 2% der Nennfrequenz fehlerfrei betrieben werden können.

C.2.7.4 Netzrückwirkungen

Das Netzteil ist so zu gestalten, dass unzulässig hohe Rückwirkungen in Form von Oberschwingungen auf das Netz nicht gegeben sind.

Es ist die Einhaltung der EN 61000-3-2 zu gewährleisten.

C.2.7.5 Medizinische Exposition

Es ist sicherzustellen, dass die elektrischen und magnetischen Felder, welche durch einen typischen Einsatz der angebotenen Komponenten entstehen, die medizinischen Grenzwerte der OVE-Richtlinie R 23-1 nicht überschreiten.

C.2.7.6 Sicherheit gegen Stoßspannung

Die Prüfung hat nach EN 62052-11 Kapitel 7.3.2 Stoßspannungsprüfung zu erfolgen.

- Wellenform des Pulses: 1,2/50 µs nach IEC 60060-1
- Impedanz der Quelle: 500 Ohm + 50 Ohm
- Prüfspannung Scheitelwert: 8 kV.

C.2.7.7 Stoßspannungsfestigkeit

Die Geräte müssen nach der EN 61000-4-5 die Prüfungen bei einer Stoßspannungswelle 1,2/50 µs – Puls standhalten.

- Wellenform des Pulses: 1,2/50 µs nach IEC 60060-1
- Impedanz der Quelle: 2 Ohm ± 10 %
- Prüfspannung Scheitelwert: 4 kV.

C.2.7.8 Erweiterte Blitzschutzfestigkeit

Die Stoßspannungsprüfung nach dem „FNN-Leitfaden zur Bewertung der Zuverlässigkeit und Messbeständigkeit von Messsystemen“ muss bestanden werden (0,1/2000 µs/ 7kV/ 1Joule/50 Ohm).

C.2.7.9 Elektromagnetische Verträglichkeit

Die Geräte müssen nach CENELEC-EN 55011, CENELEC-EN 55014 bzw. EN50065-1 und EN 55032 (CISPR 32) funkentstört sein. Eine Beeinflussung der Netzteile durch äußere elektrische und magnetische Felder, die an den Einsatzorten der Smart Meter üblicherweise erwartbar sind, darf nicht erfolgen.

C.2.7.10 Störfestigkeit gegen transiente Störgrößen (Burst)

Hier sind die Forderungen gemäß EN 61000-4-4 zu erfüllen (Prüfschärfe 4).

C.2.7.11 Magnetische Beeinflussung durch Dauermagneten

Der Smart Meter darf nach Manipulationen mit Normmagneten an beliebigen Stellen (dreidimensional) keine irreversiblen Schäden aufweisen. Die Magnetdefinition und der Prüfaufbau zur Feststellung dieser Anforderung ist dem „FNN-Leitfaden zur Bewertung der Zuverlässigkeit und Messbeständigkeit von Messsystemen“ zu entnehmen.

Felder unter 380mT dürfen weder ein messtechnisches noch ein funktionales Fehlverhalten des Smart Meters bewirken. Bei Auftreten stärkerer Fremdfelder sind diese zu erkennen und im Logbuch aufzuzeichnen.

C.2.7.12 Elektromagnetische HF-Felder

Hier sind die Forderungen gemäß EN 61000-4-3 zu erfüllen. Aus dieser Norm wird aus dem Kapitel 5 Prüfpegel (Prüfschärfe) der Prüfschärfegrad von 4 gefordert. Dies entspricht einer Prüffeldstärke von 30 V/m.

C.2.7.13 Stabilität gegen HF-Ströme „Rippelstrom“

Es ist zu gewährleisten, dass die Wechselstörgrößenprüfung nach „FNN-Leitfaden zur Bewertung der Zuverlässigkeit und Messbeständigkeit von Messsystemen“ bestanden wird.

C.2.7.14 Elektrostatische Entladung

Hier sind die Forderungen gemäß EN 61000-4-2 zu erfüllen

- Contact discharge: 8 kV
- Air discharge: 15 kV
- Prüfschärfe 4

C.2.8 Resistenz gegen Oberschwingungsströme

Bei Beeinflussung durch Oberschwingungsströme darf die Funktion und die Messgenauigkeit der Smart Meter nicht beeinflusst werden. Die in der MID erlaubten Fehlergrenzen dürfen nicht überschritten werden. Die Grenzwerte für Oberschwingungsströme im öffentlichen Niederspannungsnetz werden in der EN 61000-3-12 definiert.

C.2.9 Schutzklasse

Es sind ausschließlich Smart Meter der Schutzklasse II zu liefern. Diese Smart Meter müssen ein dauerhaftes und von der Substanz her langlebiges Gehäuse sowie einen Klemmendeckel aus Isoliermaterial besitzen. Die Materialien müssen in Hinblick auf Farbstabilität und Festigkeit UV-stabil sein.

Das Gehäuse muss alle Metallteile des Smart Meters mit Ausnahme von Kleinteilen wie z.B. Eigentumsschilder, Schrauben, Nieten u. a. umschließen.

Wenn solche kleineren Metallteile durch den Normprüffinger gemäß IEC 60529 auf der Außenseite des Gehäuses erreichbar sind, dann müssen diese durch zusätzliche Isolation gegen betriebsmäßig unter Spannung stehende Teile geschützt sein, so dass sie keine Spannung annehmen können, falls die Basisisolierung fehlerhaft wird oder Teile verloren gehen. Die Isoliereigenschaften von Lack, Email, einfachem Papier, Baumwolle, Oxydfilm auf Metallteilen, selbsthaftender Folie und Versiegelung oder ähnlich unsicheren Materialien sind für diese zusätzliche Isolierung nicht ausreichend.

Im Zuge einer Plombierung darf der Plombendraht keine spannungsführenden Teile erreichen können.

C.2.10 Beständigkeit gegen Hitze und Feuer

Der Klemmenblock, der Klemmendeckel und das Gehäuse müssen selbstlöschend, ausreichende Sicherheit gegen die Ausbreitung von Feuer gewährleisten. Sie dürfen nicht durch thermisch überlastete Teile entzündbar sein, falls diese mit ihnen in Berührung kommen. Die in EN 62052-11 und IEC 60695-2-11 diesbezüglich vorgesehenen Prüfungen sind zu erfüllen.

C.2.11 Klimatische Bedingungen und Temperaturbereich

- Betriebsbereich: 3k6 (- 25°C bis +55°C)
- Grenzbereich für Lagerung und Transport: - 25°C bis 70°C

Im gesamten Betriebstemperaturbereich muss die Klassengenauigkeit eingehalten werden.

C.2.12 Eigenverbrauch

Das Design der Geräte muss sicherstellen, dass für alle Betriebsbedingungen die höchstmögliche Energieeffizienz erzielt wird. Es obliegt dem Netzbetreiber energieeffiziente Zähler und Kommunikationsmodule wirtschaftlich zu bewerten. Die von jedem Spannungs- und Strompfad der Smart Meter bei Nennspannung, Nenntemperatur und Nennfrequenz einschließlich Versorgung der Messsysteme aufgenommene Wirk- und Scheinleistung ohne Kommunikation darf die in der EN 50470-3 angegebenen Werte nicht überschreiten.

C.2.13 Zulassung, Eichung, Nacheichung

C.2.13.1 MID- und nationale Zulassung

Für den MID zugelassenen Smart Meter sind die Zulassungsstelle, die Produktionsstätte, sowie die benannte Stelle für die Überwachung der Eichung bekanntzugeben. Es sind die Baumusterprüfbescheinigung mit allen Beilagen und den Deltaquadrat-Werten beim Angebot und bei jeder Versionsänderung vom Hersteller zur Verfügung zu stellen. Die komplette Konformitätserklärung ist bei jeder Smart Meter Lieferung beizulegen.

Der Smart Meter muss für den Einsatz in Österreich zugelassen sein (Temperaturklasse, mechanische Klasse, sowie nationale Zulassung, …).

C.2.13.2 Eichung (und Möglichkeiten für Eingangsprüfung)

Der Status des Eichmodus muss am Smart Meter über die Serviceschnittstelle und am Display erkennbar sein.

Die Smart Meter sind so auszuführen, dass eine automatische Prüfung der geforderten Messpunkte mit den üblicherweise verwendeten Prüfeinrichtungen möglich ist.

Es sind Befehle vorzusehen, die dem Smart Meter von einer Prüfeinrichtung über die Serviceschnittstelle übermittelt und vom Smart Meter ausgeführt werden können, wie z.B.:

- Eichmode EIN
- Eichmode AUS
- Setzen Zeit/Datum
- LED Konstantenerhöhung (für die messtechnische Prüfung)
- Displaytest
- LED Umschaltung Wirk/Blind
- Umschaltung LED-Messperiodenlänge (Kontrolle der 15 Minutenperiode)
- Kumulierung
- Diverse Lese- und Schreibbefehle

C.2.13.3 Leuchtdiode

Mit einem handelsüblichen optischen Tastkopf muss eine Impulsabnahme jederzeit möglich sein.

Die LED-Ausführung muss eine einwandfreie Erfassung der Impulse mit Tastköpfen, die bis zu einem Abstand von 30 mm betrieben werden können, gewährleisten.

Die EN 50470-3 ist einzuhalten.

C.2.13.4 Anordnung von Leuchtdiode und Serviceschnittstelle
Um einen einwandfreien automatischen Eichablauf zu ermöglichen, sind die für die Eichung vorgesehene Leuchtdiode einerseits und die Serviceschnittstelle andererseits so anzuordnen, dass eine gleichzeitige Prüfung bzw. Eichung des Smart Meters über beide Elemente möglich ist.

C.2.13.5 Prüfung des Anlaufverhaltens
Die Messung des Smart Meters muss unter den in EN 62053-21 bzw. vom Bundesamt für Eich- und Vermessungswesen festgelegten Bedingungen beginnen. Die Smart Meter sind so auszuführen, dass sowohl eine automatische Anlaufprüfung (mittels LED) mit den geeigneten Prüfeinrichtungen, als auch eine Prüfung durch Sichtkontrolle (z.B. Energierichtungspfeil am Display) möglich ist. Die Auflösung der LED muss umschaltbar sein, um die Überprüfung zu verkürzen. Die Auflösung der LED muss so einstellbar sein, dass eine Anlaufprüfung (Abgabe von 2 Impulsen) jedenfalls innerhalb von 10 Minuten möglich ist.

C.2.13.6 Prüfung des Leerlaufverhaltens
Der Stillstand eines Smart Meters muss den in EN 62053-21 bzw. den vom Bundesamt für Eich- und Vermessungswesen festgelegten Bedingungen entsprechen.

Der Smart Meter ist so auszuführen, dass sowohl eine automatische Leerlaufprüfung (mittels LED bzw. Serviceschnittstelle) mit den geeigneten Prüfeinrichtungen, als auch eine Prüfung durch Sichtkontrolle am Smart Meter möglich ist. Wenn die Leerlaufbedingung erfüllt ist, muss die Impuls-LED Dauerlicht anzeigen.

C.2.13.7 Stabilität des Impulsintervalls der Leuchtdiode
Für die Eichung des Smart Meters müssen leistungsproportionale Pulsfolgen zur Verfügung stehen, diese müssen so stabil sein, dass Prüfungen über 10 Impulse keine signifikanten Streuungen aufweisen.

C.2.13.8 Eichmodus
Für eine effiziente Prüfung/Eichung muss der Smart Meter einen Eichmodus implementiert haben. Die vom Eichmodus unterstützten Funktionen müssen individuell aktivier- und deaktivierbar sein. Der Status des Eichmodus muss am Display erkennbar sein. Durch einen Spannungsausfall darf der Smart Meter den Eichmodus nicht deaktivieren. Wenn der Eichmodus nicht per Befehl ausgeschalten wird, muss dieser automatisch nach 24 h deaktiviert werden (Timeout).

Der Eichmodus muss folgende Funktionen unterstützen:

- Erhöhung der LED-Impulskonstante
- Wirk/Blind Umschaltung der LED unabhängig der Anzahl der LEDs
- Im Zuge der messtechnischen Überprüfung keine Verstellung des Tastkopfes notwendig
- Umschaltung der LED-Messperiodenlänge (Kontrolle der 15 Minutenperiode)

C.2.13.9 Servicesoftware
Es ist eine Servicesoftware, welche mit allen möglichen Funktionen des angebotenen Smart Meters ausgestattet ist, zur Verfügung zu stellen. Die Lizenzen müssen für den gesamten Smart Meter Park und sämtliches Betriebspersonal zur Verfügung gestellt werden und müssen ein Benutzer- und Berechtigungskonzept beinhalten.

Die Software muss digital signiert und auf aktuellen Betriebssystemen (Windows) mit deutschem Zeichensatz installierbar sein.

Die Lizenzen für jeden Arbeitsplatz müssen alle Softwareupdates während der technischen Lebensdauer der Smart Meter beinhalten. Es dürfen keine Administratorrechte für den Betrieb der Software nötig sein.

Die Software und die jeweiligen Softwareupdates müssen über eine Kommunikationsplattform zum sicheren Datenaustausch zur Verfügung gestellt werden.

Die Servicesoftware muss so gestaltet sein, dass ein Zugriff über die Serviceschnittstelle möglich ist. Speziell muss daher auch auf die Fähigkeit geachtet werden, um mit den Verschlüsselungen der Smart Meter umgehen zu können. Des Weiteren muss es die Möglichkeit geben diese Schlüssel über einen zu definierenden Zeitraum in der Software am Endgerät des Benutzers verschlüsselt abzuspeichern.

Ein dementsprechendes Löschkonzept nach Ablauf des definierten Zeitraumes ist vorzusehen.

Es muss die Möglichkeit geben über eine Importfunktion einzelne oder mehrere (mittels Eingabe direkt in der GUI der Software und über einen Import eines Files mit darin enthaltenen Serialnummern) Serialnummern und einen oder mehrere rollenspezifische Schlüssel herunterzuladen.

Kommunikationseinstellungen müssen konfigurierbar und in der Servicesoftware speicherbar sein (z.B. Message Security Authenticated und Encrypted oder das Ausleseinterface Seriell und den jeweiligen Port, der dafür genutzt wird). Es muss die Möglichkeit geben die Momentanwerte über ein Vektor Diagramm darstellen zu lassen. Hier muss es für den Anwender die Möglichkeit geben die Drehrichtung (Rechtes -/Linkes Drehfeld) zu definieren und einen Standardwert für die Darstellung festzulegen (z.B. Beim Aufruf des Vektor Diagramms wird lt. Phasenfolge ein Rechtes Drehfeld dargestellt). Die Servicesoftware muss eine Funktion vorsehen, welche die Auslesung aller Objekte aus dem Smart Meter und dem Export im „XLSX-Format“ ermöglicht. Weiters muss eine Funktion vorgesehen werden, die einen Vergleich sowie Import von setzbaren und nicht schreibgeschützten Parametern ermöglicht.

Die Installation der Software soll über die im Unternehmen etablierte Softwareverteilung möglich sein (z.B. Softwarecenter, Unternehmensportal, ...)

Bei einem Update der Software muss dafür gesorgt werden, dass das notwendige Schlüsselmaterial (KEKs) auch nach einem Update zur Verfügung stehen.

Es muss die Möglichkeit geben, die für die Authentifizierung in den Systemen notwendigen Benutzernamen und Kennwörter einzutragen und zu aktualisieren, ohne weitere Einstellungen neu setzen zu müssen.

Sämtliche im Objektmodell für die Serviceschnittstelle spezifizierten Objekte und Rollen müssen mit der Servicesoftware unterstützt/konfigurierbar sein.

C.2.14 Messtechnik, Anschluss

C.2.14.1 Klassengenauigkeit

Wirkenergie: Klasse B

Blindenergie: Klasse 3

C.2.14.2 Saldierende Zählung

Entspricht einer antiparallelen Zusammenschaltung zweier mechanischer Drehstromzähler. Es hat die Saldomessung für Bezug und Lieferung über alle 3 Phasen gemäß dem Induktionsmessprinzip zu erfolgen. Es ist jeweils nur in jenes Register (A+ oder A-) zu zählen, in welchem die Energiemenge momentan überwiegt (keine gleichzeitige Registrierung in A+ und A-).

C.2.14.3 Leistungsmaximum

Es wird laufend die mittlere Leistung von aufeinanderfolgenden 15-Minuten-Zeiträumen ermittelt.

Über diese festgelegte springende Messperiode wird ein Leistungsmittelwert ermittelt.

Die Rückstellungen werden über die interne Uhr oder über einen Setzbefehl ausgelöst. Datum und Uhrzeit der Rückstellung werden zusätzlich abgespeichert. Eine Kummuliersperre ist nicht vorzusehen. Eine Rückstellung über eine Taste darf nicht möglich sein.

C.2.14.4 Drehfeldunabhängige Zählung

Die Messung darf durch unterschiedliche Drehfeldkonstellationen, die im Versorgungsnetz vorkommen, nicht beeinflusst werden.

C.2.14.5 Verhalten bei Ausfall und Wiederkehr der Netzspannung

Treten Spannungsausfälle innerhalb einer Messperiode auf, werden keine zusätzlichen Einträge im Lastprofil gemacht, es sind jedoch die entsprechenden Statusbits zu setzen.

Beispiel: Tritt zwischen 10:11 und 10:13 ein Spannungsausfall auf, darf keine Wertabspeicherung mit Zeitstempel um 10:11 oder 10:13 erfolgen. Stattdessen wird bis zum Ende der Messperiode gewartet. Um 10:15 erfolgt dann der Eintrag mit den gemessenen Werten jedoch mit einem Statuseintrag, welcher auf eine Spannungsunterbrechung hinweist.

Bei längeren Spannungsausfällen ist der letzte (unvollständige) Lastprofileintrag vor dem Spannungsausfall mit einem entsprechenden Status zu versehen (Power down). Der erste Wert nach Spannungswiederkehr ist mit Power-Up zu kennzeichnen.

Die Netzteile der Smart Meter 3ph müssen dreiphasig ausgeführt sein und bei Ausfall einer bzw. zweier Phasen der Netzspannung ihre volle Funktionstüchtigkeit erhalten, sofern wenigstens eine Phasenspannung UN + 10% beträgt. Bei Unterbrechung des Neutralleiters darf der Smart Meter keinen dauernden Schaden erleiden und es darf kein Datenverlust eintreten. Bei Wiederkehr der Netzspannung, egal ob 1-, 2- oder 3-phasig, muss der Smart Meter nach spätestens 5s voll funktions-fähig sein (EN 62053-21 Pkt. 8.3.1).

Datensicherungsverhalten bei Spannungsausfall: kein Datenverlust, keine Veränderung gespeicherter Werte!

C.2.14.6 Verhalten bei atypischen Betriebsfällen

Die Bewältigung folgender atypischer Betriebsfälle bei unsachgemäßer Netzbehandlung wird verlangt und darf zu keinem Defekt führen.

Ausfall von 1 Phase, 2 Phasen oder Nullleiter:

- Der Smart Meter muss messtechnisch funktionsfähig bleiben.

Vertauschen von Nullleiter und Phase:

- Ein Vertauschen von L und N darf zu keinem dauerhaften Schaden des Smart Meters führen und muss am Smart Meter angezeigt werden.

C.2.15 Funktionsüberwachung (Smart Meter Selbsttest), Watchdog

Durch den Einsatz einer Watchdog-Funktion soll verhindert werden, dass es zu einer Funktionsbeeinträchtigung des Gerätes durch Softwareversagen kommt. Verhindert wird der Ausfall, indem die Software in regelmäßigen Abständen dem Watchdog mitteilt, dass diese noch ordnungsgemäß arbeiten kann. Bei Ansprechen des Watchdogs hat ein Neustart der Software zu erfolgen.

Es ist eine laufende Plausibilitätsprüfung der Messwerte durchzuführen. Z.B.: Zählerstände dürfen nicht kleiner werden, Leistungen dürfen nicht höher sein als die technisch mögliche Leistung, alle Spannungen dürfen nicht gleichzeitig 0 V sein.

Eichtechnisch relevante Fehler z.B. Speicherfehler sind am Display als F.F. Fehler anzuzeigen, nicht eichtechnisch relevante Fehler sind nicht anzuzeigen, sondern nur im Logbuch zu vermerken.

Zusätzlich muss das Gerät die Watchdog-Funktion zur Überwachung des Betriebsstatus des Kommunikationsmoduls unterstützen. Dazu soll der Smart Meter in regelmäßigen Intervallen eine Routine zur Prüfung des ordnungsgemäßen Betriebs des Kommunikationsmoduls durchführen. Wird bei dieser Prüfung ein fehlerhafter oder instabiler Status des Kommunikationsmoduls erkannt, muss der Smart Meter das Kommunikationsmodul automatisch neu starten.

Watchdog Events, die auf einen Fehler hinweisen, sind im Logbuch zu vermerken.

C.3 Technische Ausführung

C.3.1 Nennströme

Tabelle 2: Nennströme

Größen (EN 50470-1)	**Smart Meter 1ph**	**Smart Meter 3ph**	**Hochampere-Smart Meter 3ph**
I_{Ref} Referenzstrom	5 A	5 A	5 A oder 10 A
I_{max} (max. Strom in Bezug auf Klassengenauigkeit)	60 A	60 A	100 A

I_{st} und I_{min} sind vom Hersteller bekannt zu geben

C.3.2 Messgrößen

Die Messgrößen sind aus dem Hauptdokument bzw. dem Objektmodell zu entnehmen.

C.3.3 Speichertiefe

Der Smart Meter muss für jedes parametrierte Lastprofil die Werte (inkl. Statusinformationen, Datum und Uhrzeit) mindestens 60Tage (entsprechend den gesetzlichen Rahmenbedingungen) im 15 Minutenraster speichern.

Die Speicherung der Lastprofile wird als Ringspeicher nach dem FIFO (First In First Out) Prinzip ausgeführt.

Die Speichertiefe der Logbücher muss jeweils mindestens 500 Einträge sein und als Ringspeicher ausgeführt sein. Ausgenommen sind Logbücher mit eichpflichtigem Charakter. Da diese nicht gelöscht werden dürfen, jedoch nur von der Behörde vorgegebene Änderungen speichern, sind zumindest 300 Einträge vorzusehen.

C.3.3.1 Speichertiefe Vorwerte

Die Vorwerte von Energie und Leistungsregistern müssen bei monatlicher Kumulierung 15 Kumulierungen tief gespeichert werden können. Die monatliche Kumulierung muss sowohl automatisch, jeweils am Monatsersten um 00:00 Uhr, als auch per WAN- und per Serviceschnittstelle ausgelöst werden können. Eine Kumulierung über eine Taste ist nicht zulässig.

C.3.4 Opt-Out Funktion

- Deaktivierung der Aufzeichnung und Übertragung der 15-Minuten und 24-Stunden Lastprofile
- Deaktivierung der Breaker Funktionalität
- Deaktivierung der Leistungsbegrenzungsfunktion
- Displayanzeige, aktivierte Opt-Out Funktion muss am Smart Meter erkennbar sein

C.3.5 Softwarearchitektur der Smart Meter

C.3.5.1 Allgemein

Der Aufbau bzw. die Struktur hat grundsätzlich den Empfehlungen des WELMEC Software Guide 7.2 Softwareleitfaden (Measuring Instruments Directive 2014 / 32 / EU) zu entsprechen. Besonders wird darauf hingewiesen, dass als eine verbindliche Mindestanforderung die Trennung der Firmware in einen eichpflichtigen Teil, in einen nicht eichpflichtigen und einen Teil für die Kommunikation zu erfolgen hat. Der eichpflichtige Teil der Firmware darf ausschließlich nur jene Funktionen beinhalten, welche der MID oder der nationalen Zulassung unterliegen. Alle anderen Funktionen sind ausschließlich in nichteichpflichtigen Teilen zu realisieren. Alle Firmwareteile, ausgenommen eichpflichtiger Werksparameter (z.B. Kalibrierparameter) müssen lokal und von der Ferne aktualisierbar sein.

C.3.5.2 Firmware Update

Die Möglichkeit von inkrementellen Updates und vollen Updates ist vorzusehen.

C.3.5.3 Release Notes

Die Release Notes müssen zumindest Auskunft über folgende Punkte liefern:

- Dokumenten-Header – Dokumentenname, Produktname, Release Nummer, Release Datum, Release Note Datum, Release Note Version, Anforderungsbaseline, Testfallbaseline
- Überblick – Einen kurzen Überblick über die betroffenen Firmwareteile.
- Änderungshistorie – eine kurze Übersicht der neuen Version im Vergleich zur aktuell eingesetzten Version, (z.B. numerisch) welche allgemeinen Features sind neu hinzugekommen bzw. wurden geändert, welche kundenspezifischen Änderungen wurden, inkludiert, welche Bugs wurden gefixt etc.
- Feature Beschreibung – Eine kurze Beschreibung der neuen oder geänderten Features
- Issue Beschreibung – Eine kurze Beschreibung des gefixten Bugs
- Behebungsbeschreibung – Eine kurze Beschreibung wodurch der Bug behoben wurde
- Reproduzierbarkeit – Beschreibung anhand welcher Schritte und in welcher Umgebung ein Bug reproduziert werden konnte
- Betroffenheit – Beschreibung unter welchen Umständen man von einem Bug betroffen ist
- Betriebs-Auswirkung – Welche Auswirkung haben bestimmte Änderungen und Erweiterungen in Bezug auf den Betrieb oder Endbenutzer
- Support-Auswirkung – Welche Anpassungen sind in weiteren Systemen nötig; Was ändert sich in Bezug auflaufende Administrationsroutinen
- Ressourcen-Auswirkung – Angabe der Speicherbelegung pro FW-Teil, Prozessorauslastung
- Dokumentations-Updates: beispielsweise betreffend Updates zu Benutzerhandbüchern, Installations- und Wartungshandbüchern, Designdokumenten, Anforderungsdokumentationen und Dokumentation der Use Cases
- Disclaimers – Firmen sowie standardproduktbezogene Informationen bzgl. Lizenzierung, Nutzungs- und Vervielfältigungsrechte, etc.
- Hersteller-Support-Kontaktinformationen

Mit jeder Auslieferung einer FW für die Smart Meter oder Kommunikationsmodul sowie der Servicesoftware muss ein detailliertes File mit Release Notes mitgeliefert werden.

C.3.6 Anzeigen am Smart Meter

Die Anzeige der folgenden Merkmale im Display ist insofern frei konfigurierbar zu gestalten, dass die Anzeige im rollierenden Modus bzw. über die Aufruftaste definiert werden kann. Die Vorgaben aus dem Dokument „E.3_OE_CS_Lastenheft_Displayguide.pdf“ sind einzuhalten.

Da aus datenschutzrechtlichen Gründen die Anzeige des Lastprofils am Display über die Aufruftaste nur in besonderen Fällen zulässig ist, muss diese Anzeige zusätzlich über die WAN-Schnittstelle als auch über die Serviceschnittstelle am Smart Meter aktivier- bzw. deaktivierbar sein.

Um eine Ablesung bei schlechter Beleuchtung zu gewährleisten, wird eine Hintergrundbeleuchtung bzw. ein kontrastreicher Hintergrund benötigt.

Das elektronische Display hat folgende Mindestanforderungen zu erfüllen:

Messwertanzeige:

- Mind. 10-stellig (Mindestzeichengröße 8x3 mm)
- 7 Vorkommastellen, 3 Nachkommastellen
- Darstellbare Zeichen aus dem ASCII Zeichensatz
- Anzeige der Messgröße (OBIS-Code) im Display kann auf die Darstellung von Medium (A) und Kanal (B) verzichtet werden. Es darf jedoch keine Mehrdeutigkeit entstehen.
- Anzeige der zugehörigen Einheit

Betriebszustandsanzeigen am Display:

- Betriebsanzeige für +A, -A, Q1, Q2, Q3, Q4 Pfeilanzeige, Quadrantenanzeige
- Phasenanzeige: Anzeige der spannungsführenden Phasen bzw. des Drehfeldes (z.B. Blinken bei Linksdrehfeld)
- Optional: Neutralleiterunterbrechung
- Aktuelle Firmware (eich- und nicht eichpflichtige)
- Checksummen lt. Zulassung
- Datum und Uhrzeit
- Anzeige von Momentanwerten frei konfigurierbar (z.B. Strom, Spannung, Leistungsfaktor usw.)
- Aktiver Eichmodus
- Aktueller Status des Klemmendeckelkontakt
- Signalstärke Mobilfunkempfang

Betriebszustandsanzeigen wahlweise am Display oder am Smart Meter selbst:

- Leerlaufanzeige (keine Energieregistrierung)
- Breakerstatus (Ein, Aus, einschaltbereit) und dies als eindeutige Anzeige mit Symbol, Text oder LED
- Status der Schaltkontakte (Ein, Aus)
- Die aktivierte Opt-Out Funktion muss am Smart Meter erkennbar sein
- Im Kommunikationsnetz eingebucht
- Datenübertragung aktiv
- Fehlercodes: Anzeige von ausschließlich eichrelevanter Fehlercodes

C.3.7 Uhren- und Kalenderfunktion

Die Uhr ist quarzgeführt. Das Setzen / Synchronisieren von Datum und Uhrzeit muss über die WAN-Schnittstelle von der Zentrale aus möglich sein sowie über die Serviceschnittstelle vor Ort. Das Setzen von Datum und Uhrzeit über Tastenspiel ist nicht zulässig. Die Sommerzeit/Winterzeit-Umstellung muss parametrierbar (ein- bzw. ausschaltbar) sein. Die Smart Meter müssen auch ohne Kommunikationsanbindung die Sommer- und Winterzeitumschaltung gesichert durchführen. Schaltjahre und fixe österreichische Feiertage müssen bis 2060 berücksichtigt werden.

Für alle beweglichen österreichischen Feiertage (z.B. Ostern) müssen Speicher mit mind. 200 Einträgen zur Verfügung stehen.

Hinsichtlich Ganggenauigkeit müssen die Normen EN 62054-21 bzw. EN 62052-21 erfüllt werden (mindestens 10 ppm).

Verhalten bei Spannungsunterbrechung

Die Uhr muss auch ohne Spannungsversorgung mindestens 10 Tage mit der Genauigkeit entsprechend EN 62054-21 weiterlaufen. Diese Forderung ist zu erfüllen, wenn der Supercap voll aufgeladen ist. Der Smart Meter sollte den Supercap möglichst rasch aufladen. Die Ladezeit bis zum Erreichen der Gangreserve von 10 Tagen ist im Zuge des Angebotes anzugeben.

Bei Ablauf der Gangreserve ist ein entsprechender Protokolleintrag mit Datum und Uhrzeit zu setzen.

Bei Spannungswiederkehr nach Ablauf der Gangreserve hat der Smart Meter beim zuletzt gültigen Zeitwert fortzusetzen.

Verhalten bei Abweichungen der Uhrzeit:

- Bei einer erkannten Zeitabweichung bis zu 2 Sekunden darf keine Aktion erfolgen
- Bei einer Zeitabweichung zwischen 2 und 9 Sekunden muss die Zeit synchronisiert werden. Eine Synchronisation bedeutet keinen Eintrag ins Logbuch.
- Bei einer Zeitabweichung größer 9 Sekunden muss die Zeit gesetzt und eine Eintragung ins Logbuch und ins Lastprofil (Zählerstand mit Datum und Uhrzeit und Statuseintrag) erfolgen. Die zeitliche Chronologie („Durchnummerierung“) der Messwerte muss erhalten bleiben.
- Bei Rückstellungen der Zeit dürfen keine Werte überschrieben oder verändert werden.

C.3.8 Breaker

Der Breaker muss für mindestens 30.000 Schaltspiele unter Volllast ausgelegt sein.

Falls der Breaker den Überlastbereich (Vorzählersicherung- IMax) nicht betriebsmäßig schalten kann, so muss eine interne Logik dafür Sorge tragen, dass nach Beendigung der Überlast, der Abschaltbefehl sofort ausgeführt wird. Jede Zustandsänderung (ein, aus und „ready“ für Einschaltung) muss in das nicht eichpflichtige “Disconnector Control” Logbuch eingetragen, in die Zentrale übertragen und am Smart Meter angezeigt werden.

Folgende Schalterstellungen sind am Smart Meter anzuzeigen:

- Breaker geöffnet
- Breaker geschlossen
- Breaker bereit zur Einschaltung

C.3.8.1 Sperren/Entsperren von Kundenanlagen

Sperrungen und Entsperrungen dürfen nur über Einzelbefehle erfolgen. Smart Meter dürfen auf Massensperrbefehle nicht reagieren.

Die Breakersteuerung wird in den entsprechenden Use Cases beschrieben.

C.3.9 Steuerausgänge

Mindestens 2 Stück bistabile Steuerausgänge min. 5 A (Lambda 0,8) @250 VAC Schaltleistung in Form von potentialfreien Kontakten.

Ansteuerung, durch Schalttabellen im Smart Meter und direkte Schaltbefehle (Serviceschnittstelle, WAN-Schnittstelle).

Bei Spannungsunterbrechung und Wiederkehr muss der gültige Schaltzustand lt. Schalttabelle hergestellt werden.

Mindestschaltspiele: 30.000 unter Volllast.

Der Schaltkontakt muss so konstruktiv gestaltet werden, dass der Klemmblock der Norm entspricht.

Hilfsklemmen müssen zur Aufnahme von 0,25 mm² bis mindestens 1,5 mm² mit Aderendhülse geeignet sein und können auch als schraubenlose Klemmen ausgeführt werden.

C.3.10 Schnittstelle Kommunikationsmodul - Zähler

Die konkrete Ausführung der Schnittstelle zwischen Zähler und Kommunikationsmodul ist dem Dokument „B.3. Anhang_Schnittstellen_Details.pdf“ zu entnehmen. Die Schnittstelle muss allerdings so ausgeführt werden, dass es möglich ist, jedes Kommunikationsmodul desselben Herstellers anzubinden. Die Zählerfirmware muss jedes vom Hersteller bereitgestelltes Kommunikationsmodul unterstützen, sodass bei einem Tausch kein Firmwareupdate am Zähler notwendig ist. Der Zähler muss die Type des Kommunikationsmoduls erkennen und die entsprechende hinterlegte Konfiguration automatisch anwenden. Um unberechtigten Zugriff zu verhindern ist die Schnittstelle ist nach anerkanntem Stand der Technik abzusichern.

C.3.11 Events/Alarme

Smart Meter können Sabotage, Beschädigung als auch technischen Problemen ausgesetzt sein und von Stromausfall (geplant oder ungeplant) betroffen sein. Alarme sind Ereignisse, die von diesen spontan an das zentrale System abgesetzt werden müssen. Events sind Ereignisse, welche im Gerät vor Ort registriert und gespeichert werden und bei Bedarf vom zentralen System ausgelesen werden können.

Die Zuordnung von Ereignissen zu Alarmen / Events hat durch den Netzbetreiber zu erfolgen.

Jeder Event kann in Logbücher eingetragen und als Alarm zugeordnet werden.

Das Öffnen von Klemmendeckel und Gehäusekappe sowie das Entfernen des Kommunikationsmoduls muss sowohl unter Spannung als auch im spannungslosen Zustand registriert werden.

Die Registrierung im spannungslosen Zustand muss durch den Supercap für die Dauer der Gangreserve erfolgen.

C.4 Dokumentation

Um eine ordnungsgemäße Handhabung der Geräte sicherzustellen, sind folgende Unterlagen dem Auftraggeber zur Verfügung zu stellen.

- Systembeschreibung
- Komponentenbeschreibung
- Bedienungsanleitung
- MID und BEV Zulassungsbescheide
- CE-Konformitätserklärung, auch für jedes Kommunikationsmodul
- G3-PLC bzw. G3-Hybrid Zertifikate (FCC)
- DLMS UA Certificate of Compatibility

Oesterreichs Energie Companion Standard
Smart Meter 2.0

E.2_OE_CS_Lastenheft_SM_Messwandler

Version 1.0

31.03.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Einleitung 5

B. Zulassung 5

C. Smart Meter 5

C.1 Generelle Anforderungen 5

C.2 Allgemeine konstruktive Anforderungen 5

C.2.1 Gehäuse allgemein 5

C.2.2 Klemmenblock 5

C.2.3 Zählerkontaktstifte 6

C.2.4 Klemmendeckel 6

C.2.5 Typenschild 7

C.2.6 Seriennummer 8

C.2.7 Anforderungen an die EMV, Isolationsfestigkeit; Luft- und Kriechstrecke 8

C.2.8 Resistenz gegen Oberschwingungsströme 9

C.2.9 Schutzklasse 9

C.2.10 Beständigkeit gegen Hitze und Feuer 9

C.2.11 Klimatische Bedingungen und Temperaturbereich 9

C.2.12 Eigenverbrauch 9

C.2.13 Zulassung, Eichung, Nacheichung 9

C.2.14 Messtechnik, Anschluss 10

C.2.15 Funktionsüberwachung (Smart Meter Selbsttest), Watchdog 10

C.3 Technische Ausführung 11

C.3.1 Nennströme 11

C.3.2 Messgrößen 11

C.3.3 Speichertiefe 11
C.3.4 Opt-Out Funktion 11
C.3.5 Softwarearchitektur der Smart Meter 11
C.3.6 Anzeigen am Smart Meter 11
C.3.7 Uhren- und Kalenderfunktion 12
C.3.8 Breaker 12
C.3.9 Steuerausgänge 12
C.3.10 Schnittstelle Kommunikationsmodul – Zähler 12
C.3.11 Events/Alarme 12
C.3.12 Externe Spannungsversorgung für Typ2 12
C.4 Dokumentation 12

A. Einleitung

Die in diesem Lastenheft dokumentierten Anforderungen für Smart Meter Messwandler stellen die Abweichungen bzw. Ergänzungen zu den Anforderungen im Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“ dar. Die darin zutreffenden Anforderungen gelten auch für Smart Meter Messwandler und müssen erfüllt werden.

B. Zulassung

entsprechend dem Dokument „„E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf““

C. Smart Meter

Definition des Smart Meters: Physikalische Einheit von Zählwerk (eichpflichtige und nicht eichpflichtige Firmware), Display, Kunden-, WAN- und Serviceschnittstelle.

Es werden 2 unterschiedliche Smart Meter Messwandlertypen bei über Messwandler angeschlossenem Smart Meter unterschieden.

TABELLE 1 SMART METER TYPEN

Anschluss-Varianten	**Smart Meter Messwandler CT** **Typ1**	**Smart Meter Messwandler CT/VT** **Typ2**
Nennströme	0,01 - 1(6) A	0,01 - 1(6) A
U_{Nenn} bei Nennfrequenz 50 Hz	3x 230/400 V	3x 58/100 V bis 3x 230/400 V

C.1 Generelle Anforderungen

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2 Allgemeine konstruktive Anforderungen

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.1 Gehäuse allgemein

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.2 Klemmenblock

Wenn die Klemmen in einem Klemmenblock oder in mehreren Klemmenblöcken angeordnet sind, müssen sie eine ausreichende Isolation und mechanische Festigkeit aufweisen. Um diese Forderung zu gewährleisten ist das für die Herstellung der Anschlussklemme(n) vorgesehene Isoliermaterial entsprechend zu prüfen.

Das Material des Klemmenblocks muss die Prüfungen nach ISO 75 für eine Temperatur von 135 °C und einen Druck von 1,8 MPa (Methode A) bestehen.

Einführungen in das Isolationsmaterial, die über die Klemmenbohrungen herausragen, müssen von ausreichender Größe sein, um auch die Isolierung der Leiter einführen zu können.

Die Befestigungsart der Leiter in den Klemmen muss ausreichenden und dauerhaften Kontakt gewährleisten. Es muss verhindert sein, dass sich die Leiter lockern oder übermäßig erwärmen können. Schraubverbindungen, die einen elektrischen Kontakt herstellen, und Schrauben, die während der Lebensdauer des Smart Meters mehrfach angezogen und gelöst werden dürfen, müssen eine Gewindebuchse aus Metall haben.

Die Hauptklemmen sind als Buchsenklemmen mit zwei Klemmschrauben oder Rahmenklemmen durchgängig aus elektrisch leitfähigem Material zur Verwendung von Torx- Schraubendrehern (Größe Tx-20) auszuführen.

Für die Hauptklemmen ist eine Zentrierung für die Drähte gefordert. Alle Schraubenklemmen müssen mit Sicherungen versehen sein, die ein Herausfallen von komplett gelösten Schrauben verhindern. Die Schrauben müssen dabei aber austauschbar sein.

Minimal und maximales Anzugsdrehmoment für alle Schrauben ist bekannt zu geben.

Der Klemmblock muss auch zur Aufnahme von Einzelleitern (mehrdrahtig bzw. feindrahtig mit Adernendhülse) geeignet sein.

Klemmbereich: von 2,5 mm² bis 6 mm².

Schutzart mind. IP51

Die Korrosionsgefahr durch unterschiedliche Kontaktmaterialien ist durch die geeignete Auswahl dieser Werkstoffe zu minimieren.

Elektrische Verbindungen müssen so ausgelegt sein, dass der Kontaktdruck nicht durch das Material der Isolation geführt wird.

Anschlussklemmen mit unterschiedlichem Potential, die eng nebeneinander angeordnet sind, müssen gegen zufälliges Kurzschließen gesichert sein. Dieser Schutz kann durch isolierende Zwischenstücke erreicht werden.

C.2.3 Zählerkontaktstifte

für Smart Meter Messwandler nicht erforderlich

C.2.4 Klemmendeckel

Die Anschlussklemmen des Zählers müssen einen getrennten Klemmendeckel aufweisen, der unabhängig von der Gehäusekappe plombiert werden kann. Der Klemmendeckel muss die Anschlussklemmen, die Befestigungsschrauben für die Leiter und über eine geeignete Länge auch externe Leiter und ihre Isolation, sowie alle Hilfsklemmen abdecken.

Es darf kein Zugang zu den Klemmen möglich sein, ohne die Plombierung des Klemmendeckels zu öffnen. Die Befestigungsschrauben des Klemmendeckels sind mit Torx Tx-20 Schrauben auszuführen.

Die Plombiermöglichkeiten sind so auszuführen, dass eine einfache Plombierung möglich ist, Mindestdurchmesser 3,0 mm für Durchführung des Plombierdrahts.

Klemmendeckel sind aus wiederverwertbarem Isolierstoff entsprechend Schutzklasse II herzustellen.

Der Klemmendeckel muss aus einem undurchsichtigen Kunststoff gefertigt werden.

Schrauben müssen unverlierbar, aber trotzdem tauschbar im Klemmendeckel eingebracht sein (captive Screw). Weiters müssen die Schrauben für mehrmalige Verwendung geeignet sein. Bei der Auslieferung muss der Klemmendeckel bereits auf dem Smart Meter montiert sein.

Es ist gefordert ein Schaltbild für den Anschluss des Smart Meters im Klemmendeckel anzubringen.

Dieses Schaltbild ist mit dem Auftraggeber abzustimmen.

Für Smart Meter Messwandler gilt:
Freiraum zwischen Klemmenblock und Ende des Klemmendeckel (x): 60mm.
Der Klemmendeckel darf in seiner gesamten Länge die Mindesthöhe (y) von 45 mm nicht unterschreiten.

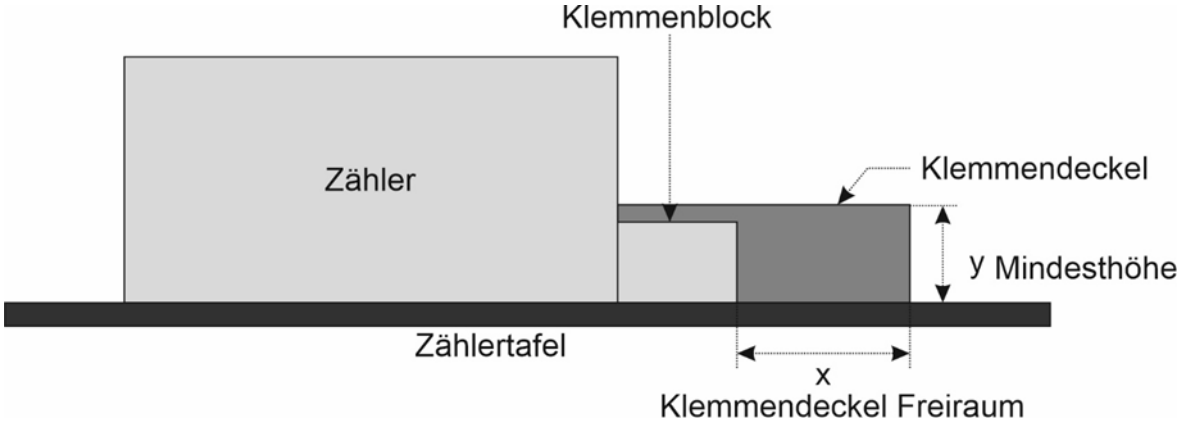


Abbildung 1: Definition der Abmessungen des Klemmdeckels

Das Öffnen des Klemmendeckels muss ohne vorherige Öffnung anderer Gehäuseteile möglich sein.

C.2.5 Typenschild

Der Mindestumfang der Aufschriften am Typenschild aus dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“ sind um folgende Angaben zu erweitern:

- Begriff „Messwandlerzähler“
  Wandlerschild zur Angabe der Messwandlerübersetzung (C = X)

C.2.5.1 Wandlerschild

Das Wandlerschild am Gehäuse des Zählers ist eine rechtlich erforderliche Information des Bundesamtes für Eich- und Vermessungswesen für Endkunden. Darauf werden die Übersetzungsverhältnisse von Strom- und Spannungswandler (Wandlerkonstante) vermerkt.

Größe mindestens. 40 x 20 mm (Länge x Breite)

<u>Beispielhafte Ausführungsvarianten:</u>

1) Austauschbares Wandlerschild

2) Plombierbares Wandlerschild

C.2.6 Seriennummer

Entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7 Anforderungen an die EMV, Isolationsfestigkeit; Luft- und Kriechstrecke

C.2.7.1 Genormte Nennspannungen

Typ 1: Nennspannung: 230/400 V (L1, L2, L3, N)
Typ 2: Nennspannung: 58/100 V bis 230/400 V (L1, L2, L3, N)

C.2.7.2 Toleranzbereich der Netzspannung

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.3 Frequenz

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.4 Netzrückwirkungen

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.5 Medizinische Exposition

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.6 Sicherheit gegen Stoßspannung
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.7 Stoßspannungsfestigkeit
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.8 Erweiterte Blitzschutzfestigkeit
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.9 Elektromagnetische Verträglichkeit
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.10 Störfestigkeit gegen transiente Störgrößen (Burst)
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.11 Magnetische Beeinflussung durch Dauermagneten
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.12 Elektromagnetische HF-Felder
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.13 Stabilität gegen HF-Ströme „Rippelstrom“
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.7.14 Elektrostatische Entladung
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.8 Resistenz gegen Oberschwingungsströme

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.9 Schutzklasse

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.10 Beständigkeit gegen Hitze und Feuer

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.11 Klimatische Bedingungen und Temperaturbereich

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.12 Eigenverbrauch

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13 Zulassung, Eichung, Nacheichung

C.2.13.1 MID-Zulassung und nationale Zulassung
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13.2 Eichung (und Möglichkeiten für Eingangsprüfung)
entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13.3 Leuchtdiode

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“ mit folgenden Impulskonstanten:

- Typ1: 10.000 kWh (kvarh)
- Typ2: 10.000 kWh (kvarh)

C.2.13.4 Anordnung von Leuchtdiode und Serviceschnittstelle

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13.5 Prüfung des Anlaufverhaltens

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13.6 Prüfung des Leerlaufverhaltens

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13.7 Stabilität des Impulsintervalls der Leuchtdiode

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13.8 Eichmodus

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.13.9 Servicesoftware

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.14 Messtechnik, Anschluss

C.2.14.1 Klassengenauigkeit

Typ1: Wirkenergie: Klasse B
Blindenergie: Klasse 2

Typ2: Wirkenergie: Klasse C
Blindenergie: Klasse 1s

C.2.14.2 Saldierende Zählung

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.14.3 Leistungsmaximum

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.14.4 Drehfeldunabhängige Zählung

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.14.5 Verhalten bei Ausfall und Wiederkehr der Netzspannung

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.14.6 Verhalten bei atypischen Betriebsfällen

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.2.15 Funktionsüberwachung (Smart Meter Selbsttest), Watchdog

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3 Technische Ausführung

C.3.1 Nennströme

Tabelle 2: Nennströme

Größen (EN 50470-1)	Smart Meter Messwandler
I_{min} Minimalstrom	0,01 A
I_{Ref} Referenzstrom	1 A
I_{max} (max. Strom in Bezug auf Klassengenauigkeit)	6 A
Thermischer Strom	1,2 x I_{max}

I_{st} ist vom Hersteller bekannt zu geben.

C.3.2 Messgrößen

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.3 Speichertiefe

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.3.1 Speichertiefe Vorwerte

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.4 Opt-Out Funktion

für Smart Meter Messwandler nicht erforderlich

C.3.5 Softwarearchitektur der Smart Meter

C.3.5.1 Allgemein

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.5.2 Firmware Update

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.5.3 Release Notes

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.6 Anzeigen am Smart Meter

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.7 Uhren- und Kalenderfunktion

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.8 Breaker

für Smart Meter Messwandler nicht erforderlich

C.3.9 Steuerausgänge

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.10 Schnittstelle Kommunikationsmodul – Zähler

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.11 Events/Alarme

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

C.3.12 Externe Spannungsversorgung für Typ2

- Die Möglichkeit zum Anschluss einer externen Spannungsversorgung (Hilfsstromversorgung) für den Eigenbedarf des Zählers (Messung, Kundenschnittstelle und Datenübermittlung usw.) muss ausgeführt sein.
- Der Anschluss muss unterhalb des Klemmendeckels ausgeführt sein.
- Hilfsklemmen müssen zur Aufnahme von mindestens 0,25 mm² bis 2,5 mm² mit Aderendhülse geeignet sein und können auch als schraubenlose Klemmen ausgeführt werden.
- Die externe Spannungsversorgung muss für 58 – 277 VAC ausgelegt sein.

C.4 Dokumentation

entsprechend dem Dokument „E.1_OE_CS_Lastenheft_SM_Direktmessung.pdf“

Oesterreichs Energie Companion Standard
Smart Meter 2.0

E.3_OE_CS_Lastenheft_Displayguide

Version 1.0

31.03.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Einleitung - Definition 4

B. Standardmodus 4

C. Menümodus 4

D. Grundlegende Voraussetzungen 4

E. Beispiel Menüführung: 5

A. Einleitung - Definition

Die Menüführung der Anzeige am Display muss mindestens folgende Funktionen erfüllen. Die Bedienung muss vom Hersteller mit den Angaben aus dem Objektmodell (siehe Dokument „D.1_OE_CS_Objektmodel.xlsx“) endkundenfreundlich umgesetzt werden.

B. Standardmodus

In diesem Modus zeigt der Zähler rollierend die Register nach den Einstellungen im Objektmodell des „General display readout (auto-scroll) “ am Display an. Ausnahme ist hier das „Metrological Error Register“, dieses muss beim Auftreten eines kritischen Fehlers automatisch und unabhängig von der Parametrierung angezeigt werden. Dieser Modus stellt den Normalzustand des Zählers dar.

C. Menümodus

Durch Drücken der Bedientaste(n) müssen am Display folgende Anzeigen möglich sein:

- Display-Test-Anzeige (Alle Elemente des Displays werden angezeigt)
- General display readout (manual-scroll)
- Load profile with period 1 (15 Minuten)
- Load profile with period 2 (24h)
- Billing profile with period 1 (monatlich)
- Certification Log

Für die Anzeige der Profile sind zwei Varianten zulässig:

Variante 1:
Die Anzeige der Profile ist durch ein Untermenü möglich (selbe Bedienebene).

Variante 2:
Die Anzeige der Profile ist ein eigener Menüpunkt nach dem Menümodus (weitere Menüebene).

D. Grundlegende Voraussetzungen

Die Anzeige der Profile am Display muss individuell aktivier- bzw. deaktivierbar sein.

Zur Bedienung ist ein kurzer Tastendruck (< 2 Sek), mittlerer Tastendruck (2-5 Sek) und langer Tastendruck (> 5 Sek) vorzusehen, alternativ kann auch ein kurzer doppelter Tastendruck zur Anwendung kommen.

Informationen aus dem „Consumer Message Code - Meter Display“ muss bei Eintrag in der jeweiligen „Capture List“ bei Überlänge horizontal gescrollt werden, bevor das nächste Objekt angezeigt wird.

Es muss von der Menüführung die Möglichkeit geben den oberen Menüpunkt (vorhergehender Menüpunkt) wieder zu erreichen.

Freigabe zur Wiedereinschaltung des Breakers:

- Eindeutige Anzeige der Freigabe zur Wiedereinschaltung am Display.
- Diese Anzeige hat die höchste Priorität und erlischt mit der Einschaltung oder erneuter Sperrung.
- Ein mittlerer Tastendruck schaltet innerhalb der definierten Zeit ohne loslassen der Taste ein.
- Wenn innerhalb von 60 Sekunden keine Taste gedrückt wird oder mit einem langen Tastendruck muss der Zähler in den Standardmodus (auto-scroll) zurückfallen.

Die Bedienung ist im eigenen „Display Guide“ des Herstellers anzugeben.

Es ist kein Servicemenü (Installationshilfe) für die Montage des Zählers vorgesehen.

E. Beispiel Menüführung:

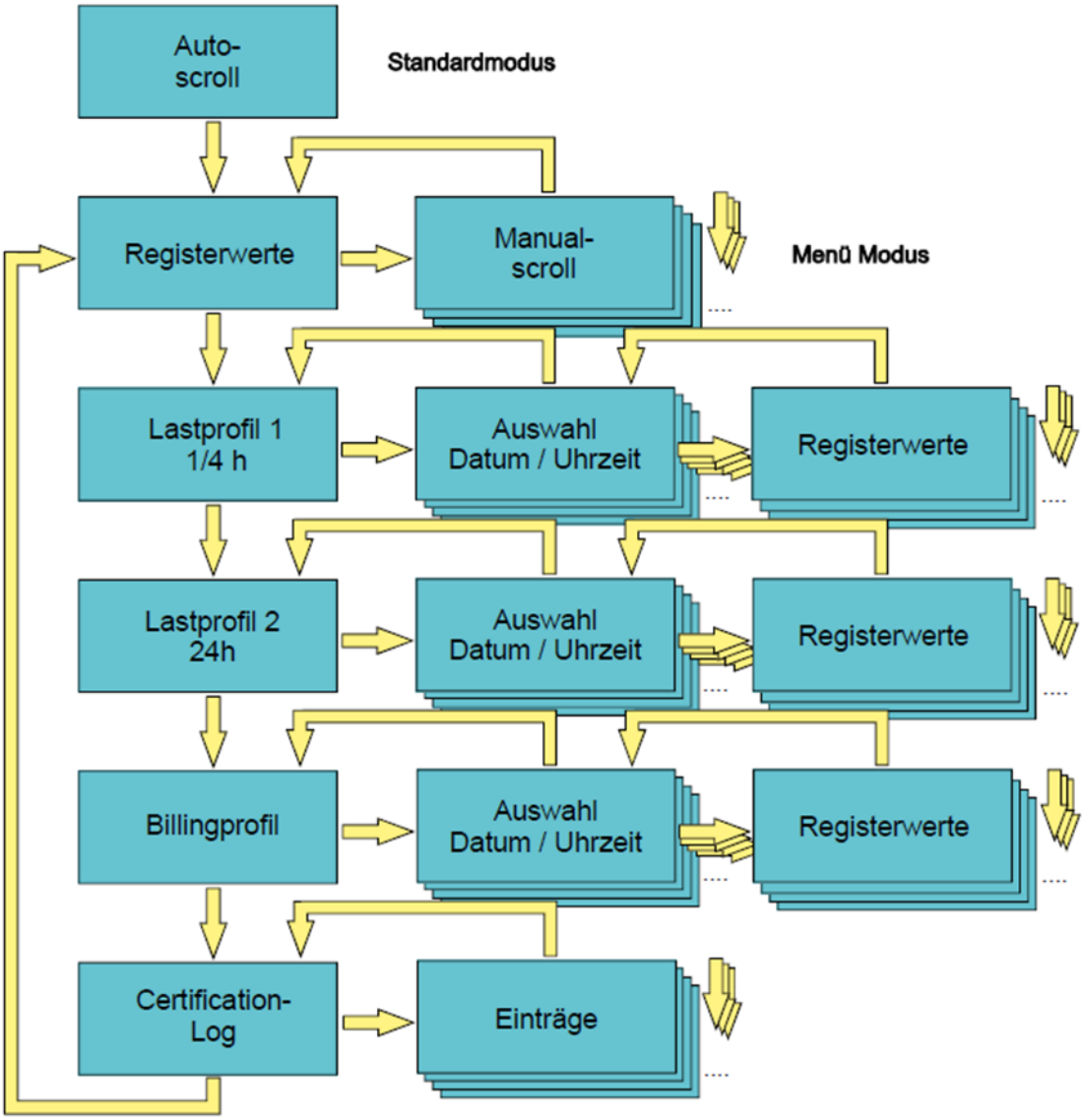


Abbildung 1: Beispiel Menüführung. Jeder gelbe Pfeil stellt einen Tastendruck dar. Die genaue Ausführung ist mit dem Netzbetreiber abzustimmen.

Oesterreichs Energie Companion Standard
Smart Meter 2.0

E.4_OE_CS_Lastenheft_Dualmode-Gateway

Version 1.0

31.03.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Einleitung - Definition 5

B. Allgemeine Anforderungen 5

B.1 Konstruktive Anforderungen 6

B.2 Generelle Gehäuseanforderungen 6

B.3 Spannungsversorgung 7

B.4 Verhalten bei Ausfall und Wiederkehr der Netzspannung 7

B.5 Leistungsschild 7

B.6 Betriebskontrolle vor Ort 8

B.7 Schnittstellen / Modulschächte 8

B.8 Elektromagnetische Verträglichkeit 8

B.8.1 Netzrückwirkungen 8

B.8.2 Sicherheit gegen Stoßspannung 8

B.8.3 Elektromagnetische HF-Felder 8

B.8.4 Störfestigkeit gegen transiente Störgrößen (Burst) 9

B.8.5 Elektrostatische Entladung 9

C. Sicherheitsanforderungen 9

D. Zugriff auf das Dualmode-Gateway 9

E. Betrieb 9

E.1 Inbetriebnahme 9

E.2 Betriebskontrolle vor Ort 9

E.3 Verhalten im Betrieb 10

E.4 Betrieb des Dualmode-Gateways 10

E.4.1 Betrieb als reines Gateway (Gateway-Mode) 10

E.4.2 Dualer Betrieb als Gateway und Datenkonzentrator (Dualmode) 11

E.5 Funktionen des DGW 12
E.5.1 Funktionen im reinen Gateway-Mode 12
E.5.2 Funktionen im dualen Betrieb 12
E.6 G3-PLC Funktionen 13
E.6.1 Allgemeine Anforderungen 13
E.6.2 G3-PLC Netzwerkinformationen 13
E.7 Event-Logbuch 13
E.8 Kommunikations-Logbuch 14
E.9 Firmware-Update 14
E.10 Watchdog, Funktionsüberwachung (Selbsttest) 14
E.10.1 Allgemeine Anforderung 14
E.10.2 Kommunikationsmodulspezifische Anforderungen 14
F. Eigenverbrauch 15
F.1 Leistungsaufnahme 15

A. Einleitung - Definition

Das gegenständliche Dokument beschreibt die möglichen funktionalen Anforderungen an Dualmode-Gateways (DGW) für die G3-PLC bzw. G3-Hybrid Kommunikation. Es obliegt dem Netzbetreiber die konkreten Anforderungen im Rahmen der Ausschreibung festzulegen.

Das Dualmode-Gateway bildet die Übertragungskomponente zwischen G3-PLC bzw. G3-Hybrid Kommunikationsmodulen, der angebundenen Smart Meter und dem zentralen System. Die Kommunikation zwischen dem Kommunikationsmodul der Smart Meter und dem zentralen System erfolgt über die Schnittstellen C und G2 am Dualmode-Gateway.

Gemäß Dokument „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ kann das Dualmode-Gateway auf zwei verschiedene Arten betrieben werden
Siehe Beschreibung in diesem Dokument unter

- E.4.1 Betrieb als reines Gateway (Gateway-Mode)
- E.4.2 Dualer Betrieb als Gateway und Datenkonzentrator (Dualmode)

Diese verschiedenen Betriebsweisen erfordern nicht zwingend unterschiedliche Hardwareausführungen.

B. Allgemeine Anforderungen

TABELLE 1: Allgemeine Anforderungen

Technische Daten	**Mindestanforderung**
Externe Antenne	• Schnittstelle G2: Anschluss einer externen Mobilfunkantenne (z.B. eine SMA-m-Buchse) am Kommunikationsmodul • Schnittstelle C: Anschluss einer externen RF-Antenne
Schutzart	• Schutzklasse II gemäß EN 61140 • Mindestens IP 51
Luftfeuchte	• Mind. 5% bis 90% R.H. (nicht kondensierend)
Spannungsversorgung	• 3 x 230/400 V 50Hz (Weitbereich: 140 V bis maximal 260 V) • Absicherung mit maximal 16 A Sicherung • Anschluss bis maximal 2,5 mm^2 Cu-Leiterquerschnitt
PLC - Übertragungsverfahren	• G3-PLC Übertragungsverfahren nach ITU-T G.9903 (CENELEC A-Band und FCC-Band) • Anbindung von bis zu 1.200 Endgeräten
Meshed Radio (RF)	• Bei G3-Hybrid steht neben der PLC-Kommunikation auch eine RF-Kommunikation zwischen Smart Meter (SM) und dem Dualmode-Gateway zur Verfügung. • Es dürfen nur die in Österreich erlaubten Frequenzen und Sendepegel verwendet werden.
Software	• „Plug and Play“ Installation, ohne vor Ort Parametrierungen durchführen zu müssen. • Updates sind über die WAN- als auch Serviceschnittstelle möglich.
Temperaturbereich	Betriebsbereich: - 25°C bis 55°C Grenzbereich für Lagerung und Transport: - 25°C bis 70°C
Schnittstellen am Gerät	WAN-Ethernet (Für den Anschluss von Kommunikationsgeräten)

	Serviceschnittstelle (Ethernet) WAN-Mobilfunk Schnittstelle ○ optional: realisiert über ein einsteckbares Mobilfunkmodul ○ mögliche Technologien: ▪ LTE CAT-1(bis) (inkl. 450MHz) ▪ LTE CAT-M (inkl. 450MHz) ▪ 5G
Normenkonformität	• Es gelten die einschlägigen Normen entsprechend: „A.1_OE_CS_Gesetze_Normen_und_Standards.pdf“
Netzwerkprotokolle	TCP, UDP, IP, HTTPS, SFTP oder SCP, SNMPv3, CoAP, SSH
Internes Uhrenmodul / Zeitbasis	• **NTPv4 /** (RFC 5905) (Network Time Protocol) Server Synchronisation

B.1 Konstruktive Anforderungen

Das Dualmode-Gateway muss aufgrund der konstruktiven Gestaltung und Herstellung so beschaffen sein, dass bei festgelegten Betriebs- und normalen Einsatzbedingungen keine Gefährdungen auftreten können. Insbesondere muss sichergestellt sein:

- die Sicherheit von Personen gegen gefährliche Körperströme
- die Sicherheit von Personen gegen Auswirkungen erhöhter Temperatur
- die Sicherheit und Beständigkeit gegen Hitze und Feuer
- der Schutz gegen das Eindringen von Festkörpern, Staub und Wasser

Es ist sicherzustellen, dass die elektrischen und magnetischen Felder, welche durch einen typischen Einsatz der angebotenen Komponenten entstehen, die medizinischen Grenzwerte der OVE-Richtlinie R 23-1 nicht überschreiten.

Alle unter normalen Einsatzbedingungen der Korrosion ausgesetzten Teile müssen wirksam geschützt sein. Die Schutzschichten müssen so widerstandsfähig sein, dass sie bei den festgelegten Einsatzbedingungen nicht durch atmosphärische Einwirkungen beschädigt werden können. Diese Anforderungen sind für die Wahl der Schutzklasse maßgebend.

B.2 Generelle Gehäuseanforderungen

- Montagemöglichkeiten über DIN-Hutschiene mit 165 mm und/oder Dreipunktmontage
- Thermisches Design ohne Lüfter und Filter (wartungsfreie Systeme)
- Geeignet für einen 24/7 Dauerbetrieb
- Wahlweise für Einsatzorte innen und außen (d.h. auch in einem Outdoorschrank) geeignet
- Formstabil, UV-beständig, mechanisch beanspruchbar - über die gesamte Produkteinsatzdauer
- Das Gehäuse muss so konstruiert und angeordnet sein, dass eine vorübergehende Deformation den zuverlässigen Betrieb nicht beeinträchtigt
- Das Gehäuse muss plombierbar sein, damit die inneren Teile des Gerätes erst nach Brechen der Plombe(n) zugänglich ist. Eine Entfernung der Gehäusekappe darf ohne Benutzung eines Werkzeugs nicht möglich sein.

B.3 Spannungsversorgung

Die Versorgungsanschlüsse dienen ebenfalls dazu, das PLC-Signal auf allen 3 Phasen aufzuprägen.

Die Befestigungsart der Leiter in den Klemmen muss ausreichenden und dauerhaften Kontakt bis Imax gewährleisten. Es muss verhindert sein, dass sich die Leiter, auch bei mehrfach Befestigung lockern oder übermäßig erwärmen können. Die Korrosionsgefahr durch unterschiedliche Kontaktmaterialien ist durch geeignete Auswahl dieser Werkstoffe zu minimieren.
Elektrische Verbindungen müssen so ausgelegt sein, dass der Kontaktdruck nicht durch das Material der Isolation geführt wird.

Anschlussklemmen mit unterschiedlichem Potential, die eng nebeneinander angeordnet sind, müssen gegen zufälliges Kurzschließen gesichert sein. Dieser Schutz kann durch isolierende Zwischenstücke erreicht werden.

Alle Anschlüsse müssen dauerhaft erkennbar bezeichnet sein.

B.4 Verhalten bei Ausfall und Wiederkehr der Netzspannung

Die Netzteile für den Betrieb an drei Phasen müssen dreiphasig ausgeführt sein und bei Ausfall einer bzw. zweier Phasen der Netzspannung ihre volle Funktionstüchtigkeit erhalten. Bei Unterbrechung des Neutralleiters darf das Dualmode-Gateway keinen dauernden Schaden erleiden und es dürfen keine gespeicherten Parameter oder Logfiledaten verloren gehen.

B.5 Leistungsschild

Am Gerät sind mindestens folgende Aufschriften aufzubringen, welche auch im montierten Zustand – ohne Verwendung weiterer Hilfsmittel – gut leserlich sind:

- Name des Herstellers oder Firmenzeichen
- Typenbezeichnung
- Eindeutige Fabrikationsnummer und das Herstellungsjahr. Die auf dem Leistungsschild vermerkte Fabrikationsnummer muss auch im Geräteinneren (zur Verhinderung von Verwechslungen) dauerhaft vermerkt sein, wenn das Leistungsschild Teil der Gehäusekappe ist. Ein Leistungsschild an abnehmbaren Teilen wie dem Klemmendeckel ist unzulässig.
- Seriennummer lt. Vorgabe des Netzbetreibers
- 2D Data Matrix Barcode lt. Vorgabe des Netzbetreibers
- Bei modularer Ausführung muss auch das Kommunikationsmodul mit eigenen Fabrikations-Seriennummer und 2D Data Matrix Barcode ausgeführt sein.
- Eigentumsvermerk
- Anzahl der Phasen und die Anzahl der Leiter für den elektrischen Anschluss, kann auch in Form von graphischen Symbolen nach EN 62053-52 (Symbole für Wechselstromzähler Teil 52 Symbole) erfolgen
- Spannungsbereich
- Nennfrequenz: in Hertz
- Temperaturbereich
- Zeichen für Schutzisolierung
- CE – Kennzeichen
- Anschlussschema
- Beschreibung der Status-LEDs

Die Ausgestaltung des Leistungsschildes ist mit dem Netzbetreiber abzustimmen

B.6 Betriebskontrolle vor Ort

Das Dualmode-Gateway muss über Anzeigemöglichkeiten verfügen, welche die wichtigsten Betriebszustände der Kommunikation für die vorhandenen Schnittstellen darstellen können (Träger vorhanden, Signalpegel ausreichend, Störung vorhanden etc.).

Es muss eine klare Trennung durch Symbole oder Bezeichnungen pro Schnittstelle für die Statusanzeigen ersichtlich sein, damit Verwechslungen unwahrscheinlich sind.

B.7 Schnittstellen / Modulschächte

Die Schnittstellen bzw. etwaige Modulschächte müssen ein marktübliches, patentfreies Stecksystem bzw. einfache Klemmen aufweisen.

B.8 Elektromagnetische Verträglichkeit

Es darf nicht zu einer Beeinträchtigung/Störung von fremden Anwendungen/Systemen (z.B. Funkanlagen, elektronische Geräte) durch die dezentralen Komponenten kommen. Umgekehrt dürfen die dezentralen Komponenten nicht durch fremde Anwendungen/Systeme gestört werden, die den geltenden EMV-Richtlinien entsprechen.

B.8.1 Netzrückwirkungen

Das Gerät (inkl. Netzgerät und Modem) ist so zu gestalten, dass unzulässig hohe Rückwirkungen in Form von Oberschwingungen auf das Netz nicht gegeben sind. Es ist die Einhaltung der EN 61000-3-2 (Elektromagnetische Verträglichkeit (EMV) Teil 3-2: Grenzwerte für Oberschwingungsströme) zu gewährleisten.

B.8.2 Sicherheit gegen Stoßspannung

Die Geräte müssen nach der EN 61000-4-5 (Elektromagnetische Verträglichkeit Teil 4-5: Prüf- und Messverfahren, Prüfung der Störfestigkeit gegen Stoßspannungen (Surge)) die Prüfungen bei einer Stoßspannungswelle 1,2/50 µs – Puls standhalten.

- Wellenform des Pulses 1,2/50 µs nach EN 60060-1
- Impedanz der Quelle: 2 Ohm ± 10 %, Prüfspannung Scheitelwert von 6 kV.

ODER

Das Gerät ist mit einer Stoßspannungswelle 1,2/50 µs gemäß EN 61000-4-5 bei einem Scheitelwert von 2 kV (vorzugsweise/SOLL mit 4 kV) zu prüfen und es muss der Stoßspannungsprüfung nach EN 62052-11 (Wechselstrom-Elektrizitätszähler – Allgemeine Anforderungen, Prüfungen und Prüfbedingungen – Teil 11: Messeinrichtungen) Kapitel 7.3.2 standhalten.

- Wellenform des Pulses 1,2/50 µs nach EN 60060-1.
- Impedanz der Quelle: 500 Ohm + 50 Ohm, Prüfspannung Scheitelwert von 8 kV.

B.8.3 Elektromagnetische HF-Felder

Hier sind die Forderungen gemäß EN 61000-4-3 zu erfüllen. Bezogen auf Kapitel 5 Prüfpegel (Prüfschärfe) wird ein Prüfschärfegrad von 4 gefordert. Dies entspricht einer Prüffeldstärke von 30 V/m. Das Gerät muss nach EN 55011 funkentstört sein. Eine Beeinflussung der Netzteile durch äußere elektrische und magnetische Felder, die an den Einsatzorten üblicherweise zu erwarten sind, darf nicht erfolgen.

B.8.4 Störfestigkeit gegen transiente Störgrößen (Burst)

Es sind die Forderungen gemäß EN 61000-4-4 zu erfüllen (Prüfschärfe 4).

B.8.5 Elektrostatische Entladung

Es sind die Anforderungen gemäß EN 61000-4-2 zu erfüllen (Schärfegrad 3 oder 4)

- Luftentladung 8 oder 15 kV
- Kontaktentladung 4 oder 8 kV

C. Sicherheitsanforderungen

Das Dualmode-Gateway muss die Anforderungen aus dem Dokument „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ erfüllen. Nur für den Betrieb im Datenkonzentrator Mode muss das DGW aus Sicherheitsgründen mit einem Sicherheitsmodul ausgestattet sein, welches für die sichere Verwahrung der kryptografischen Schlüssel sowie bei der verschlüsselten Speicherung der gesammelten Informationen unterstützt.

D. Zugriff auf das Dualmode-Gateway

Der Zugriff auf das Dualmode-Gateway für Konfiguration und Diagnose muss zumindest über die folgenden drei verschiedenen Methoden möglich sein:

1. Lokaler Zugriff via Serviceschnittstelle auf Web-GUI mittels mobilen Geräts oder Laptop, der über eine Ethernet-Schnittstelle verfügt.
2. Remote Zugriff auf Web-GUI, Adressierung erfolgt via fixer IP-Adresse des Dualmode-Gateways.
3. Remote Zugriff vom Zentralen System via Web-Services.

Der Zugriff erfolgt in (1) und (2) mittels Webbrowser, der sich via https mit dem Dualmode-Gateway verbindet. Als Webbrowser müssen zumindest aktuelle Standardwebbrowser unterstützt werden.

E. Betrieb

E.1 Inbetriebnahme

Grundsätzlich muss das Dualmode-Gateway nach Herstellung der Kommunikationsverbindung unter Einhaltung der Security Rahmenbedingungen eine Selbstidentifikation und eine automatisierte Authentifizierung mit einem zentralen System durchführen. Die Kommunikationsaufbauzeit der Fernschnittstelle muss jedenfalls binnen Minuten stattfinden.

E.2 Betriebskontrolle vor Ort

Das Gerät muss über Anzeigemöglichkeiten verfügen, welche die wichtigsten Betriebszustände der Powerline- und Fern-Kommunikation darstellen können. LEDs können beispielsweise ein- oder mehrfärbig anzeigen.

Am Leistungsschild muss eine klare Trennung durch Symbole oder Bezeichnungen zwischen PLC und Fernkommunikation Statusanzeigen ersichtlich sein, damit Verwechslungen unwahrscheinlicher sind.

Im Falle von integrierter und modularer Mobilfunkkommunikation müssen Signalpegel und Fehlermeldungen angezeigt werden.

E.3 Verhalten im Betrieb

Die folgenden für ein Dualmode-Gateway mit G3-PLC Kommunikation beschriebenen Funktionen gelten sinngemäß auch für Dualmode-Gateway mit G3-Hybrid mit zusätzlicher Möglichkeit zur RF-Kommunikation.

Das PLC-Netzwerk, bei G3-Hybrid auch das RF-Mesh Netzwerk, organisiert sich eigenständig innerhalb der Rahmenbedingungen, welche die Spezifikationen für G3-PLC bzw. G3-Hybrid Systeme vorgeben. Über die WAN- und Serviceschnittstelle sind alle G3-PLC bzw. G3-Hybrid Parameter einstellbar.

Änderungen, Meldungen, Alarme, usw. müssen im Logbuch/Logbüchern (siehe E.7 und E.8) aufgezeichnet werden

E.4 Betrieb des Dualmode-Gateways

Das DGW bietet die Möglichkeit, sowohl als reines Gateway als auch im dualen Modus als Gateway und Datenkonzentrator Nachrichten zu verarbeiten.

Dabei gibt es die folgenden Betriebsmodi der Nachrichtenverarbeitung:

E.4.1 Betrieb als reines Gateway (Gateway-Mode)

In diesem Mode wird eine transparente Ende-zu-Ende-Kommunikationverbindung zwischen dem zentralen System und den Zählern auf Basis von DLMS COSEM hergestellt.

Wird das Dualmode-Gateway im Gateway-Mode betrieben, verfügt es über keine kryptografischen DLMS-Schlüssel oder Berechtigungsnachweise der angebundenen Smart Meter. Dadurch ist das Dualmode-Gateway nicht in der Lage, die durchgeleiteten Daten einzusehen oder zu verändern.

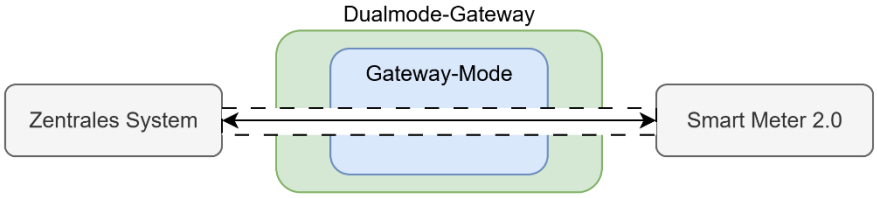


Abbildung 1: Dualmode-Gateway im reinen Gateway-Mode betrieben

Alle Aktionen, die den Smart Meter betreffen, werden ausschließlich vom zentralen System initiiert und gesteuert. Somit initiiert das Dualmode-Gateway selbst keine Aktionen, die den Smart Meter betreffen.

E.4.2 Dualer Betrieb als Gateway und Datenkonzentrator (Dualmode)

In diesem Modus wird die Verarbeitung der Nachricht nach der Quelle unterschieden.

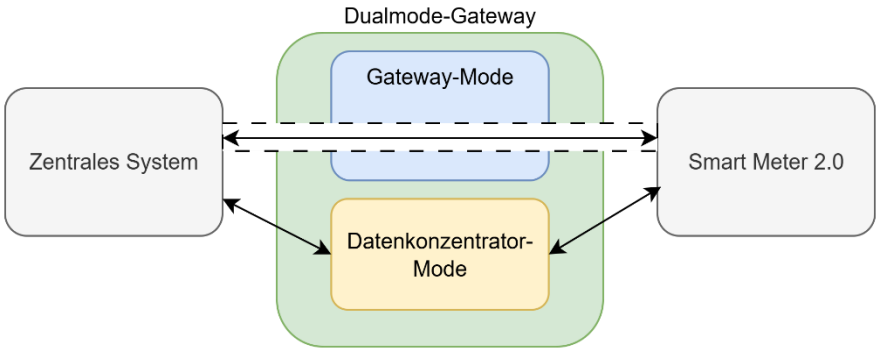


Abbildung 2: Dualmode-Gateway sowohl im Gateway-Mode, als auch im Datenkonzentrator-Mode betrieben.

E.4.2.1 Nachrichten zwischen zentralem System und Smart Meter 2.0 (Gateway-Mode)

Werden Nachrichten zwischen zentralem System und den angebundenen Smart Metern ausgetauscht, werden diese vom Dualmode-Gateway weitergeleitet. Die Verarbeitung folgt den Regeln des reinen Gateway-Betriebs. (E.4.1 Betrieb als reines Gateway (Gateway-Mode).

Die direkte Verbindung zwischen zentralem System und Smart Meter dient vorrangig zur Ausführung von kritischen Befehlen. Diese sind im Dokument „F.1_OE_CS_E2E-Sicherheit-Anforderungskatalog.pdf“ definiert.

E.4.2.2 Nachrichten zwischen DGW und Smart Meter 2.0 (Datenkonzentrator-Mode)

Werden Nachrichten zwischen DGW und den angebundenen Smart Metern ausgetauscht, wird eine DLMS COSEM Verbindung direkt zwischen DGW und den Smart Metern aufgebaut, um die Operationen des Datenkonzentrators durchzuführen. Entsprechende DLMS COSEM Clients stehen hier zur Verfügung und sind in Dokument "B.2_OE_CS_Schnittstellen_Details.pdf" zu finden.

Das DGW sammelt die geforderten Daten entsprechend dem konfigurierten Ausleseplan von den konfigurierten Smart Metern ein und legt dabei alle zwischengespeicherten Informationen so lange verschlüsselt ab, bis diese an das Zentrale System übermittelt werden.

E.4.2.3 Nachrichten zwischen zentralem System und DGW

Werden Nachrichten zwischen zentralem System und DGW ausgetauscht, wird eine Verbindung direkt zwischen zentralem System und DGW aufgebaut. Hier erfolgt die Datenübertragung der Zählerdaten und Konfiguration des DGW.

E.5 Funktionen des DGW

E.5.1 Funktionen im reinen Gateway-Mode

Über folgende Funktionsweisen muss das Dualmode-Gateway im reinen Gateway-Betrieb verfügen:

- Das Zentrale System kommuniziert über das Dualmode-Gateway mit einem SM.
- Ende-zu-Ende Datenverschlüsselung zur Sicherung der zu übertragenden Daten.
- Kommunikation mit SM über G3-PLC.
- Bei Einsatz von G3-Hybrid, zusätzliche Kommunikationsmöglichkeit mit den SM über RF-Mesh.
- Eine Um-Parametrierung der WAN-Schnittstelle von Ethernet zu Mobilfunk und Mobilfunk zu Ethernet muss möglich sein.
- Die Kommunikationsparameter zwischen dem DGW und den zugehörigen SM müssen vollständig konfigurierbar sein.

E.5.2 Funktionen im dualen Betrieb

Zusätzlich zu den Funktionen im reinen Gateway-Mode (E.5.1) müssen folgende Funktionsweisen durch das Dualmode-Gateway zur Verfügung stehen:

- Automatische Sammlung und die Weitergabe von Daten und Events vom SM an das zentrale System. Die Daten werden am DGW zwischengespeichert, bis diese erfolgreich an das zentrale System übermittelt wurden. Nach erfolgreicher und vollständiger Übermittlung stehen die Daten im DGW nicht mehr zur Verfügung.
- Konsequente und zuverlässige Kommunikation mit allen SM und Wiederholungen für nicht erreichbare SM.
- Überwachung von Datum und Uhrzeit der SM und mögliche NTPv4-Synchronisation des DGW mit dem Zentralen System.
- Unterstützung einer Ende-zu-Ende Datenverschlüsselung zur Sicherung der zu übertragenden Daten.
- Intelligente Datenkomprimierung zur Reduktion der Datenmenge.
- Firmware Update-Management für die mit dem DGW in Verbindung stehenden SM.
- Bidirektionale Kommunikation zwischen DGW/Zentralem System sowie DGW/SM
- Folgende Kommunikationsart ist zu unterstützen:
    - Punkt-zu-Punkt: Das DGW kommuniziert direkt mit einem SM
    - Multicast: Nur für die Übertragung von Firmwarepaketen mit eigenem Client erlaubt. Die Initiierung des Update-Prozesses und Aktivierung der Firmware am SM muss Punkt-zu-Punkt erfolgen.
- Folgende periodische Aktionen müssen möglich sein:
    - Periodische Auslesung der SM
    - Automatische Erfassung von neu eingebauten SM
    - Statistik über die Kommunikation
- Folgende PLC-Parameter müssen konfigurierbar sein:
    - Aktionsplan mit zeitlicher Steuerung für die Datenerfassung
    - Die Anzahl der Versuche, um mit fehlenden SM zu kommunizieren
    - Die Priorität für die Datenübertragung
- Lesemodus der SM
    - Die Auslesung der Registerwerte inklusive der Monatswerte, Tageswerte und Lastprofile
    - Die Auslesung der Logbücher
    - Die spontane Auslesung von vordefinierbaren COSEM-Objekten aus den SM (z.B. Wirkleistung, Blindleistung, usw.)

E.6 G3-PLC Funktionen

Das Dualmode-Gateway verfügt über ein integriertes G3-PLC Modul, welches alle Funktionalitäten für die automatisierte Organisation der Smart Meter im PLC-Netzwerk in den Niederspannungsabzweigen der Transformatorstationen bereitstellen muss.

Zusätzlich muss es möglich sein, G3 spezifische Kommandos (z.B. Ping, Route Request, Path Request, etc.) direkt vom Gateway auszuführen.

E.6.1 Allgemeine Anforderungen

- Alle SM mit G3-PLC bzw. G3-Hybrid Kommunikation müssen sich automatisch an dem Dualmode-Gateway anmelden.
- Es ist möglich alle erfassten Adressen der SM (z.B. MAC-Adresse, Identifikationsnummern) in das zentrale System zu laden.
- Es sind Statusinformationen wie Seriennummer des Gerätes, Software-/Firmware Version, Uhrzeit, Datum, verfügbarer und belegter Speicherplatz zur Verfügung zu stellen.
- Es müssen Logfiles für zumindest 1 Woche am Gerät zur Verfügung stehen. Die maximale Dauer der Speicherung beträgt 3 Monate und muss konfigurierbar sein.
- Alle Listen, Adressen, Logbücher etc. sind über einen PULL-Mechanismus über die Serviceschnittstelle SG und vom Zentralen System über G2 auslesbar.

E.6.2 G3-PLC Netzwerkinformationen

Es müssen sämtliche Parameter gem. ITU-T G.9903 für G3-PLC Kommunikation von der Ferne konfigurierbar sein.

Es muss ein NMS (Netzwerk Management System) zur Verwaltung und Wartung das Dualmode-Gateway bereitgestellt werden oder die Integration in ein bestehendes NMS ermöglichen.

E.7 Event-Logbuch

Das Event-Logbuch muss über die Serviceschnittstelle SG auslesbar sein.

Es muss ein Eventlogbuch in Form eines Ringspeichers vorhanden sein, welches zumindest folgende Ereignisse mit Zeitstempel ablegt:

- Durchgeführte DLMS-Sessions
- Ein SM hat sich im PLC-Netzwerk angemeldet.
- Software-Updates
- Zeitsynchronisation

E.8 Kommunikations-Logbuch

Das Gerät muss über ein zusätzliches Kommunikations-Logbuch verfügen, welches ebenso mit einem Ringspeicherverfahren realisiert wird. Anhand dieses Logbuchs muss eine detailliertere Analyse von Fehlern im Kommunikationsablauf zwischen zentralem System und Dualmode-Gateway möglich sein.

Zumindest folgende Ereignisse müssen im Logbuch mit Zeitstempel abgelegt werden:

- Fehler (z.B. Kommunikationsunterbrechungen, Protokollfehler, etc.)
- Warnungen (z.B. Uhrzeitabweichungen)
- Information (z.B. Uhrzeit über NTP synchronisiert)

E.9 Firmware-Update

Über die WAN- und Serviceschnittstelle ist es möglich, einzelne Teile der Software bzw. der Firmware auszutauschen. Dieser Vorgang muss völlig nachvollziehbar bleiben.

Die Übernahme der neuen Firmware erfolgt erst nach automatischer Prüfung, ob die Hardwarekomponenten für das geplante Download kompatibel sind. Prüfroutinen und Selbsttests sind vorzusehen. Ein Rücksprung auf die vorhergehende Software muss im Fehlerfall automatisch erfolgen. Dies ist an das veranlassende System rückzumelden.

E.10 Watchdog, Funktionsüberwachung (Selbsttest)

E.10.1 Allgemeine Anforderung

Durch den Einsatz einer Watchdog-Funktion ist zu verhindern, dass es zu einem Komplettausfall des Gerätes durch Softwareversagen kommt. Verhindert wird der Ausfall, indem die Software in regelmäßigen Abständen dem Watchdog mitteilt, dass diese noch ordnungsgemäß arbeiten kann. Bei Ansprechen des Watchdogs hat ein Neustart der Software zu erfolgen.

Zusätzlich muss ein parametrierbarer Zeitintervall und definierter Befehl (adHoc-Funktion) vorgesehen werden, welcher zu einem Reset führt, der funktional einem Hardreset des Dualmode-Gateways entspricht.

Definition – Hardreset:

Beim Hardreset erfolgt ein vollständiger Neustart des Dualmode-Gateways, der funktional einer realen Spannungsunterbrechung entspricht. Dabei wird die notwendige Hardware in einen Zustand versetzt, der einem Power-Cycle gleichkommt. Ein Hardreset darf keine Konfigurations- oder Nutzdaten löschen und setzt das Gerät bei veränderter Konfiguration nicht in den Auslieferungszustand zurück.

E.10.2 Kommunikationsmodulspezifische Anforderungen

Das Kommunikationsmodul muss eine konfigurierbare Watchdog-Funktion enthalten, welche u. a. die Funktionalität der Verbindung zum Mobilfunknetz überprüft und im Falle von Problemen das Modem neustartet.

F. Eigenverbrauch

Das Dualmode-Gateway muss die EU-Richtlinien zur Energieeffizienz erfüllen (2023/1791/EU).

F.1 Leistungsaufnahme

Es ist der durchschnittliche Eigenverbrauch unter typischen Betriebsbedingungen anzugeben.

Die Messung des durchschnittlichen Eigenverbrauchs unter typischen Betriebsbedingungen erfolgt unter realen Betriebsbedingungen (d.h. schwankender Leistungsfaktor, schwankende Leistung, Messung in einem ausgerollten Gebiet).

Requirements Catalog

End-to-End Security for Smart Metering

Commissioned by Oesterreichs Energie, Brahmsplatz 3, 1041 Wien

By European Network for Cyber Security, Grote Marktstraat 47, 2511 BH Den Haag, The Netherlands

Version:	2026-1.0
Editor:	Project Group End2End Security Smart Metering
Date:	March 26th, 2026
Pages:	90

Disclaimer

Despite careful checking it is not possible to guarantee the accuracy of contents. With the exception of intent and gross negligence, no liability shall be accepted by the issuer and media proprietor for the contents of this document.

This publication is protected by copyright.

Media proprietor:
Österreichs E-Wirtschaft
1040 Vienna, Brahmsplatz 3
Phone: +43 1 501 98- 0
Fax: +43 1 501 98- 900
info@oesterreichsenergie.at,
www.oesterreichsenergie.at

All rights reserved. © 2026

AUTHORS: PG END2END SECURITY SMART METERING, Oesterreichs Energie

MAARTEN HOEVE, European Network for Cyber Security (Projektleitung ENCS)
WOLFGANG LÖW, EVN AG (Projektleitung PG)

STEFAN AUER, Salzburg Netz GmbH
CHRISTIAN BLANK, Illwerke VKW AG
MICHAEL BUSS, Meter Performance Services Ltd
MARTIN BOGENSPERGER, Salzburg Netz GmbH
MARKUS FLOHBERGER, Netz Oberösterreich GmbH
WOLFGANG FRUEWIRTH, Netz Burgendland GmbH
CHRISTIAN HAISJACKL, TINETZ-Tiroler Netze GmbH
LEONARD HASLINGER, LINZ NETZ GmbH
PIA HOSCHEK, Wiener Netze GmbH
GUSTAV KRAIGHER, KNG-Kärnten Netz GmbH
TOBIAS NEBEL, Stromnetz Graz GmbH & Co KG
CHRISTOPH OBERMAIR, Netz Oberösterreich GmbH
DAVID PRODINGER, Salzburg Netz GmbH
MATTHAEUS RIEDLER, Netz Oberösterreich GmbH
ELVIRA SÁNCHEZ ORTIZ, ENCS
ALOIS SCHAFFERHOFER, Stromnetz Graz GmbH & Co KG
MARKUS SCHMIDT, Salzburg Netz GmbH
THOMAS SCHNEIDER, Illwerke VKW AG
ARMIN SELHOFER, Österreichs Energie
MICHAEL SIMMER, Linz AG Telekom
ANDREA STEINBAUER, Energie Steiermark AG
PHILIP STÖGERER, Netz Burgendland GmbH
MARC WALLINGER, Wiener Netze GmbH

Table of Contents

A. Setup ... 6
A.1 Scope ... 6
A.2 Wording ... 6
A.3 Structure of the Requirements ... 7
A.4 Applicability ... 7
A.5 Outline ... 8
B. End-to-End Security Architecture ... 9
B.1 Smart Meter Architecture ... 9
B.1.1 Option A: Directly connected Smart Meter system ... 10
B.1.2 Option B: End-to-End Secure Smart Meter system ... 10
B.1.3 Option C: Dualmode Approach ... 11
B.2 Architecture of the Central System ... 14
B.3 Roles ... 18
B.3.1 Meter Roles ... 18
B.3.2 Dualmode-Gateway Roles ... 20
B.3.3 Central System Roles ... 21
Head-End System ... 21
MDM System ... 22
Customer Portal ... 23
Key Management System ... 23
B.4 Security Events ... 24
C. Secure Meter Communication ... 25
C.1 General Security Requirements ... 25
C.1.1 Future Proof ... 25
C.1.2 Interface Minimization ... 30
C.1.3 Cryptographic Algorithms ... 32
C.2 Data Integrity ... 34
C.3 Resilience ... 44
C.4 Access Control ... 52
C.5 Confidentiality ... 58
C.6 Audits and Logs ... 60
C.7 Product Lifecycle and Governance ... 65
C.8 Secure element ... 71
Appendix A Example Processes ... 75
Appendix A.1 Process for Provisioning of Cryptographic Key Material ... 75
Appendix A.1.1 Requirements for the Process Environment ... 75
Appendix A.1.2 Requirements for Generation and Provisioning ... 76
Appendix A.1.3 Requirements for the Transfer Process ... 76
Appendix A.2 Firmware Update Process ... 77
Appendix A.2.1 Background Digital Signatures ... 77

Appendix A.2.2 Firmware Release Process 78
Appendix A.2.3 Managing and Securing Secret Key Material 78
Appendix A.2.4 Provisioning Process 79
Appendix A.2.5 Update Process of the Device 79
Appendix A.3 Firmware Update Process 79
Appendix A.4 Secured Calibration or Verification Process 80
Appendix A.4.1 Transfer to Calibration or Testing Organization and Transfer of Key Material 80
Appendix A.4.2 Providing a Secure Calibration and Test Mode 80
Appendix A.4.3 Transfer into Operation Mode 81
Appendix A.5 Disposal Process 81
Appendix B Glossary 82
Appendix C References 88

A. Setup

A.1 Scope

This catalog describes the minimum requirements for end-to-end secured Smart Metering in Austria. These requirements apply to manufacturers during tender processes for the Smart Meter, Dualmode-Gateway, Central System, and their communication links. The application of end-to-end security is in accordance with the recommended measures of the risk analysis presented by E-Control Austria (ECA) on 27 February 2014 [1] for the information systems of the electricity industry.

The term *Smart Metering* is not to be confused with the term *Smart Grid*; the security of control and telecommunication systems for electrical transmission and distribution, for example, is not part of this list of requirements. The underlying end-to-end security architecture for Smart Metering is described in Chapter B.

The measures in this catalog are based on the current state of the art in ICT security, i.e., security of the information and communication technology. The objectives of ICT security are to ensure the authenticity and integrity of information in digital data traffic[1], as well as to keep confidential data secret. The terms *secure*, *secured*, and *security* should be understood in this catalog within the context of ICT security. Other interpretations, such as *security* and *safety* in terms of operational safety or accident prevention, are explicitly marked.

This document describes the requirements of the grid operators for manufacturers and suppliers in the tender process for equipment and systems that are used in Smart Metering with end-to-end security.

A.2 Wording

To distinguish between normative and informative content, this requirement catalog follows the terminology of the Technical Guideline TR-03109 (e.g., [2], Section 1.5) of the German Federal Office for Information Security. Keywords are printed in capital letters in accordance with RFC2119 [3]:

- MUST / SHALL means that the requirement is mandatory.
- MUST NOT / SHALL NOT / SHALL NEITHER... NOR means the absolute prohibition of the specification(s).
- SHOULD describes a strong recommendation. Deviations from the recommended specifications must be justified.
- SHOULD NOT identifies a strong recommendation to exclude a specification. Deviations from the recommended specifications must be justified.

[1] Digital data traffic should be understood in terms of the end-to-end Smart Metering architecture (see Chapter B).

- CAN / MAY means that the specifications are optional.

A.3 Structure of the Requirements

Each requirement is labelled with an identifier (Req._ID) and consists of the following three items:

1. Requirement
2. Recommendation and Implementation Guidance
3. Recommended Assurance Activity

These are defined as follows:

1. Requirement: A *Requirement* describes a requirement or expectation that is mandatory. This tender document uses the term *Requirement* in the sense of a normative, i.e. compulsory, requirement.

2. Recommendation and Implementation Guideline: A *Recommendation* describes possibilities for how a requirement can be implemented. A requirement may be solved equivalently as long as the equivalent method is justified in detailed writing. *Implementation Guidelines* provide examples and explanations of how the requirement should be interpreted.

3. Recommended Assurance Activity: *Recommended Assurance Activities* provide suggestions for how the request should be checked. The objective is to make recommendations for both the test organization and the manufacturer, and to notify the manufacturer of expected test processes. These recommended testing procedures are explained in detail in Appendix B.

A.4 Applicability

Unless stated otherwise the requirements apply to the Meter, the Dualmode-Gateway, and the Central System.

The requirements for the security of the software used in the Central System are to be understood as a basis and must be complemented by the security policy of the system operator.

Requirements with an ID ending in “.M” specifically apply to the Meter.

Requirements with an ID ending in “.GW” specifically apply to the Dualmode-Gateway.

Requirements with an ID ending in “.CS” specifically apply to the Central System.

References to a group are labelled with an asterisk, e.g., SXR_01.*.

A.5 Outline

The requirements in this document fall into the following categories:

- Chapter C concerns requirements for the Smart Metering system. In particular, the following areas are covered:
  - General Security Requirements
    - Future Proof
    - Interface Minimization
    - Cryptographic Algorithms
  - Data Integrity
  - Resilience
  - Access Control
  - Confidentiality
  - Audits and Logs
  - Product Lifecycle and Governance
- Appendix A provides descriptions of selected processes. These serve as examples of how selected security requirements can be implemented in terms of end-to-end security. The processes should not be interpreted in a normative sense but as support for better understanding.
- Appendix B contains a glossary of terms and abbreviations.
- Appendix C contains references to guidelines and related literature.

B. End-to-End Security Architecture

B.1 Smart Meter Architecture

The generic architecture of the Smart Metering system is shown in Figure 1. The number of interfaces is kept to the necessary minimum. The descriptions are based on the specifications in the Austrian legislation “Intelligente Messgeräte-AnforderungsVO” (IMA-VO).

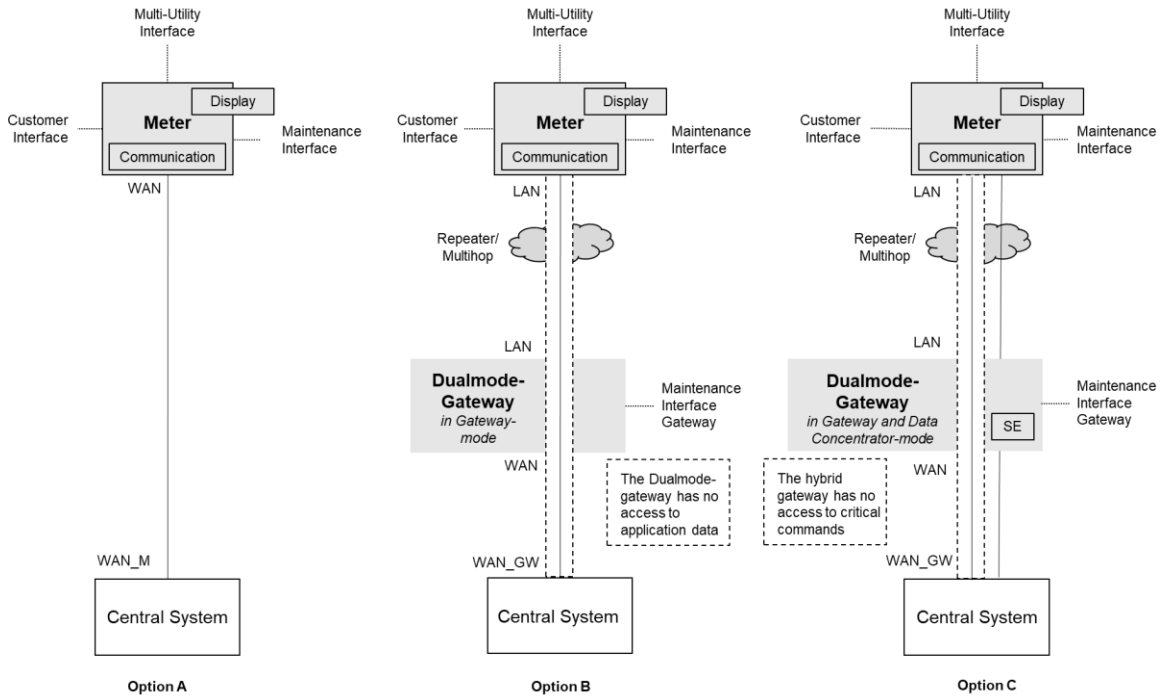


Figure 1: End-to-End Security Architecture for Smart Metering

The end-to-end secure Smart Meter architecture considers two types of meters. The first type are meters connected via a WAN interface to the Central System. The second type are meters that are connected via a local area network (LAN) to a Dualmode-Gateway which is then connected over the WAN to the Central System. The Dualmode-Gateway is placed in a secondary (medium-voltage) substation owned by the Distribution System Operator.

Three different options are allowed for securing the communication between the central system and the head-end. They are described below. In all these options, critical commands to individual meters must be end-to-end secured. Devices between the Central System and the Meter do not have permission to call critical functions, or to change critical settings on the Meter. For this reason, the term *Dualmode-Gateway* is used instead of the term *Data Concentrator*.

In particular, it should be noted that in Option B the Dualmode-Gateway does not store any cryptographic key material to decrypt, modify, or analyse data that is exchanged between the Meters and the Central System. In Option C only the keys for the Dual-mode Gateway role are allowed to be stored on the Dualmode-Gateway, and these are protected by a secure element.

In case the Meter and the WAN or LAN communication module are realized by physically separated components, the interfaces between these components must be secured exclusively with cryptographic methods approved in this document.

For an implementation of the Smart Meter infrastructure, the realization of a multi-layer security concept is also recommended. In addition to the end-to-end secured application layer between the meters and Central System, cryptographic techniques can also be used to secure the lower communication layers. However, security requirements for such a concept are not part of this document.

In the Austrian architecture, the Dualmode-Gateway does not have any connections to authorized third parties, such as utility providers. Communication with third parties is controlled through the central system. Hence, Dualmode-Gateways do not fit the technical description of a Smart meter gateway under the Cyber Resilience Act as included in Implementing Regulation (EU) 2025/2392[2].

B.1.1 Option A: Directly connected Smart Meter system

In architecture option A, Smart Meters communicate directly with the Head-End System over the WAN. The WAN is assumed to be maintained by a party other than the grid operator. The requirements do not cover this network but are set up to provide end-to-end security: the Smart Meter and Central System can ensure the integrity and confidentiality of data sent over the WAN, without depending on any network components in the WAN. Of course, availability will depend on the WAN.

B.1.2 Option B: End-to-End Secure Smart Meter system

In architecture option B, the Dualmode-Gateway is acting in Gateway-Mode. It does not hold any keys and credentials of the smart meters with which it communicates and cannot read or modify the data that passes through it.

[2] See: *Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council*

The requirements for option B are set up so that the communication between Smart Meters and the Central Systems is end-to-end secure. In that sense, option B is like Option A. The difference is that while in Option A all network components are managed by another party, in option B the gateway is managed by the grid operator. Hence, the grid operator must take measures to secure it. Requirements are, therefore, included for the Dualmode-Gateway in Gateway-Mode.

B.1.3 Option C: Dualmode Approach

In Option C, the Dualmode-Gateway is acting in two modes:

- For critical commands (such as switching the breaker, changing keys, or updating the firmware), Dualmode-Gateway is acting in Gateway-mode. The commands are sent from the Central Systems to the Smart Meter over and end-to-end secure connection.
- For reading out measurement data from Smart Meters the meter is acting in Data Concentrator mode. It has keys to connect to the meters in the *Readout gw* role and directly reads out the measurements.

This Dual Mode approach is implemented by separating roles on the Smart Meter, as described in Section B.3 below. The Dualmode-Gateway only gets the credentials for the *FW upload* and *Readout gw* roles, so that it can only gather information from the Smart Meter. It cannot change any settings or perform critical commands such as activating firmware updates or changing keys.

To achieve the same level of security as in Options A and B, a secure element should be used to protect the keys, customer data and other data from the meter that are stored on the Dualmode-Gateway acting in Data Concentrator Mode. Requirements for the secure element are included in Section C.8.

Meter:

The term *Meter* refers to the electricity meter. Other utility meters such as gas, water, or heat, can be connected to the multi-utility interface of the electricity meter.

Communication:	The Meter supports either a WAN or LAN interface.
Display:	Display refers to the integrated display of the meter. The requirements of the IMA-VO apply.
Customer Interface:	The Customer Interface provides current consumption information to the consumer according to the IMA-VO. The interface must implement exclusively unidirectional communication.

Multi-Utility Interface:	Meters for utilities in the gas, water, and heat domains are connected to the Multi-Utility Interface of the electricity meter.
Maintenance Interface:	Access to the electricity meter within the calibration facility, in a test lab, or locally by a technician is realized over the maintenance interface on the electricity meter. The interface must be implemented with bidirectional communication.
LAN Interface:	The LAN Interface of the Meter provides a connection to a Gateway and thus a connection to the Central System. The interface must implement bidirectional communication.
WAN Interface:	The WAN Interface of the Meter provides a direct connection to the Central System. The interface must implement bidirectional communication.

Dualmode-Gateway:

The Gateway is the component within the Smart Metering architecture that provides a transparent communication link between the Central System and the Meter. Transparent is to be interpreted in the context of an end-to-end security architecture.

The term *Gateway* can be seen as the partial functionality of a Data Concentrator reflecting the requirements of end-to-end secured Smart Metering communication.

Maintenance Interface:	The Gateway can be accessed by a technician within a test organization or in the field via the Maintenance Interface. The interface must implement bidirectional communication.
LAN Interface:	The LAN Interface of the Gateway connects the Gateway to the Meters. The interface must implement bidirectional communication.
WAN Interface:	The WAN Interface of the Gateway provides the connection to the Central System. The interface must implement bidirectional communication.

Central System:

The Central System is the central readout and management application that uses and controls the Smart Metering architecture.

WAN_GW Interface:	The WAN_GW Interface of the Central System provides the connections to the Gateways. The interface must implement bidirectional communication.
WAN_M Interface:	The WAN_M Interface of the Central System provides direct connections to the Meters. The interface must implement bidirectional communication.

B.2 Architecture of the Central System

Figure 2 describes the architecture of the Central System. The number of interfaces is kept to the necessary minimum. The arrows indicate whether an interface implements unidirectional or bidirectional communication.

The Central System includes the Head-End, MDMS and a Key Management System of the Smart Meter infrastructure. The Customer Portal is not part of the Central System.

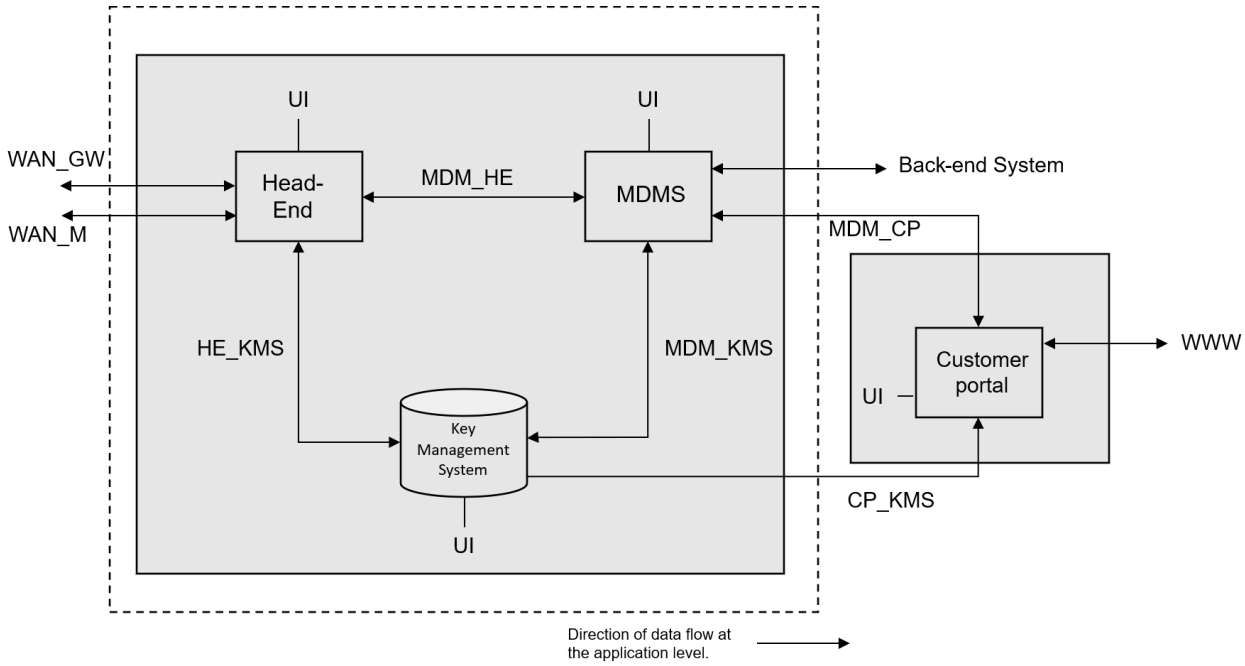


Figure 2: Architecture of the Central System

Head-End System:

The Head-End System communicates with the electricity meters and the Dualmode-Gateway, provides data to the Meter Data Management System (MDMS), and forwards messages from the MDMS to the Meters.

User Interface (UI): Operational and maintenance services of the Head-End System are performed via this interface. The User Interface can also include a remote maintenance interface.

HE_KMS Interface: This interface allows the Head-End System to communicate with the Key Management System.

MDM_HE Interface: The Head-End System and the Meter Data Management System communicate using the MDM_HE Interface.

Meter Data Management System:

The Meter Data Management System (MDMS) stores, processes and manages the metering data and should make this data available for the Customer Portal and internal operating processes. The MDMS can also fulfil functions such as substitute value generation or firmware file management.

User Interface (UI):	Operational and maintenance services of the Meter Data Management System are performed via this interface. The User Interface can also include a remote maintenance interface. In that case, operators should consider additional requirements, such as using two-factor authentication or a jump server, based on a risk assessment.
Back-End System Interface:	This interface connects the Meter Data Management System to the internal Back-End System for internal operating processes. The Back-End System can include systems to analyse and store power quality information from the Meters.
MDM_HE Interface:	The Head-End System and the Meter Data Management System communicate using the MDM_HE Interface.
MDM_KMS Interface:	This interface allows the MDMS to communicate with the Key Management System.

Key Management System:

The Key Management System (KMS) manages and protects cryptographic keys. The KMS provides secure storage for key material and provides access control for the use of the key material. If certificates are used, the KMS can act as the Certificate Authority for the public key infrastructure. The Key Management System should consist of independent components, such as a component used by the Head-End and a separate component for the Customer Portal.

User Interface (UI):	Maintenance services of the Key Management System are performed via this interface. If remote access is used on this interface, strong measures should be taken to prevent and detect unauthorized access.
HE_KMS Interface:	The Head-End System and the Key Management System communicate using the HE_KMS Interface.

MDM_KMS Interface: This interface allows the MDMS to communicate with the Key Management System.

CP_KMS Interface: Customer Portal and the Key Management System communicate using the CP_KMS Interface.

Customer Portal:

The Customer Portal (CP) in this architecture is to be understood as the customer portal of the grid operator not a third party. The Customer Portal provides access for customers and authorized third parties. The Customer Portal is the only zone with access from the public Internet. The Customer Portal is not part of the Central System. This document does not provide detailed security specifications for the Customer Portal.

User Interface (UI): Maintenance services of the Customer Portal are performed via this interface. The User Interface can also include a remote maintenance interface.

Web Interface (WWW): The Web Interface is the connection to the public Internet. Customers and third parties can access the Customer Portal via this interface.

CP_KMS Interface: The Customer Portal and the Key Management System may communicate using the CP_KMS Interface to export keys used on the Customer Interface of the Meter to the Customer Portal. The communication is one-way, in the sense that the Key Management System should not allow the Customer Portal to change keys. Measures, such as the use of proxies, should be taken to protect the Key Management System from attacks through the customer portal.
The Customer Portal may also communicate with the Key Management System indirectly, for instance through the MDMS.

MDM_CP Interface: The Meter Data Management System and the Customer Portal communicate using the MDM_CP Interface. The communication can be unidirectional to protect the MDMS against a corrupted customer portal.

Back-End System Interface: This interface connects the Customer Portal to the internal Back-End System for internal operating processes.

B.3 Roles

This section defines roles and associated privileges for role-based access control roles with respect to the described architecture. The number of roles for the components defined within the architecture is kept to the necessary minimum. The proposed privileges are exemplary. The final privilege settings are to be determined by the grid operator.

B.3.1 Meter Roles

Role	Privileges	Applicability	Meter Interfaces
Management	The *Management* role has access to all memory areas and functions, except for updating the keys of the Security Officer role on the meter.	Central System	WAN or LAN
Data readout	The *Read-Only* role has read access to defined memory areas (register, load profiles, etc.).	Central System	WAN or LAN
FW upload *(only in Option C)*	The *FW upload* role has only the rights to upload firmware. It does not have rights to activate the firmware.	Dualmode-Gateway acting in Data Concentrator Mode	LAN
Comms mgmt	The *Comms mgmt*. role allows to only change the parameters of the meter communications module (such as the PLC or wireless modem).	Communications management system	WAN or LAN
Readout gw *(only in Option C)*	The *Readout gw* role has only the following rights: • Reading consumption data • Reading power quality data • Reading log files The *Readout gw* shall not have any other access right.	Dualmode-Gateway acting in Data Concentrator Mode	LAN
Maintenance	<u>Tasks</u> of the *Maintenance* role: Configure device locally. <u>Privileges</u> of the *Maintenance* role:	Handheld Terminal, Service Application	Maintenance Interface

	Firmware updates, read measurement registers, configuration (e.g., set time, pair with utility meter (gas, heat, water)), set off switch.		
Certification	Tasks of the *Calibration and Testing* role: Provide access for the calibration body, external validation authority, market surveillance, experts or the certification body. Privileges of the *Calibration and Testing* role: Set off switch, configure measurement, read measurement registers, set tariffs, perform firmware update, access log files, parameterization and configuration.	Internal calibration laboratory of the grid operator, External Validation Authority, Market Surveillance, Certification Body	Maintenance Interface
Public	Tasks of the *Public* role: Allows to check the availability of the smart meter and to retrieve the DLMS frame counter to open a secure application association.	All users	WAN, LAN, and Maintenance interface
Security officer	Tasks of the *Security officer* role: Allows to update all keys and credentials on the meter. The security officer role is meant as a backup mechanism in case the Central System would be compromised. In such a scenario, attackers could also change the keys of the Management role and other roles, so that it is no longer possible to communicate with the meters. The Security Officer role can then be used to update the key of the	Central System	WAN or LAN

	Management role to a known key, and in this way restore the meters. For this backup mechanism to be effective, it is recommended to store the keys of the Security Officer role offline, so that they can only be used by the Central System after a manual action by an administrator.		
Pre-established	Tasks of the *Pre-established* role: Allows to send alarms or events to the Central System.	Central System	WAN or LAN
Customer Information Interface (CII)	Tasks of the *CII* role: Unidirectional customer interface to display consumption data. Privileges of the *Customer* role: Read register with the current consumption data as required by the IMA-VO. Note: Access to the register values can take place without input by the customer, e.g., it is possible to send consumption data permanently on the customer interface.	Customer Interface	Customer Interface

B.3.2 Dualmode-Gateway Roles

Role	Privileges	Applicability	Gateway Interfaces

Maintenance	Tasks of the *Maintenance* role: Configure device locally. Privileges of the *Maintenance* role: Firmware updates, read out log files, configuration (e.g., set time).	Handheld Terminal, Service Application	Maintenance Interface
Read only	The *Read-Only* role has read access to defined memory areas (e.g., configuration files or log files).	Central System	WAN
Management	The *Read-Write* role has access to all memory areas and functions. This role can change the privileges of all roles.	Central System	WAN

B.3.3 Central System Roles

This section defines roles and associated privileges for role-based access control roles with respect to the described architecture. The number of roles for the components defined within the architecture is kept to the necessary minimum. The proposed privileges are exemplary. The final privilege settings are to be determined by the grid operator.

Head-End System

Role	Privileges	Applicability	Central System Interfaces
Head-End Maintenance	The *Head-End Maintenance* role can configure the Head-End.	Head-End	User Interface

MDMS	The MDMS uses the *MDMS* role for user authentication at the Head-End.	Head-End	MDM_HE
Operator Read-Only	The user with the *Operator Read-Only* role can read out data from connected Meters or Dualmode-Gateways.	Head-End	User Interface
Operator Read-Write	The user with the *Operator Read-Write* role can read and write data from connected Meters or Dualmode-Gateways.	Head-End	User Interface

MDM System

Role	Privileges	Applicability	Central System Interfaces
Head-End	The Head-End uses the *Head-End* role for user authentication at the MDMS.	MDMS	MDM_HE
MDMS Maintenance	The *MDMS Maintenance* role can configure the MDMS. This role can define which information may be forwarded to the Customer Portal and to the Back-End System.	MDMS	User Interface
Operator Read-Only	The user with the *Operator Read-Only* role can read out data from the MDMS.	MDMS	User Interface
Operator Read-Write	The user with the *Operator Read-Write* role can read and write data in the MDMS.	MDMS	User Interface

Customer Portal

Role	Privileges	Applicability	Central System Interfaces
Customer	The *Customer* role can access one or more records in the Customer Portal. Each customer and third party is assigned an individual role.	Customer Portal	Internet
Customer Portal Maintenance	The *Customer Portal Maintenance* role can configure the Customer Portal.	Customer Portal	User Interface
MDMS_CP	The MDMS uses the *MDMS_CP* role for user authentication at the Customer Portal.	Customer Portal	MDM_CP

Key Management System

Role	Privileges	Applicability	Central System Interfaces
KMS Maintenance	The *KMS Maintenance* role can configure the Key Management System.	Key Management System	User Interface
Customer Portal	The Customer Portal uses the *Customer Portal* role for user authentication at the KMS.	Key Management System	CP_KMS
Head-End	The Head-End uses the role of *Head-End* for user authentication at the KMS.	Key Management System	HE_KMS
MDMS	The Meter Data Management System uses the role *MDMS* for user authentication at the KMS.	Key Management System	MDM_KMS

B.4 Security Events

Each security event should, where possible, log the time, user or system identification (ID), interfaces, as well as the result of the event.

The Meter and Gateway should support at least the following event types:

Event	Device
Logging of a successful or failed user authentication for a particular role.	Meter and Dualmode-Gateway
Firmware Updates • Logging of successful firmware updates. • Logging of failed firmware updates due to invalid digital signatures. • Distinction between receiving a firmware image and the activation of a firmware update.	Meter and Dualmode-Gateway
Setting the system time.	Meter and Dualmode-Gateway
Events that are registered by tamper-detection sensors. These include the opening of device covers, for example.	Meter and Dualmode-Gateway
Startup of the device (boot process).	Meter and Dualmode-Gateway
Performing a reset or reboot of the device.	Meter and Dualmode-Gateway
Reset of error or event registers or the associated log files.	Meter and Dualmode-Gateway
Logging of device errors. See Requirements SRR_02.*.	Meter and Dualmode-Gateway

Reconfiguration of cryptographic parameters. For example, • Update of cryptographic key material for a selected role. • Change of access rights for a selected role. • Reset of random number generator (seed).	Meter and Dualmode-Gateway
Off switch: on/off.	Meter
Events related to utility meters: • Device pairing of utility meter and electricity meter • Update of cryptographic key material for the utility meter	Meter
Modification of the parameters of the load limitation	Meter

C. Secure Meter Communication

C.1 General Security Requirements

C.1.1 Future Proof

Req._ID	
SFR_01.M	**Requirement**
	The Meter SHALL have sufficient memory (volatile and non-volatile) and computational power reserves to allow updates of security functionality. The updatability MUST be ensured throughout the product lifecycle.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that sufficient reserves are available to update security functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. This specifically includes cryptographic algorithms and communication protocols. Please refer to SPR_01. 3. The Meter SHOULD have storage reserved solely for updating security functionality. 4. If DLMS is used, the Meter SHOULD support upgrading to suite 2 for cryptographic algorithms if these are not yet implemented. Suite 2 is required in the *Oesterreichs Energie Companion Standard Smart Meter*

	2.0. To be compatible with this standard, the Meter SHOULD also support the HLS(5) and HLS(7) authentication mechanisms.
	Recommended Assurance Activity
	1. It is recommended to analyse the design documentation provided by the manufacturer.
SFR_01.GW	Requirement
	The Dualmode-Gateway SHALL have sufficient memory (volatile and non-volatile) and computational power reserves to allow updates of security functionality. The updatability MUST be ensured throughout the product lifecycle.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that sufficient reserves are available to update security functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. This includes, in particular, cryptographic algorithms and communication protocols. Please refer to SPR_01. 3. The Dualmode-Gateway SHOULD have storage reserved solely for updating security functionality. 4. If DLMS is used, the Dualmode-Gateway SHOULD support upgrading to suite 2 for cryptographic algorithms if these are not yet implemented. Suite 2 is required in the *Oesterreichs Energie Companion Standard Smart Meter 2.0.* To be compatible with this standard, the Dualmode-Gateway SHOULD also support the HLS(5) and HLS(7) authentication mechanisms.
	Recommended Assurance Activity
	1. It is recommended to analyse the design documentation provided by the manufacturer.
SFR_01.CS	**Requirement**

	The Central System MUST support updates of security functionality. If cryptographic algorithms are implemented in the KMS, it SHALL be possible to update them. The updatability MUST be ensured throughout the product lifecycle.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that sufficient reserves are available to update security functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. This specifically includes cryptographic algorithms and communication protocols. Please refer to SPR_01. 3. If DLMS is used, the Central System SHOULD support upgrading to and suite 2 for cryptographic algorithms if these are not yet implemented. Suite 2 is required in the *Oesterreichs Energie Companion Standard Smart Meter 2.0.* To be compatible with this standard, the Central System SHOULD also support the HLS(5) and HLS(7) authentication mechanisms.
	Recommended Assurance Activity
	1. It is recommended to analyse the design documentation provided by the manufacturer.
SFR_02.M	**Requirement**
	The Meter SHALL allow all parts of the firmware that implement cryptographic algorithms, external communication, and metrology to be updated through local and remote firmware updates.
	Recommendation and Implementation Guidance
	1. See also Requirement SPR_01.
	Recommended Assurance Activity
	1. It is recommended to analyse the design documentation provided by the manufacturer.

	2. It is recommended to carry out a fuzzing test of the firmware update functions.
SFR_02.GW	**Requirement**
	The Dualmode-Gateway SHALL allow all parts of the firmware that implement cryptographic algorithms and external communication to be updated through local and remote firmware updates.
	Recommendation and Implementation Guidance
	1. See also Requirement SPR_01. 2. Remote updates of the Dualmode-Gateway SHOULD be carried out by remote firmware updates or remote patching.
	Recommended Assurance Activity
	1. It is recommended to analyse the design documentation provided by the manufacturer. 2. It is recommended to carry out a fuzzing test of the firmware update functions.
SFR_03.M	**Requirement**
	The Meter SHALL support the capability to locally and remotely update or revoke: • all privileges of the respective roles • all cryptographic keys • public key material that is used for the validation of the digitally signed firmware updates The Meter SHALL allow cryptographic keys used for communication to be updated without support from the manufacturer. The integrity and confidentiality of keys SHALL be protected during updates.
	Recommendation and Implementation Guidance
	1. See Section C.4 for requirements for role-based access control.

	2. An authenticated key exchange protocol SHOULD be used for updating cryptographic keys to protect their integrity. When deploying public key cryptography, the device SHOULD be capable of generating new key pairs together with a certificate signing request. When deploying public key cryptography, the Meter SHOULD be capable of importing new certificates. 3. Privileges and public keys used for firmware signing may be updated through firmware updates.
	Recommended Assurance Activity
	1. This requirement is verified by a functional security test.
SFR_03.GW	**Requirement**
	The Dualmode-Gateway SHALL support the capability to remotely update or revoke • All privileges of the respective roles • all cryptographic keys. • public key material that is used for the validation of the digitally signed firmware updates The integrity and confidentiality of keys SHALL be protected during updates.
	Recommendation and Implementation Guidance
	1. See Section C.4 for requirements for role-based access control. 2. An authenticated key exchange protocol SHOULD be used for updating cryptographic keys to protect their integrity. 3. When deploying public-key cryptography the device SHOULD be capable of generating new key pairs together with a certificate signing request. When deploying public-key cryptography the Dualmode-Gateway SHOULD be capable of importing new certificates.
	Recommended Assurance Activity
	1. This requirement is verified by a functional security test.

SFR_03.CS	**Requirement**
	The Central System SHALL support the capability to update the cryptographic keys of the Meters and Dualmode-Gateways. The Central System SHALL be able to update or revoke privileges or roles on the Meters and Dualmode-Gateways.
	Recommendation and Implementation Guidance
	1. See SIR_01.CS for the protection of the integrity of cryptographic key material. 2. The keys of the Security Officer role can only be updated by the Security Officer role itself, not through the management role, see Section B.3.1. The keys of the Security Officer role SHOULD be kept offline, so that they can only be used by the Central System after a manual action. 3. Privileges and roles may be updated or revoked through firmware updates.
	Recommended Assurance Activity
	1. This requirement is verified by a functional security test.

C.1.2 Interface Minimization

Req._ID	
SMR_01	**Requirement**
	Each interface SHALL support only the functions and protocols needed to meet the functional requirements. Debugging or analysis functions used during the development process SHALL be disabled in production Meters.
	Recommendation and Implementation Guidance

	1. The manufacturer SHOULD provide design evidence that only the described functionality is implemented. Design evidence SHOULD be at a level of detail that enables easy verification. 2. The manufacturer SHOULD provide a complete list of supported data types and supported communication protocols. 3. Examples of debugging or analysis functions are webservers of a Dualmode-Gateway used during the development phase as a debugging tool; or specialized keystroke combinations to enter an engineering menu of a Meter, allowing security-relevant modifications.
	Recommended Assurance Activity
	1. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.
SMR_02	**Requirement**
	Disabled or unused functionality SHALL NOT compromise security.
	Recommendation and Implementation Guidance

	1. The manufacturer SHOULD provide design evidence that any required additional functionality does not compromise security; additional functionality is functionality that goes beyond the operational tasks and regular communication between the Meter and Central System. Design evidence SHOULD be at a level of detail that enables easy verification.
	2. Functionality that is disabled and will never be needed on the device SHOULD be completely removed.
	3. Disabled functionality should be addressable neither via undocumented functions nor through undefined or faulty operating states.
	  - Examples of unused functionality are routines contained in the firmware that are not used in normal operational mode.
	  - Further examples are testing and debugging functions used for initialization during the production process.

	Recommended Assurance Activity

	1. Carrying out a penetration test can provide further assurance that this specification is adequately implemented. 2. Requesting proof of a code review from the manufacturer is recommended.

C.1.3 Cryptographic Algorithms

Req._ID	
SPR_01	**Requirement**
	1. The manufacturer SHALL follow the most recent version one of the following guidelines when employing cryptographic primitives and key lengths: • European Cybersecurity Certification Group Sub-group on Cryptography - Agreed Cryptographic Mechanisms [4] or any newer revision. • BSI TR-02102-1: Cryptographic Mechanisms: Recommendations and Key Lengths [5] or any newer revision • NIST SP 800-57 Part 1 Rev 5, Recommendation for Key Management: Part 1 - General [6] or any newer revision. 2. The manufacturer SHALL NEITHER employ proprietary cryptographic functions NOR modify the cryptographic primitives mentioned in item 1.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence at a level of detail that enables easy verification, including at least the algorithms and key lengths used for all cryptographic functions 2. See SFR_01.* regarding necessary storage for updating cryptographic functions. 3. When using certificates, a trusted time or time source SHOULD be guaranteed on the systems / devices used. 4. In some cases, it may be needed to allow algorithms that are no longer allowed by the above guidelines to be able to communicate with legacy equipment. In that case, a risk assessment SHOULD be performed to

	determine if the older equipment should be updated or the older algorithms may be allowed on the newly procured equipment.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SPR_02	**Requirement**
	All security-relevant random values SHALL be generated by cryptographic random number generators that are in accordance with the guidelines for cryptography in requirement SPR_01. The manufacturer SHALL evaluate the implementation of deterministic random number generators using one of the following methods: • A Common Criteria certification that covers the generator and follows the AIS 20 [7] guidelines. • FIPS 140-3 certification through NIST Cryptographic Module Validation Program [8] at level 1 or higher. • By using an open-source library implementation that has been certified through one of the above methods. The deterministic random number generator SHALL be seeded from a true random source with sufficient entropy following the specifications of the deterministic random number generator.
	Recommendation and Implementation Guidance
	1. The OpenSSL and WolfSSL open-source libraries have been FIPS 140-3 certified. 2. The amount of entropy required for seeding is normally defined in the specification of the deterministic random number generator. 3. The manufacturer SHOULD provide design evidence that this requirement is addressed, including the algorithms used for deterministic random number generator and the way in which these are seeded. Design evidence SHOULD be at a level of detail that enables easy verification. 4. Security-relevant random values are used for the generation of digital signatures, cryptographic keys, or authentication protocols, for example.

	Special care should be taken when (private) keys are generated on the smart meter, as this use case carries a particularly high risk.
	Recommended Assurance Activity
	1. Analysis of the design documentation provided by the manufacturer is recommended. 2. It is recommended that the manufacturer provides a FIPS 140-3 or Common Criteria certificate if they choose to use that evaluation method. 3. If a manufacturer chooses to use a certified open-source library, a code review can be used to verify that this library is used correctly. 4. For additional assurance on the true random source, evaluation using AIS 31 [9] could be requested.

C.2 Data Integrity

Req._ID	
SIR_01.M	**Requirement**
	The Meter SHALL verify the authenticity and integrity of all data received on the following interfaces: • Multi-Utility Interface between the electricity meter and other utility meters. • Maintenance Interface, • LAN between the electricity meter and Dualmode-Gateway, • WAN between the electricity meter and Central System. Both authenticity of the source (sender) and authenticity of the received message SHALL be verified. The message SHALL be dropped if the integrity of the sender or the data cannot be verified.
	Recommendation and Implementation Guidance
	1. Messages SHOULD be authenticated by attaching a message authentication code (MAC).

	2. The authenticity of the sender can be verified by checking the attached valid digital signature. 3. Requirement SPR_01 lists the allowed cryptographic algorithms. 4. In the context of the end-to-end security architecture this requirement concerns the Application Layer (OSI Layers 5-7).
	Recommended Assurance Activity
	1. The manufacturer SHOULD provide design evidence of the implementation of the required functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.
SIR_01.GW	**Requirement**
	The Dualmode-Gateway SHALL verify the authenticity and integrity of data received on the following interfaces: • Maintenance Interface, • WAN Interface to the Central System unless data is passed directly to the Smart Meter, • LAN interface to the Smart Meters unless data is passed directly to the Central System. Both authenticity of the source (sender) and authenticity of the received message SHALL be verified. The message SHALL be dropped if the integrity of the sender or the data cannot be verified.
	Recommendation and Implementation Guidance
	1. Messages SHOULD be authenticated by attaching a message authentication code (MAC). 2. The authenticity of the sender can be verified by checking an attached valid digital signature. 3. Requirement SPR_01 lists the allowed cryptographic algorithms. 4. In the context of the end-to-end security architecture this requirement concerns the Application Layer (OSI Layers 5-7).

	Recommended Assurance Activity
	1. The manufacturer SHOULD provide design evidence of the implementation of the required functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.
SIR_01.CS	**Requirement**
	The authenticity and integrity of data received on all interfaces and data traversing between the implemented zones in the Central System SHALL be verified. Both authenticity of the source (sender) and authenticity of the received message SHALL be verified. The message SHALL be dropped if the integrity of the sender or the data cannot be verified.
	Recommendation and Implementation Guidance
	1. Requirement SRR_04.CS provides details on zoning in the Central System. 2. Messages SHOULD be authenticated by attaching a message authentication code (MAC). 3. The authenticity of the sender can be verified by checking an attached valid digital signature. 4. Requirement SPR_01 lists the allowed cryptographic algorithms. 5. In the context of the end-to-end security architecture this requirement concerns the Application Layer (OSI Layers 5-7).
	Recommended Assurance Activity
	1. The manufacturer SHOULD provide design evidence of the implementation of the required functionality. Design evidence SHOULD be at a level of detail that enables easy verification. 2. Carrying out a penetration test can provide further assurance that this specification is adequately implemented.

SIR_02.M	**Requirement**
	The Meter SHALL verify the validity of all data packets and the format of data received on the following interfaces: • Multi-Utility Interface between the electricity meter and other utility meters, • Maintenance Interface, • LAN between the electricity meter and Central System, • WAN between the electricity meter and Central System.
	Recommendation and Implementation Guidance
	1. Both the device design and implementation SHOULD ensure that the correct functioning of the Meter is not negatively affected by corrupt or deliberately malformed packets. 2. The requirement is valid for all layers in the OSI model.
	Recommended Assurance Activity
	1. It is recommended to carry out fuzzing tests on the described interfaces. 2. The manufacturer should document performed security tests in a sufficient level of detail to allow for validation. The manufacturer should add the performed security tests to the product documentation.
SIR_02.GW	**Requirement**
	The Dualmode-Gateway SHALL verify the validity of all data packets and the format of data received on the following interfaces: • Maintenance Interface, • WAN Interface to the Central System unless data is passed directly to the Smart Meter, • LAN interface to the Smart Meters unless data is passed directly to the Central System.
	Recommendation and Implementation Guidance

	1. Both device design and implementation SHOULD ensure that the correct functioning of the Dualmode-Gateway is not negatively affected by corrupt or deliberately malformed packets. 2. The requirement is valid for all layers in the OSI model.
	Recommended Assurance Activity
	1. It is recommended to carry out fuzzing tests on the described interfaces. 2. The manufacturer should document performed security tests with a sufficient level of detail to allow for validation. The manufacturer should add the performed security tests to the product documentation.
SIR_02.CS	**Requirement**
	The Central System SHALL verify the validity of all data packets and the format of data received on all interfaces as well as for the data exchange between implemented zones.
	Recommendation and Implementation Guidance
	1. Requirement SRR_04.CS provides details on zoning in the Central System. 2. The requirement concerns both the external as well as internal interfaces (zone-to-zone). 3. Both the device design and implementation SHOULD ensure that the Central System is not negatively affected by corrupt or deliberately malformed packets. 4. SQL Sanitization is a countermeasure for SQL injection; it is an example of data validation in the Central System. Further examples of data validation on web servers are described in the ÖNORM A 7700 [10] and in the OWASP Chapter "*Input Validation*" [11]. 5. The requirement is valid for all layers in the OSI model.
	Recommended Assurance Activity
	1. It is recommended to carry out fuzzing tests on the described interfaces.

	2. The manufacturer should document performed security tests with a sufficient level of detail to allow for validation. The manufacturer should add the performed security tests to the product documentation.
SIR_03.M	**Requirement**
	The Meter SHALL verify the integrity of firmware images before they are applied. • The manufacturer SHALL digitally sign the entire firmware update. • Firmware updates without a valid digital signature MUST be dropped. • The firmware update MUST be dropped if its version number is lower than the version number of the installed firmware. • The Meter SHALL support the downgrade to an older firmware version if necessary for operations. Any such downgrade SHALL be imported under a new version number. • Data on the Meter (e.g., stored meter data, log entries or customer specific configurations) SHALL NOT be altered or deleted by a firmware update. • When a firmware update installs new functionality, the functionality SHALL be installed in a secure default configuration. All new parameters in the firmware SHALL be initialized to secure values.
	Recommendation and Implementation Guidance
	1. The ECDSA algorithm with an allowed key strength SHOULD be used to generate a digital signature. See SPR_01. 2. The public key for the validation of the digital signature SHOULD be installed on the Meter during the manufacturing process. See Example Processes in Appendix A. 3. Digitally signed firmware updates can be sent out as a broadcast/multicast. See Example Processes in Appendix A. 4. Adequate release management of the firmware build at the manufacturer SHOULD ensure the digital signature of the image is trustworthy.
	Recommended Assurance Activity
	1. The functional requirement should be verified by testing the implemented firmware update functions.

	2. With respect to the requirements for processes, security audits can be performed as part of acceptance or functional tests. 3. Security audits of development and firmware release processes can be conducted as part of a general security audit, e.g., ISO 27001. 4. Carrying out a fuzzing test to verify that the firmware update functions are adequately implemented.
SIR_03.GW	**Requirement**
	The Dualmode-Gateway SHALL verify the integrity of firmware images before they are applied. • The manufacturer SHALL digitally sign the firmware update. • Firmware updates without a valid digital signature MUST be dropped. • The firmware update MUST be dropped if its version number is lower than the version number of the installed firmware. • The Dualmode-Gateway SHALL support the downgrade to an older firmware version if necessary for operations. Any such downgrade SHALL be imported under a new version number. • Data on the Dualmode-Gateway (e.g., log entries) SHALL NOT be altered or deleted by a firmware update. Necessary changes of the configuration of deployed functions SHALL be carried out automatically during the update process.
	Recommendation and Implementation Guidance
	1. The ECDSA algorithm with an allowed key strength SHOULD be used to generate a digital signature. See SPR_01. 2. The public key for the validation of the digital signature SHOULD be installed on the Dualmode-Gateway during the manufacturing process. See Example Processes in Appendix A. 3. Digitally signed firmware updates can be sent out as a broadcast/multicast. See Example Processes in Appendix A. 4. Adequate release management of the firmware build at the manufacturer SHOULD ensure the digital signature of the image is trustworthy.
	Recommended Assurance Activity

	1. The functional requirement should be verified by testing the implemented firmware update functions. 2. With respect to the requirements for processes, security audits can be performed as part of acceptance or functional tests. 3. Security audits of development and firmware release processes can be conducted as part of a general security audit, e.g., ISO27001. 4. It is recommended to carry out a fuzzing test to verify that the firmware update functions are adequately implemented.
SIR_03.CS	Requirement
	The Central System SHALL verify the integrity of software images before they are applied. • The manufacturer SHALL digitally sign the software update. • Software updates without a valid digital signature MUST be dropped. • The Central System SHALL support the downgrade to an older firmware version if necessary for operations. Any such downgrade SHALL be imported under a new version number.
	Recommendation and Implementation Guidance
	1. The ECDSA algorithm with an allowed key strength SHOULD be used to generate a digital signature. See SPR_01. 2. Adequate release management of the software build at the manufacturer SHOULD ensure the digital signature of the update is trustworthy.
	Recommended Assurance Activity
	1. The functional requirement should be verified by testing the implemented software update functions. 2. With respect to the requirements for processes, security audits can be performed as part of acceptance or functional tests. 3. Security audits of development and update release processes can be conducted as part of a general security audit, e.g., ISO27001.
SIR_04.M	**Requirement**

	The Meter SHALL be able to detect replay attacks on the following interfaces: • Multi-Utility Interface between the electricity meter and other utility meters, • Maintenance interface, • LAN between the electricity meter and Central System, • WAN between the electricity meter and Central System. The Meter MUST drop replayed messages.
	Recommendation and Implementation Guidance
	1. To prevent replay attacks all messages SHOULD be secured in one of the following possible ways: • A sequence number (counter). • An authenticated nonce. It is essential that the nonce is authenticated using a MAC algorithm. • Authenticated encryption using a method such as AES-CBC-CMAC, AES-CCM, or AES-GCM.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SIR_04.GW	**Requirement**
	The Dualmode-Gateway SHALL be able to detect replay attacks on the following interfaces: • WAN Interface to the Central System unless messages are passed on directly to the Smart Meter, • LAN interface to the Smart Meter unless messages are directly passed on to the Central System, • Maintenance Interface. The Dualmode-Gateway MUST drop replayed messages.

	Recommendation and Implementation Guidance
	1. To prevent replay attacks all messages SHOULD be secured in one of the following possible ways: • A sequence number (counter). • An authenticated nonce. It is essential that the nonce is authenticated using a MAC algorithm. • Authenticated encryption using a method such as AES-CBC-CMAC, AES-CCM, or AES-GCM.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SIR_04.CS	**Requirement**
	The Central System SHALL be able to detect replay attacks on all external and internal interfaces and between implemented zones (zone-to-zone). The Central System MUST drop replayed messages.
	Recommendation and Implementation Guidance
	1. To prevent replay attacks all messages SHOULD be secured in one of the following possible ways: • A sequence number (counter). • An authenticated nonce. It is essential that the nonce is authenticated using a MAC algorithm. • Authenticated encryption using a method such as AES-CBC-CMAC, AES-CCM, or AES-GCM. 2. Use of TLS or a VPN can provide this functionality. See also SPR_01.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.

	2. Analysis of the design documentation provided by the manufacturer is recommended.

C.3 Resilience

Req._ID	
SRR_01.M	**Requirement**
	The Meter SHALL separate measurement functionality from communication functionality, so that it keeps measuring electricity correctly under denial-of-service attacks on the communication. Non-security functionality SHALL NOT affect the overall system security. The manufacturer SHALL provide design evidence of compartmentalization of security and non-security functions and blocks.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide documentation that the Meter is sufficiently separated into functional blocks. 2. An example for the separation of functional blocks of the Meter is the separation of metrology and communication. Communication problems SHOULD have no negative impact on the metrology.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that the requirement was adequately implemented. 2. Carrying out a fuzzing test is recommended to provide evidence that functional blocks of the Meter do not affect each other.
SRR_01.GW	**Requirement**

	Separate functional blocks of the Dualmode-Gateway MUST NOT negatively affect each other. Non-security functionality SHALL NOT affect the overall system security. The manufacturer SHALL provide design evidence of compartmentalization of security and non-security functions and blocks.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide documentation that the Dualmode-Gateway is sufficiently separated into functional blocks. 2. An example for the separation of functional blocks of the Dualmode-Gateway is memory protection of separate processes (e.g., routing or remote access).
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that the requirement was adequately implemented. 2. Carrying out a fuzzing test is recommended to provide evidence that functional blocks of the Dualmode-Gateway do not affect each other.
SRR_02.M	Requirement
	The Meter SHALL be *fail-secure*. • Confidentiality and integrity of the data and device functions of the Meter MUST still be guaranteed during failures. • The Meter SHALL not allow access controls to be bypassed remotely during failures. • The Meter SHALL restore availability after software failures as soon as possible. The manufacturer SHALL provide design evidence and test reports that show how the Meter responds to the following failures: • Voltage drop • Integrity errors, e.g., of settings, configurations or log files • Failures during self-tests of the Meter

	• Failures during execution of cryptographic functions • Failures during validation of login credentials • Failures when entering data (wrong data format, wrong data length, invalid commands, etc.) • Failures when using the local buttons (pressing buttons too fast or at the same time)
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that the Meter is fail-secure. 2. This can be addressed by implementing a watchdog functionality that allows the Meter to maintain a secured operational state in the event of a failure. 3. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SRR_02.GW	**Requirement**
	The Dualmode-Gateway SHALL be *fail-secure*. • Confidentiality and integrity of data and device functions of the Dualmode-Gateway MUST still be guaranteed during failures. • The Dualmode-Gateway SHALL not allow access controls to be bypassed remotely during failures. • The Dualmode-Gateway SHALL restore availability after software failures as soon as possible. The manufacturer SHALL provide design evidence and test reports that show how the Dualmode-Gateway responds to the following failures: • Voltage drop

	• Integrity errors, e.g., of settings, configurations or log files • Failures during self-tests of the Meter • Failures during execution of cryptographic functions • Failures during validation of login credentials • Failures when entering data (wrong data format, wrong data length, invalid commands, etc.)
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that the Dualmode-Gateway is fail-secure. 2. This can be addressed by implementing a watchdog functionality that allows the Dualmode-Gateway to maintain a secured operational state in case of a failure. 3. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SRR_02.CS	**Requirement**
	The Central System SHALL be *fail-secure*. • Confidentiality and integrity of the data and device functions from components of the Central System MUST still be guaranteed during failures. • The Central System SHALL not allow access controls to be bypassed remotely during failures. • The Central System SHALL restore availability after software failures as soon as possible. The manufacturer SHALL provide design evidence and test reports that show how the Meter responds to the following failures:

	• Integrity errors, e.g., of settings, configurations or log files • Failures during execution of cryptographic functions • Failures during validation of login credentials • Failures when entering data (wrong data format, wrong data length, invalid commands, etc.)
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence that the Central System is fail-secure. 2. The manufacturer SHOULD provide design evidence for which relevant failures are covered and how these were tested. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness. 2. Analysis of the design documentation provided by the manufacturer is recommended.
SRR_03.M	**Requirement**
	Physical manipulations of the Meter SHALL be recognizable. • The meter case SHALL provide sufficient protection against physical manipulations. • The Meter case SHALL be sealed where possible. • Additionally, the opening of the terminal cover and separately the case of the Meter SHALL be recognized using suitable means such as contacts or sensors. Any opening of the terminal cover or case SHALL generate an event in the security log. • If the Meter possesses any removable parts, the removal of such a part SHALL generate an event in the security log. An independent penetration test of the physical security MUST be conducted.
	Recommendation and Implementation Guidance

	1. The security log is defined in Requirement SLR_01.M. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification. 3. It SHOULD be possible to seal the meter case and the terminal cover. 4. The penetration tests SHOULD be conducted over an adequate period by an experienced tester.
	Recommended Assurance Activity
	1. Analysis of the vulnerabilities reported in the penetration test is recommended.
SRR_03.GW	**Requirement**
	Physical manipulations of the Dualmode-Gateway SHALL be recognizable. • The case SHALL provide sufficient protection against physical manipulations. • If the Dualmode-Gateway possesses any removable parts, the removal of such a part SHALL generate an event in the security log.
	Recommendation and Implementation Guidance
	1. The security log is defined in Requirement SLR_01.GW. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SRR_04.CS	**Requirement**
	1. The Central System SHALL support separation into at least the following zones: a. Head-End System

	b. Key-Management System (KMS) c. Meter-Data Management System (MDMS) 2. It MUST be possible to limit communication between the zones and from the zones to external systems.
	Recommendation and Implementation Guidance
	1. Generic examples for mechanisms to separate zones are: • Firewalls: A firewall controls the information flow between two components. Note that wrong configuration of firewalls can be disastrous: the configuration flexibility provided by a firewall can easily lead to misconfigurations, making way for an attacker. • Network gateways[3]: A gateway regulates which components may communicate with each other. • Data diodes: A data diode enforces traffic flowing only in one direction. The receiving end has no permissions to send data to the sender and thus cannot be abused as entry point for an attack. Data diodes are more secure but also much less flexible than firewalls or gateways. • Micro kernels: a micro kernel or hypervisor enables the separation of processes and thus provides the possibility to enable zoning without hardware separation. 2. If possible, the separation functionality should be implemented as an individual component.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SRR_05.CS	**Requirement**
	The Central System SHALL store cryptographic keys in a secured environment of a Key Management System. This secured environment SHALL at least comply with Level 3 in FIPS 140-2 [8].

[3] Here the term “gateway” should be understood as a classical means to connect computer networks.

	Recommendation and Implementation Guidance

	1. Usage of cryptographic functions and keys is detailed in SPR_01.
	2. The use of cryptographic keys outside of the secured environment SHOULD be minimized.
	  ○ Processes SHOULD be designed to only give devices the keys they need. So, Dualmode-Gateway acting in Data Concentrator Modes SHOULD only get keys for the meters connected to them, and handheld terminals or mobile devices SHOULD only get keys needed to perform their work orders.
	  ○ If keys are exported to devices outside of the smart metering systems, such as handheld terminals or mobile devices, the keys SHOULD only be usable for a limited time. They SHOULD be purged from the device after use and be changed on the Meter or Dualmode-Gateway. The time for which a key may remain valid SHOULD be determined through a risk assessment.
	  ○ The Central System SHOULD enforce a limit on how many keys a device such as a Dualmode-Gateway acting in Data Concentrator Mode or handheld terminal can obtain.
	3. Keys SHOULD NOT leave the secured environment unencrypted.
	4. It SHOULD be possible to generate new cryptographic keys within the secured environment.
	5. The interface connecting the secured environment and the Key Management System SHOULD use an open interface standard, such as PKCS #11 [12].
	6. All interfaces of the secured environment SHOULD be clearly documented.
	7. It SHOULD be possible to limit the intervals of access to the secured data.
	8. It SHOULD be possible to secure selected data (and keys in particular) using the four-eyes principle.

	Recommended Assurance Activity
	1. Analysis of the design documentation and certifications provided by the manufacturer is recommended.
SRR_06.CS	**Requirement**

	The Central Systems SHALL be protected from threats coming from the Customer Portal. It SHALL not be possible to compromise the integrity of the information in the MDMS from the Customer Portal.
	Recommendation and Implementation Guidance
	1. Operators SHOULD define security requirements for the Customer Portal based on a risk assessment. The Customer Portal is not in scope for the requirements in this document.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance of the design robustness.

C.4 Access Control

Req._ID	
	Requirement
SAR_01.M	The Meter SHALL support Role Based Access Controls (RBAC) to protect the device from unauthorized access by enforcing different access rights based on the role of a user. • The Meter SHALL allow to implement the role model as defined in Section B.3.1. • It MUST be possible to configure the privileges of individual roles. • It MUST be possible to assign individual key material to each role. These keys MUST be updatable. • It MUST be possible to bind roles to interfaces. • It MUST be possible to define more roles for future applications that are implemented remotely or via firmware updates.

	• It MUST be possible to disable all implemented roles remotely and individually.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each role has only the defined and necessary privileges.
SAR_01.GW	**Requirement**
	The Dualmode-Gateway SHALL support Role Based Access Controls (RBAC) to protect the device from unauthorized access by enforcing different access rights based on the role of a user. • The Dualmode-Gateway SHALL support at least the roles defined in Section B.3.2. • It MUST be possible to configure the privileges of individual roles. • It MUST be possible to assign individual key material to each role. These keys MUST be updatable. • It MUST be possible to bind roles to interfaces. • It MUST be possible to define more roles for future applications that are implemented remotely or via firmware updates. • It MUST be possible to disable all implemented roles remotely and individually.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.

	2. When the gateway uses keys to authenticates to the users (for instance when using certificates in a web interface), it is required to support individual keys for each gateway by SFR_03.GW.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each role has only the defined and necessary privileges.
SAR_01.CS	**Requirement**
	The Central System SHALL support Role Based Access Controls (RBAC) to protect against unauthorized access by enforcing different access rights based on the role of a user. • The Central System SHALL support at least the roles defined in Section B.3.3. • It MUST be possible to configure the privileges of individual roles. • It MUST be possible to assign individual key material to each role. These keys MUST be updatable. • It MUST be possible to bind roles to interfaces. • It MUST be possible to define more roles for future applications that are implemented remotely or via software updates. • It MUST be possible to disable all implemented roles individually. The Central System SHALL have measures to ensure that authorized users cannot switch the breaker on large numbers of Meters in a short time.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification. 2. The connection between user authorization (e.g., passwords or smartcards) and the roles SHOULD be implemented using a suitable system, such as LDAP. 3. It SHOULD be possible to set up roles to enable access using the four-eyes principle.

	4. The Central System SHOULD support individual user accounts by integrating with a central access control system, such as Active Directory. 5. The measures against switching the breaker large numbers of meters SHOULD also prevent users from indirectly switching, for instance by putting scripts on the Central System or the Meter, setting actions with a certain timer, or limiting the maximum electricity use to zero.
	Recommended Assurance Activity
	1. It is recommended to conduct a functional test of the appropriate role-based access controls. This is to ensure that in the implementation of each role only the necessary permissions were provided.
SAR_02.M	**Requirement**
	The Meter SHALL support mechanisms to prevent and detect unauthorized access.
	Recommendation and Implementation Guidance
	1. The Meter SHOULD implement mechanisms to detect unauthorized access attempts. Where possible, the Meter SHOULD log the incident as a security event. An example of such an event would be the attempt to access a data object for which the user does not have permission. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of detection mechanisms can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_02.GW	**Requirement**

	The Dualmode-Gateway SHALL support mechanisms to prevent and detect unauthorized access.
	Recommendation and Implementation Guidance
	1. The Dualmode-Gateway SHOULD implement mechanisms to detect unauthorized access attempts. Where possible, the Dualmode-Gateway SHOULD log the incident as a security event. An example of such an event would be the attempt to access a data object for which the user does not have permission. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of detection mechanisms can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_02.CS	**Requirement**
	The Central System SHALL support mechanisms to prevent and detect unauthorized access.
	Recommendation and Implementation Guidance
	1. The Central System SHOULD implement mechanisms to detect unauthorized access attempts. Where possible, the Central System SHOULD log the incident as a security event. An example of such an event would be the attempt to access a data object for which the user does not have permission. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity

	1. The implementation of detection mechanisms can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_03.M	Requirement
	The Meter SHALL log successful logins as well as failed authentication attempts in the security log.
	Recommendation and Implementation Guidance
	1. The implementation of the security log SHOULD ensure that the entries do not overwrite other security-relevant entries. 2. The Meter SHOULD notify the Central System after a configurable number of failed login attempts. 3. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of correct event logging can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_03.GW	**Requirement**
	The Dualmode-Gateway SHALL log successful logins as well as failed authentication attempts in the security log.
	Recommendation and Implementation Guidance
	1. The implementation of the security log SHOULD ensure that the entries do not overwrite other security-relevant entries. 2. The Dualmode-Gateway SHOULD notify the Central System after a configurable number of failed login attempts.

	3. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of correct event logging can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SAR_03.CS	**Requirement**
	The Central System SHALL log successful logins as well as failed authentication attempts in the security log.
	Recommendation and Implementation Guidance
	1. The implementation of the security log SHOULD ensure that the entries do not overwrite other security-relevant entries. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The implementation of correct event logging can be verified in a functional security test. 2. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.

C.5 Confidentiality

Req._ID	
SCR_01.M	**Requirement**

	The following interfaces of the Meter SHALL support application-layer encryption with an allowed algorithm: • LAN between the electricity meter and the Dualmode-Gateway, • WAN between the electricity meter and Central System, • Multi-Utility Interface between the electricity meter and other utility meters. • Customer Interface.
	Recommendation and Implementation Guidance
	1. Allowed encryption algorithms are defined in SPR_01. 2. Communication SHOULD be encrypted using symmetric algorithms and preferably using an authenticated cipher.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each interface supports the allowed cryptographic algorithms.
SCR_01.GW	**Requirement**
	The WAN-interface and LAN-interface of the Dualmode-Gateway SHALL support application-layer encryption except for messages that are sent directly between the Smart Meter and Central System.
	Recommendation and Implementation Guidance
	1. Allowed encryption algorithms are defined in SPR_01. 2. Communication SHOULD be encrypted using symmetric algorithms and preferably using an authenticated cipher.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should specifically ensure that each interface supports the allowed cryptographic algorithms.

SCR_01.CS	Requirement

	The following interfaces of the Central System SHALL support application-layer encryption with an allowed algorithm (as defined in SPR_01):
	• WAN_M between the electricity meter and Central System
	• WAN_GW:
	  ○ between the electricity meter and the Central System
	  ○ between the Dualmode-Gateway and Central System if the interface is used for maintenance purposes
	• User Interfaces (UI)
	• All internal interfaces of the Central System (zone-to-zone)
	• Web Interface (WWW) of the customer portal
	• Interface to the Back-End System in the MDMS

	Recommendation and Implementation Guidance
	1. Allowed encryption algorithms are defined in SPR_01. 2. Requirement SRR_04.CS provides details on zoning in the Central System. 3. Section B.2 provides details on the interfaces of the Central System.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test. The test should ensure that each interface supports the allowed cryptographic algorithms.

C.6 Audits and Logs

Req._ID	
SLR_01.M	**Requirement**
	The Meter SHALL log at least the security events described in Section B.4.

	The Meter SHALL provide a local audit trail for all security events. In addition to the existing log files, a dedicated security log SHALL exist to store security-relevant events. The security log SHALL be accessible from the Central System. The Meter SHALL be equipped with dedicated registers counting the number of occurrences of security events during a particular interval. This interval SHALL be configurable.
	Recommendation and Implementation Guidance
	1. Each security event SHOULD record, where possible, the user or system identification (ID), the interface, the timestamp, as well as the result of the event. 2. The manufacturer SHOULD provide a list of all supported security events.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test of the security log. 2. Carrying out a penetration test is recommended to provide assurance that this requirement is adequately implemented.
SLR_01.GW	**Requirement**
	The Dualmode-Gateway SHALL provide a local audit trail for all security events. In addition to the existing log files, a dedicated security log SHALL exist to store security-relevant events. The security log SHALL be accessible from the Central System. The Dualmode-Gateway SHALL log at least the security events described in Section B.4.
	Recommendation and Implementation Guidance

	1. Each security event SHOULD record, where possible, the user or system identification (ID), the interface, the timestamp, as well as the result of the event. 2. The manufacturer SHOULD provide a list of all supported security events.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test of the security log. 2. Carrying out a penetration test can provide assurance that this requirement is adequately implemented.
SLR_01.CS	**Requirement**
	The Central System SHALL provide a local audit trail for all security events. In addition to the existing log files, a dedicated security log SHALL exist to store security-relevant events, or it MUST be possible to filter a log file for all security events
	Recommendation and Implementation Guidance
	1. Each security event SHOULD record, where possible, the user or system identification (ID), the interface, the timestamp, as well as the result of the event. 2. The manufacturer SHOULD provide a list of all supported security events. 3. The Central System SHOULD forward the security events to a log monitoring or SIEM system to allow monitoring and analysis by a security operations centre.
	Recommended Assurance Activity
	1. This requirement is verified in a functional security test of the security log. 2. Carrying out a penetration test is recommended to provide assurance that this requirement is adequately implemented.

SLR_02	**Requirement**
	Entries of all log files SHALL be protected from changes, only addition of new entries shall be possible.
	Recommendation and Implementation Guidance
	1. Role-Based Access Controls SHOULD protect the security log.
	Recommended Assurance Activity
	1. Carrying out a penetration test is recommended to provide further assurance that this specification is adequately implemented.
SLR_03.M	**Requirement**
	The Meter SHALL provide enough memory for the security log to store at least the last 100 security events. The security log file SHALL be set up as a rolling log file.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The requirement is verified by a functional test to ensure that the security log has sufficient capacity.
SLR_03.GW	**Requirement**
	The Dualmode-Gateway SHALL provide enough memory for the security log to store at least the last 1000 security events.

	The security log file SHALL be set up as a rolling log file.
	Recommendation and Implementation Guidance
	1. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The requirement is verified by a functional test to ensure that the security log has sufficient capacity.
SLR_03.CS	**Requirement**
	The components of the Central System SHALL support a connection to a logging server. It MUST be possible to operate the log server on a dedicated system (i.e., not on the HES, MDMS, or KMS).
	Recommendation and Implementation Guidance
	1. The Central System SHOULD support a dedicated logging server (e.g., a syslog server). This log server SHOULD log all security events of all components of the Central System. 2. The manufacturer SHOULD provide design evidence ensuring that this requirement is addressed. Design evidence SHOULD be at a level of detail that enables easy verification.
	Recommended Assurance Activity
	1. The requirement is verified by a functional test to ensure that log server manages the security events correctly.

C.7 Product Lifecycle and Governance

Req._ID	
SDR_01	**Requirement**
	The manufacturer MUST be able to present an ISO/IEC 27001 certification for all development processes, manufacturing processes, and provisioning processes for devices and products deployed in the Smart Metering system (Meters, Gateways and Central System applications). Proof of certification MUST be provided upon delivery at the latest.
	Recommendation and Implementation Guidance
	1. The requirement applies to all security-relevant development processes, manufacturing processes, and provisioning processes for the Meter and Dualmode-Gateway. 2. Moreover, this requirement applies to the development processes and provisioning processes for the Central Systems. 3. If security-related components are purchased from third-party suppliers, then the related areas and hand-over processes SHOULD be ISO/IEC 27001 certified. 4. Moreover, the ISO/IEC 27001 norm SHOULD be applied to any security-related tools and devices used in the Smart Metering architecture, e.g., the handheld terminal or maintenance software. 5. The manufacturer SHOULD share the corporate security policies.
SDR_02	**Requirement**
	The manufacturer SHALL use a secure configuration management system for managing products. All changes of deposited information SHALL be appropriate, comprehensible, tested and documented. 1. The manufacturer SHALL implement adequate measures to guarantee IT security and physical security of the configuration management system. 2. The manufacturer SHALL provide an audit mechanism identifying the user of each change made. 3. Third party suppliers of security-relevant functions and products SHALL implement comparable processes for configuration management.

	Recommendation and Implementation Guidance
	1. The requirement applies to the development processes, manufacturing processes, and provisioning processes for the Meter, the Dualmode-Gateway and the Central System. 2. The following examples of a secured configuration management system SHOULD be considered: • Administration of hardware configurations of devices and their changes. • Administration of source code and firmware and their changes. • Administration of (customer-related) parameters of devices and their changes.
SDR_03	**Requirement**
	Secured versioning process: 1. All released versions (hardware and firmware) of a device or product MUST be uniquely identifiable. 2. Each version SHALL be accompanied by a release note, available to all relevant parties, that details the changes made. 3. Firmware SHALL be uniquely identifiable by its hash value. 4. The manufacturer SHALL be able to reproduce released versions for devices within the product lifecycle, with traceability provided by the hash value(s) as identifier(s). 5. Exchangeable hardware modules SHALL be versioned separately. 6. Software and software updates SHALL be uniquely identifiable by their hash value.
	Recommendation and Implementation Guidance
	1. The requirement concerns the versioning processes for developing the firmware of the Meter and the Dualmode-Gateway. 2. Moreover, the requirement concerns the versioning processes for developing software that is used in the Central System. 3. Requirement SPR_01 lists the allowed cryptographic hash algorithms. 4. Appendix A.2 describes an example process for generating digital signatures.
SDR_04	**Requirement**

	The manufacturer SHALL implement a vulnerability remediation and reporting process: 1. The manufacturer SHALL actively monitor for vulnerabilities and actively participate in testing for vulnerabilities. 2. The manufacturer SHALL immediately provide information about vulnerabilities including a description of the vulnerabilities, information allowing users to identify the devices affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping buyers to remediate the vulnerabilities. 3. The manufacturer SHALL without delay provide updates fixing vulnerabilities reflecting all technical possibilities. 4. The manufacturer SHALL implement a process for externally reported vulnerabilities, including providing a contact address for reporting vulnerabilities. 5. The manufacturer SHALL draw up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products and make it available to the buyer.
	Recommendation and Implementation Guidance
	1. The requirement concerns the vulnerability remediation and reporting processes for the development and manufacturing of the Meter, the Dualmode-Gateway and the Central System. 2. The following cases of a vulnerability remediation and reporting process SHOULD be considered: • Identification and addressing of security vulnerabilities found by the manufacturer. • Identification and addressing of security vulnerabilities found by the grid operator. • Identification and addressing of security vulnerabilities found by external parties, e.g., security vulnerabilities published by researchers. 3. A service level agreement (SLA) SHOULD be agreed between the manufacturer and operator on reporting and mitigating vulnerabilities. Timelines SHOULD be defined to fix vulnerabilities based on their severity, for instance defined through their CVSS score.
SDR_05	**Requirement**

	The manufacturer SHALL carry out extensive testing of products. These tests MUST include security tests, including tests of the cryptographic measures. 1. All equipment MUST comply with the specifications of the documentation supplied by the manufacturer. 2. Using non-trivial test cases, the manufacturer SHALL be able to demonstrate evidence of correct behaviour under security and functional testing. 3. The tests MUST cover the entire scope of functions of the product and specifically include tests of the entire communication chain. 4. The tests SHALL cover adequate testing of both regularly used as well as rarely used functions, such as software updates. 5. The manufacturer SHALL provide the results of the conducted security tests at the time of release to the grid operator. 6. The manufacturer SHALL perform testing of new functions after major changes and SHALL perform tests covering the full scope of functions at least every three years. 7. The manufacturer SHALL provide support testing by an independent third party on request of the operator by providing the required documentation, access and technical support. The manufacturer SHALL allow an independent third party to perform source code reviews.
	Recommendation and Implementation Guidance
	1. The requirement concerns security testing of the Meter, the Dualmode-Gateway and the Central System. 2. The following examples of security tests SHOULD be considered: • Fuzzing tests • Robustness tests • Penetration tests Appendix B lists details for the above-mentioned test types. 3. Source code reviews may be performed on-site at the manufacturer to protect the source code.
SDR_06	**Requirement**
	The manufacturer SHALL have a high ICT security awareness and provide training on ICT security for the staff. The manufacturer SHALL demonstrate

	possession of the necessary knowledge to develop and produce secure products. The manufacturer SHALL designate a technical contact for security-related matters.
	Recommendation and Implementation Guidance
	1. Example: • Documented professional experience in IT security or a security certification, such as CISSP or CISM.
SDR_07	**Requirement**
	Security-enhancing features of the underlying platform, implementation language and tool chain SHALL be deployed. The manufacturer SHALL provide evidence if this is not necessary or possible.
	Recommendation and Implementation Guidance
	1. Examples of security-enhancing features are: • Secure boot process where the boot loader verifies the authenticity of the firmware. • Deactivation of hardware debug interfaces, such as JTAG interfaces. • Activation of microcontroller functions that enable read-out protection.
SDR_08	**Requirement**
	The manufacturer SHALL ensure secure provisioning of cryptographic keys during the manufacturing process. It MUST be possible to individually provision any cryptographic key material to the devices within the manufacturing process. The manufacturer SHALL ensure a secure hand-over process to the grid operator.

	Recommendation and Implementation Guidance
	1. Examples: • The manufacturer SHOULD provide a secured production area to ensure the secure initial provisioning of cryptographic keys. • A secure hand-over process of the provisioned information to the Central System SHOULD be established. • Appendix A.1 describes an example process for secured provisioning.
SDR_09	**Requirement**
	The manufacturer SHALL present a security concept and detailed documentation of the components of the Central System that provide a remote maintenance function to a third party.
	Recommendation and Implementation Guidance
	1. Remote maintenance functions SHOULD be avoided where possible. 2. An example for securing the remote maintenance function would be a terminal server.
SDR_10	**Requirement**
	The Central System SHALL support a process to securely dispose of Meters and Dualmode-Gateways by disabling them in the system and retiring the cryptographic keys.
	Recommendation and Implementation Guidance
	1. See Appendix A.5 for recommendations on the disposal process.
SDR_11	**Requirement**
	The manufacturer SHALL implement a secure product development lifecycle following IEC 62443-4-1. The manufacturer SHALL implement all requirements in that document for all development processes related to the delivered products.

	The manufacturer SHALL be able to present upon delivery an IECEE certificate for this implementation demonstrating they achieve at least maturity level managed.
	Recommendation and Implementation Guidance
	1. The implementation and certification SHOULD cover not only the development processes for the Meter, the Dualmode-Gateway and the Central System, but also of any related tools and devices used in the Smart Metering architecture, such as the handheld terminal or maintenance software.

C.8 Secure element

The following requirements concern the secure element on a Dualmode-Gateway acting in Data Concentrator Mode. *These requirements only apply in case a Dual Mode approach is used* (Option C in Section B.1). They do not apply to Option B and non-Dualmode-Gateway acting in Data Concentrator Modes.

Req._ID	
SER_01.GW	**Requirement**
	If the Dualmode-Gateway supports Data Concentrator Mode, then it SHALL have a secure element to protect any keys it stores. The secure element SHALL meet the following requirements: • The secure element receives keys from the HSM at the central system in such a way that the integrity and confidentiality are protected end-to-end. • Stored keys are protected against advanced physical threats in which attackers have full physical access to the device. • Communication between the main processor and the secure element is cryptographically protected to prevent Man-in-the-Middle attacks. The secure element shall be Common Criteria (CC) Certified against a security target that covers the above requirements and an assurance level of EAL 4 or higher. The vendor shall present all relevant Common Criteria certificates.

	Recommendation and Implementation Guidance
	1. Separate Common Criteria certificates may be presented for the IC, Platform and applet. 2. The secure element protects all keys used by the Dualmode-Gateway acting in Data Concentrator Mode, including those for communication with the Meters, and any private keys used for TLS or SSH. 3. The cryptographic algorithms used in the secure element must comply with the requirements in Section C.1.3.
	Recommended assurance activity
	1. The requirements are verified by reviewing the certificate of the secure element. The security targeted against which the element is certified must have the right assurance level and cover the requirements listed. 2. It is recommended to perform a code review on how the secure element is used correctly by the applications on the data concentrator.
SER_02.GW	**Requirement**
	If the Dualmode-Gateway supports Data Concentrator Mode, then it SHALL have hardware support for secure boot in which the authenticity of all software loaded during the boot sequence is cryptographically verified. The secure boot process: • has a root of trusted that is anchored in immutable hardware (ROM or OTP) • protects the confidentiality and integrity of all parts of the secure boot chain • verifies the authenticity of all data cryptographically before use • copies all data into volatile memory (SRAM/DRAM) before verification and decryption
	Recommendation and Implementation Guidance
	An anti-rollback feature SHOULD be implemented so that an attacker cannot downgrade the firmware to a known vulnerable version. However, this feature can add operational problems if the newly rolled out firmware version has issues. A solution to this is to have the manufacturer also sign the previous

	version of the firmware as if it was the next version. However, such a scheme would also mandate that the firmware should contain the customer ID, so that other customers cannot be attacked using this downgrade.
	Recommended assurance activity
	1. The requirements are verified by asking for a certificate showing that the hardware can support secure boot. 2. It is recommended to do a penetration test to verify that the secure boot is correctly used by the firmware on the gateway.
SER_03.GW	**Requirement**
	If the Dualmode-Gateway supports Data Concentrator Mode, then it SHALL be able to cryptographically protect the integrity and confidentiality of all data that is not stored on the same package as the processor. The keys used are stored in hardware that is resistant against advanced physical attacks. Before each use, the processor verifies that data loaded from storage has not been modified since it was written.
	Recommendation and Implementation Guidance
	-
	Recommended assurance activity
	1. It is recommended to do a penetration test to verify that stored data is protected as required.
SER_04.GW	**Requirement**
	When the Dualmode-Gateway acts in Data Concentrator Mode, it SHALL only have access to the keys for the *FW upload* and *Readout gw* roles as described in Section B.3.1.
	Recommendation and Implementation Guidance

	1. The Dualmode-Gateway acting in Data Concentrator Mode does not have access to the other keys, such as those for the Central System, to prevent it from executing critical commands.
	Recommended assurance activity
	1. It is recommended to do a penetration test to verify that stored data is protected as required.

Appendix A Example Processes

The processes described are examples of how selected requirements can be implemented in the context of end-to-end security. The following sections with example processes are not normative but are meant to be interpreted as an aid for understanding.

Appendix A.1 Process for Provisioning of Cryptographic Key Material

One of the main requirements for the security architecture of the Smart Metering System is the use of cryptographic key material, which must be unique per device and per role configured on the device. The cryptographic key material must be generated cryptographically secure randomly and securely provisioned and stored for the device.

To optimize the installation process while maintaining security, it is suggested to perform the provisioning of key material at the manufacturers as one of the final steps in the manufacturing process. This initial cryptographic key material is used to perform a first, secure connection with the devices, for example, from the central system or handheld terminal. The security of the communication between these devices is therefore based on the established processes at the manufacturer for provisioning the cryptographic key material.

This results in the following main points which should be considered:

- Requirements for the trustworthiness of the process environment
- Process requirements for generating and provisioning the cryptographic key material
- Requirements for the transfer processes of the provisioned cryptographic key material

The areas in scope at the manufacturer must be ISO/IEC27001 certified according to requirement SDR_01.

Appendix A.1.1 Requirements for the Process Environment

The process environment itself must meet several requirements to establish trustworthiness of the provisioned cryptographic key material.

First, the trustworthiness of the hardware to be provisioned with cryptographic key material must be guaranteed by the manufacturer. The manufacturer shall demonstrate that no manipulation of the hardware has occurred.

Furthermore, the trustworthiness of the firmware on the device must be ensured. The manufacturer must be able to prove the authenticity of the firmware of the device to be provisioned.

As a third point, the security of the provisioning area itself must be ensured. This includes the security of the IT components being used and the physical access controls of the provisioning area.

Appendix A.1.2 Requirements for Generation and Provisioning

Generating, provisioning, and storing cryptographic key material shall occur in a secure process environment.

To generate the cryptographic key material an approved random number generator shall be used as described in requirement SPR_02.

A distinction must be made whether a symmetric key or public/private key pair will be used:

- Initial symmetric keys should be generated outside of the device, within the secure process environment using an external random number generator. The key generated in this way is then provisioned to the device.
- A public/private key pair shall be generated within the device and within the secure process environment. Parts of entropy for the generation of the private key should be generated by an external random number generator. Corresponding random seed should be provisioned for the device. After generating the key pair, it shall only be possible to obtain the public key in the form of a Certificate Signing Requests (CSRs) from the device. After processing the CSRs into a valid device certificate, it must be securely imported into the device together with other information (such as root certificates).
- Any key material used by the devices should be initialized individually as part of the provisioning process at the manufacturer.

Appendix A.1.3 Requirements for the Transfer Process

The manufacturer and the operator of the Central System must share secure procedures for the exchange of provisioned cryptographic key material. The confidentiality and authenticity of provisioned cryptographic key material must be guaranteed at the transfer.

Such a transfer process can be modelled with the use of encryption mechanisms and digital signatures, for example:

> Manufacturers and operators of the Central System each may generate a public/private key pair and exchange their public keys in a secure fashion, i.e., using a public key infrastructure (PKI).
>
> The authenticity of the exchanged public keys must be strictly verified and documented.
>
> The manufacturer now uses the received public key to encrypt of all the devices' provisioned sensitive data (e.g., all keys individually generated per role on a device).

This encrypted data is inserted by the manufacturer into an electronic shipment file or an equivalent document that can be processed by the operator of the Central System. The VDE Elektronischer Lieferschein[4] provides a standard format for a shipment file that may be useful.

The serial number (or other unique device identifier) of a device is assigned to the encrypted information. Before this electronic shipment file is provided to the operator of the Central System, the manufacturer signs the file using their own private key.

Upon receipt, the operator of the Central System checks the manufacturer's digital signature of the electronic shipment file by using the manufacturer's public key and thus verifies the authenticity of the received document.

As a second step, the operator of the Central System can decrypt the information encrypted by the manufacturer and import the data into the Central System. Unencrypted data should not be stored and MUST be securely removed afterwards.

Similar requirements apply as described in "Firmware Update Process" regarding securing access to the respective private key.

Appendix A.2 Firmware Update Process

The integrity of firmware is ensured by attaching a digital signature. The device can verify that the firmware originates from the manufacturer based on the digital signature. The device may only accept the firmware if it can clearly verify the manufacturer's authorship based on the digital signature.

To ensure the trustworthiness of a digital signature, the manufacturer shall establish a process for securely generating digital signatures.

Appendix A.2.1 Background Digital Signatures

When creating a digital signature first a hash value of the firmware is calculated. The digital signature is the result of the encryption of the hash value using the private key of the manufacturer. Upon receipt of the firmware, the device verifies the digital signature using the public key and then compares the hash value of the received file.

This results in the following main points that should be considered:

- Requirements for the release process for firmware updates.

[4] https://www.vde.com/de/fnn/arbeitsgebiete/digitalisierung-metering/vorbereitungen-rollout/hinweis-e-lieferschein

- Requirements for the access procedures and the security of the secret cryptographic key material, with which the digital signature of the firmware file is created (see requirements for key management).
- Requirements for the process of securely provisioning public cryptographic key material on the device (see requirement SDR_07).
- Requirements for the update process of the device itself (see requirements SIR_03. *).

It is strongly recommended that the areas described are certified according to ISO27001 (see requirement SDR_01).

This section describes suitable sample processes and relevant requirements in terms of ICT security.

Appendix A.2.2 Firmware Release Process

The manufacturer should establish a release process for new firmware versions. The manufacturer should appoint a person responsible for the approval process.

The release process should be documented by the manufacturer. The process must generate relevant evidence of the release process of firmware versions. It is important to note which person at which time authorized the release of firmware updates.

The version of the firmware updates must be documented based on its hash value. If a firmware update is comprised of several components (i.e., different files), they must be individually named and documented based on their hash value. By authorizing the release of a firmware update, the manufacturer documents that the firmware file can be uniquely identified with its hash value.

Appendix A.2.3 Managing and Securing Secret Key Material

After a firmware release, a digital signature must be created. If a firmware update consists of several components (i.e., different files), they must be individually signed.

The manufacturer must operate a system that controls access to the secret key material that is used for signature generation of firmware updates.

This system shall be operated in a secure IT environment.

The manufacturer should designate a person who is responsible for the generation of digital signatures. This person must then use the system to create a digital signature for the firmware. It can be useful to apply the four-eyes principle to firmware signing.

It must not be possible for the responsible person to have direct access to the signing keys. The system shall only provide functions that digitally sign the firmware. Furthermore, the system must provide an audit mechanism that provides proof of time, responsible person, firmware version, and hash of the firmware when generating a signature.

In addition, the system shall protect the secret key material sufficiently with respect to physical access, for example, by storing the key on a hardware security module.

After successfully creating the signature, the released firmware version can be combined along with the signature to form the final firmware update. This firmware update will be made available to the operator of the Central System.

Appendix A.2.4 Provisioning Process

To enable the automated verification of the digital signature of a firmware update, the corresponding public key material must be provisioned on the device.

This provisioning process of the public key material must be initially performed at the manufacturer in a secure environment. This process ensures the authenticity of the public key material that is provisioned on the device.

The public key material may be changeable afterwards by an authorized (digitally signed) firmware update.

Ideally, this provisioning process is performed together with the provisioning of all required cryptographic keys.

Appendix A.2.5 Update Process of the Device

Before a device is allowed to accept a firmware file to update from, it must verify the file's digital signature. Should the verification fail or if a digital signature is missing entirely, the device shall not accept the firmware. The device can thus ensure that the received firmware update is authentic, meaning it is supplied by the vendor.

Appendix A.3 Firmware Update Process

Multicast is a useful method to send firmware updates, which require significant bandwidth, to multiple devices at the same time. According to the IMA-VO the relevant data must be encrypted and authenticated when using multicast. Therefore, the multicast process is initiated by individual unicasts.

This results in the following example process:

1. The Central System creates a temporary multicast key. This multicast key will be the same for all devices but must be encrypted with the individual key of the device, authenticated, and then can be sent to the appropriate device via unicast.
2. The Central System sends the firmware update via multicast to all initialized devices. The firmware update is encrypted and authenticated with the multicast key previously generated. Then the Central System discards the multicast key.
3. The Central System sends an activation message via unicast to all initialized devices. Each activation message is encrypted and authenticated with the individual key of the device.
4. The device decrypts and verifies the integrity of the message that contains the firmware update. Then, the device discards the multicast key.

5. Next, the device checks the integrity of the firmware file based on the digital signature and the validity of the version number (see also Appendix A.2).
6. The device activates the firmware after it receives the activation message, decrypts it, and verifies the integrity.

Appendix A.4 Secured Calibration or Verification Process

The following process description is an example for ensuring the security of the Meter when it is passing through a calibration or test process. This example process can be used both for the company's internal calibration or testing procedures as well as for the calibration or testing procedures of a third party.

Appendix A.4.1 Transfer to Calibration or Testing Organization and Transfer of Key Material

The Meter and the associated key material of the "Calibration and Testing" role are made available for the calibration or testing organization.

In the Key Management System, the key material for the "Calibration and Testing" role is marked as *active*. *Active* means that the key material was issued for this role and that an update of this issued key material must be carried out as soon as this meter is put back into operation mode.

The transfer of the key material to a calibration or testing organization can be realized via a direct connection to the Key Management System, for example. Alternatively, the provisioned key material of the meter can be exported and passed through a secure "offline process". For example, this can be similar to the described transfer process in "Process for provisioning of cryptographic key material (at the manufacturer)."

Appendix A.4.2 Providing a Secure Calibration and Test Mode

Authentication between the calibration or testing organization and the Meter must be performed. For this, the provided key material is used. After successful authentication, the calibration or testing organization may put the Meter in a calibration mode or a test mode using the corresponding commands. All communication between the Meter and calibration or testing organization should be authenticated. The given key material is used.

In this state, the calibration or testing of the Meter can take place.

After a successful calibration or test, the Meter must be reset into the "*normal operation*" mode with a corresponding command. The calibration or testing organization shall perform this last step, as the secured calibration mode may not be available outside of the calibration or testing organization.

The Meter should automatically disable the "Calibration and Testing" role when entering normal operation mode.

Appendix A.4.3 Transfer into Operation Mode

The Meter is returned from the calibration or testing organization and can be used normally again. When returning, the key material for the role of "Calibration and Testing" is marked as "*update*" in the Key Management System.

Once the Meter is installed in the field and can be reached by the Central System, the key material for “Calibration and Testing” is updated by the "Central System Read-Write” role. Furthermore, the role of "Calibration and Testing" is activated again by the Central System.

For Meters that do not have an online connection at installation, the role of "Calibration and Testing" can be provisioned with new key material and reactivated using a Handheld Terminal through the "Maintenance" role.

Appendix A.5 Disposal Process

When a Meter or Dualmode-Gateway is being disposed of, the Central System first blocks communication from it. Typical steps are:

- Disabling the device in the MDMS
- Disabling access to the communication networks, e.g., by blocking the SIM
- Retiring keys in the Key Management System
- Removing information in the Central System that is no longer needed

If a Meter will be reused for another customer, the personal data from the previous customer should be removed.

After a Dualmode-Gateway has been removed, it should be physically destroyed in a secure way, so that data stored on it cannot be recovered.

For Meters, the operator should decide based on a risk assessment if they need to be physically destroyed in a secure way. The Meter contains personal data of only one customer. The keys stored on the Meter are usually unique and are disabled in the Central System. Hence, the risks are lower than for a Dualmode-Gateway.

Appendix B Glossary

The glossary is intended to explain special terms and abbreviations in the document. For detailed descriptions of test procedures, background information, or details about cryptographic methods, see the recommended literature.

Application Layer	**OSI**-Layer 5-7.
Authentication	For authentication one distinguishes between **entity authentication** (e.g., a person or a device) and **message authentication**. Authentication is used to verify the **integrity** of the communication partners or to verify **data integrity**.
Authenticity	Truthfulness of origin.
Bidirectional	Functioning in two directions. See also **bidirectional interface**.
Bidirectional interface	The signals can move in both directions during data transmission.
Block cipher	A cryptographic encryption method used to encrypt messages of fixed (block) length.
Broadcast	Data transmission technique in which a message is simultaneously transmitted to all subscribers on the network. Using a **multicast**, the message is sent to a group of selected participants in the network. Using a **unicast**, the message is sent to exactly one network participant.
BSI	The Federal Office for Information Security in Germany (German: Bundesamt für Sicherheit in der Informationstechnik).
Certificate	A digital certificate is a file that allows the verification of the authenticity of a communication participant or a message. See **Public Key Infrastructure**.
Confidentiality	Only selected users are allowed to access confidential messages. This is often done by **encryption** of messages, where only authorized persons get access to the secret **key material**.
Configuration Management System	The Configuration Management System is the system at the manufacturer that manages the lifecycle of the device from its development through manufacturing and procurement. In

	particular, the system includes the management of software and sources of (customer-specific) configurations of a device.
Cryptographic Hash Function	Cryptographic hash functions must behave like one-way functions and be collision resistant and strong collision resistant. Changes in the input message must lead to a significant change in the hash value. Example: SHA-256. See also ECRYPT [13].
Cryptography	ECRYPT's Algorithms, Key Sizes and Parameters Report [13] provides details on the state of the art in cryptography.
Data Integrity	See **integrity** and **message authentication**.
DAVID-VO	Austrian legislation: Datenformat- und VerbrauchsinformationsdarstellungsVO 2012. This catalog refers to the version DAVID-VO 2012 Design.
Device	The term "device" may refer to both the Gateway and the Meter. The Recommendation and Implementation Guidance provides further details.
Digital Signature	To ensure the **integrity** of the source. When generating a digital signature, first a **hash value** of the file is calculated. The sender generates the digital signature by encrypting this hash value using the secret key. The recipient verifies the digital signature using the public key and compares the **hash value** of the received file. In practice, digital signatures are generated using **elliptic curve** (**EC**) based algorithms.
Display	See *Chapter B*.
EC	Elliptic Curve. See also ECRYPT [13].
Encryption	The message is converted using a cryptographic method into a string called a ciphertext that is unreadable for an attacker. Decryption is the transformation of the ciphertext back into the original message text; it is performed with the same key (symmetric cryptography) or using the private key (**public key cryptography**).
Engineering Menu	A functionality of the device that allows a service engineer to change settings and perform information retrieval on the local display using keyboard inputs.

Entity Authentication	Verification of the identity and **integrity** of the communication partners (e.g., users on the Meter). Moreover, verification that the communication partners are still alive throughout a session. See also **password authentication** and **strong authentication**.
EPRI	Electric Power Research Institute.
Fail-Secure	Construction principle in which security-relevant designs can guarantee confidentiality and integrity of the system in case of failures.
Four-Eyes Principle	Double checking. Decisions must be made by more than one person.
Fuzzing Test	A fuzzing test is carried out for quality assurance of software for secure network communications. This is done by generating a large, mostly random data volume, and may also contain erroneous data packets that are introduced in a structured manner in the data traffic. A detailed introduction to fuzzing can be found in [14].
Gateway	See Chapter B.
GPRS	General Packet Radio Service.
HAN	Home Area Network.
Handheld Terminal	A tool used by a service engineer to change settings and send information queries through the Maintenance Interface of a Meter or Gateway.
Hash Function	A function mapping a message to a bit sequence (i.e., **hash value**) of fixed length. See **Cryptographic Hash Function**.
Hash Value	Output of a **(cryptographic) hash function**.
Hybrid Encryption	Since **public-key cryptography** is resource-intensive in terms of key length, computational power, etc., algorithms, such as RSA, are used only in so-called hybrid methods. First a random symmetric session key is generated (for example, a 128-bit AES key). Then the session key is sent encrypted under the public key of the recipient. The actual messages are then encrypted and decrypted using the session key with the corresponding symmetric cipher (e.g., AES).

ICT Security	Information and Communications Technology Security.
IETF	Internet Engineering Task Force.
IMA-VO	Austrian legislation: Intelligente Messgeräte-AnforderungsVO. This catalog refers to the “339. Verordnung ausgegeben am 25. Oktober 2011 Teil II” version.
Integrity	The integrity of a message means protection against tampering. See also **authentication**.
Intrusion Detection System	An intrusion detection system monitors the behaviour of components either on the component itself, or by monitoring the communication. Known attack patterns or anomalies can be detected and reported.
ISO 27001	ISO standard for ICT Security.
Key Material	**Key material** includes all cryptographic keys. Examples are master keys, symmetric keys, **session keys**, private keys and public keys (in **public-key cryptography**).
LAN	Local Area Network.
Log File	Events in the operation of meters are recorded in one or more log files. Another term is log. In a rolling log file, entries can (with appropriate permissions) be overwritten after exhausting the reserved storage space for logs.
MAC	Message Authentication Code. For verification of data integrity. Examples: CMAC, GMAC. See also ENISA [13].
Maintenance Interface	See Chapter B.
Message authentication	The **authenticity** of the message, i.e., that the message is genuine, must be guaranteed. This is done either by appending a message authentication code (e.g., AES-CBC-CMAC) or by using a block cipher in an authenticating mode of operation (e.g., AES-CCM, AES-GCM).
Meter	**Meter** refers primarily to the electricity meter. If necessary, electricity meter and **utility meter** will be explicitly distinguished.
Monitoring System	See **Intrusion Detection System**.

Multicast	Using a **multicast**, the message is sent to a group of selected participants in the network. A **multicast** is a special case of a **broadcast**.
NESCOR	National Electric Sector Cybersecurity Organization Resource. Program by the US organization **EPRI**. See also [15].
NIST	National Institute of Standards and Technology.
Nonce	A nonce is a unique, randomly generated string that must be used exactly once (in medieval English the common term "for the nonce" means "for this one time"). Appended to message to detect or prevent **replay attacks**.
OSI	Open Systems Interconnection. Reference model for network communication.
Password Authentication	The user logs into the device with the username and password or PIN. The device itself does not need to authenticate. This method is particularly vulnerable to stealing passwords using social engineering attacks. For critical areas mutual/strong authentication is recommended.
Penetration Test	The **EPRI** Program **NESCOR** is one of the organizations that provides guidelines on penetration testing with their “AMI Penetration Test Plan”.
Personal data	See Data Protection Regulation. Example: load profile values.
PLC	Power Line Communication.
Product Lifecycle	The product lifecycle includes the stages of design, development, production and procurement, operation and decommissioning of an appliance.
Public Key Infrastructure	System to issue, distribute and verify certificates.
Public-Key Cryptography	A cryptographic method in which a public key is provided for **encryption** as well as the verification of **digital signatures**. There exists a corresponding private key for each public key; this private key must not be made public under any circumstances (i.e., the private key needs to be kept secret). The private key is used to decrypt and **digitally sign** messages.

	Public-key cryptography is not used for direct encryption of messages. Rather, using so-called hybrid encryption a symmetric session key is sent encrypted under the public key. The authenticity of a public key is to be ensured with certificates in a **Public Key Infrastructure** (PKI). See also ECRYPT [13]. The best-known method of public-key encryption is RSA. In principle it is possible to digitally sign with RSA; in practice, however, digital signatures are created using elliptic curve (**EC**) based algorithms.
Read-Only	The user may read data. It is not allowed to write new information or to change existing information.
Read-Write	The user has read and write permissions.
Replay Attack	The attacker records the data of a session and uses it later to impersonate a different identity.
RFC	Requests for Comments. Published by the **IETF**.
Robustness Test	A robustness test is carried out for quality assurance of the stability of the system design. In particular, fault tolerance is tested.
Role	See Section B.3.
Session Key	Symmetric key used for encryption of all messages within a limited time frame (session).
Strong Authentication	In strong authentication, both sides need to authenticate themselves and thus prove their identity. Challenge-response protocols are often applied. Other common methods use certificates.
Unicast	Using a **unicast**, the message is sent to exactly one participant in the network. See also **Broadcast**.
Unidirectional	Functioning in only one direction. See also **unidirectional interface**.
Unidirectional Interface	The signals can move in only one direction during data transmission, e.g., from the Meter to the Customer on the Customer Interface.

Utility Meter	For example, meters for gas, water and heat consumption.
Versioning Process	A versioning process is part of **Configuration Management**.
WAN	Wide Area Network.

Appendix C References

[1] E-Control Austria, “Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft,” 2014 February 27. [Online]. Available: https://www.e-control.at/publikationen/publikationen-strom/studien/ikt-risikoanalyse.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), “BSI TR-03109-1. Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Version 1.1,” Bonn, Germany, September 2021.

[3] Internet Engineering Task Force, “RFC 2119: Key words for use in RFCs to Indicate Requirement Levels,” 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2119.txt.

[4] European Cybersecurity Certification Group Sub-group on Cryptography, “Agreed Cryptographic Mechanisms, Version 2.0,” April 2025.

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI), “BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2026-01,” 2026.

[6] National Institute for Sandards and Technology (NIST), “Special Publication 800-57 Part 1 Rev. 5: Recommendation for Key Management,” 2020.

[7] Bundesamt für Sicherheit in der Informationstechnik, “Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0,” Bonn, Germany, 2013.

[8] National Institute of Standards and Technology (NIST), “FIPS PUB 140-3, Security Requirements for Cryptographic Modules,” 2019.

[9] Bundesamt für Sicherheit in der Informationstechnik, “Anwendungshinweise und Interpretationen zum Schema, AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013.,” Bonn, Germany, 2013.

[10] Österreichischen Normungsinstitut, “ÖNORM A-7700 Sicherheitstechnische Anforderungen an Webapplikationen,” 2019. [Online].

[11] Open Web Application Security Project (OWASP), “Input Validation Cheat Sheet,” [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html.

[12] OASIS, “PKCS #11: Cryptographic Token Interface Standard.,” 2015. [Online]. Available: https://www.oasis-open.org/standards.

[13] ECRYPT - CSA, “D5.4 Algorithms, Key Size and Protocols Report,” 2018.

[14] J. D. C. M. Ari Takanen, “Fuzzing for Software Security Testing and Quality Assurance (1 ed.),” Artech House, Inc, Norwood, MA, USA, 2008.

[15] Electric Power Research Institute, “National Electric Sector Cybersecurity Organization Resource,” [Online]. Available: http://smartgrid.epri.com/NESCOR.aspx.

Oesterreichs Energie Companion Standard
Smart Meter 2.0

H.3_OE_CS_Zählerstifte_und_Steckleisten

Version 1.0

31.03.2026

Versionsverlauf

Version	Änderungen	Datum	Autor
1.0	Veröffentlichung Erstversion	31.03.2026	Oesterreichs Energie

Inhalt

A. Zählerstifte und Steckleisten 4

A.1 Zählerstifte 4

A.2 Steckleisten 5

A. Zählerstifte und Steckleisten

Dieses Dokument dient zur Übersicht und ist ein Auszug der aktuell in Österreich eingesetzten Zählerstifte und Steckleisten.

A.1 Zählerstifte

Tabelle 1: Zählerstifte; Hersteller, Typenbezeichnung, Anmerkung-Datenblatt

Hersteller	Typenbezeichnung	Anmerkung
ABN	53078	Siehe Datenblatt ABN_53078
ADOCK (Bruchmann)	1010	Siehe Datenblatt ADOCK_OVE
ADOCK (Bruchmann)	1011	Siehe Datenblatt ADOCK_OVE
ADOCK (Bruchmann)	1011-44	Siehe Datenblatt ADOCK_OVE
ADOCK (Bruchmann)	1011-50	Siehe Datenblatt ADOCK_OVE
ADOCK (Bruchmann)	1011-S	Siehe Datenblatt ADOCK_OVE
Dietzel	F8040/07	Siehe Datenblatt Dietzel_F8040_07
Seidl	SL-5-5-44-R-Z-Set-7-D	Siehe Datenblatt SL-5-5-44-R-Z-Set-7-D
Seidl	SL-6-6-45-RV-Z	Siehe Datenblatt SL-6-6-45-RV-Z

A.2 Steckleisten

Tabelle 2: Steckleisten; Hersteller, Typenbezeichnung, Anmerkung-Datenblatt

Hersteller	1/3ph	Typenbezeichnung	Anmerkung
ADOCK (Bruchmann)	1ph	1002	Siehe Datenblatt ADOCK_1002_1005_1007
ADOCK (Bruchmann)	1ph	1002-T	Siehe Datenblatt ADOCK_1002_1007-T
ADOCK (Bruchmann)	3ph	1005	Siehe Datenblatt ADOCK_1002_1005_1007
ADOCK (Bruchmann)	3ph	1007	Siehe Datenblatt ADOCK_1002_1005_1007
ADOCK (Bruchmann)	3ph	1007-T	Siehe Datenblatt ADOCK_1002_1007-T
derLESO	3ph	ZSL63/W	Siehe Datenblatt derLESO_ZSL63_W
Elsta Moosdorfer	3ph	ZAK50	Siehe Datenblatt Elsta_ZAK50
Geiger	1ph	ZAK40D-4pol.	Kein Datenblatt verfügbar
Geiger	1ph	ZST-S/2	Kein Datenblatt verfügbar
Geiger	3ph	ZSK-GS80	Kein Datenblatt verfügbar
Geiger	3ph	ZST-S	Kein Datenblatt verfügbar
Geiger	3ph	ZST-SW	Kein Datenblatt verfügbar
Hager	1ph	KJ10AT	Siehe Datenblatt Hager_KJ10AT
Hager	3ph	KJ30ATT	Siehe Datenblatt Hager_KJ30ATT
Hager	3ph	KJ30S	Siehe Datenblatt Hager_KJ30S

Seidl	1ph	SL-ZAKW 63(100)A-2N o.TRE	Siehe Datenblatt SL-ZAKW 63(100)A-2N o.TRE
Seidl	3ph	SL-AKS/Z 63(100)A-1N EVN o.TRE	Siehe Datenblatt SL-AKS_Z 63(100)A-1N-EVN
Seidl	3ph	SL-AKS/Z 63(100)A-2N EVN o.TRE	Siehe Datenblatt SL-AKS_Z 63(100)A-2N-EVN
Seidl	3ph	SL-ZAKD 80(128)A-1N o.TRE	Siehe Datenblatt SL-ZAKD 80(128)A-1N o.TRE
Seidl	3ph	SL-ZAKD 80(128)A-2N m.TRE	Siehe Datenblatt SL-ZAKD 80(128)A-2N m.TRE
Seidl	3ph	SL-ZSK 50(80)A-2N m.TRE	Siehe Datenblatt SL-ZSK 50(80)A-2N m.TRE
Seidl	3ph	SL-ZSK 63A-2N m.TRE	Siehe Datenblatt SL-ZSK 63A-2N m.TRE
Wagner	3ph	ZKL-D	Kein Datenblatt verfügbar

Produktdatenblatt

Technische Daten

53078

Kontakt-Stift 45mm mit 1 Einstich 5 µm Silberbeschichtet, mit Anlaufschutz

Verfügbarkeit lieferbar

Steckstifte für Zählersteckklemme AT425A

Hauptmerkmale

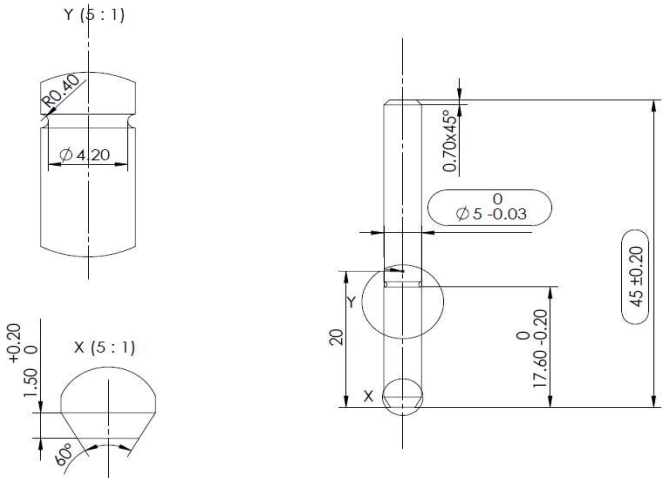
Baureihe	Zubehör Zählerschrank
Produktname	---
Produkt oder Komponententyp	Steckerstift
EAN Code	4015153801080
Verpackungseinheit	1 Stk.
Zolltarif Nr.	74152900

Technische Daten

Nennspannung U_N AC	230 V
Maximaler Bemessungsstrom I_{NA}	63 A
Bemessungsfrequenz $_{fn}$	50/60 Hz
Steckerstift Länge	45 mm
Steckerstift Höhe	5 mm
Steckerstift Breite	5 mm
Oberflächenbehandlung	5 µm Silver Beschichtug mit Anlaufschutz

Verpackungsinformationen

Breite	50 mm
Höhe	100 mm
Tiefe	5 mm
Gewicht	0,008 g



ABN GmbH, Daimlerstraße 10-12
74196 Neuenstadt
Tel. 07139/94-0, Fax 07139/94 49
E-Mail: abn@abn-elektro.de, www.abn-elektro.de

Technische Änderungen vorbehalten
Abbildungen dienen nur zur Veranschaulichung
© ABN GmbH by Schneider Electric

ADOCK®

der Energiesparer

Austria Docktechnologie für Smart Meter

sichert die Zukunft, erfüllt **ÖVE R21**

A-DOCK® der Energiesparer

Technische Daten

A-DOCK® Steckleiste

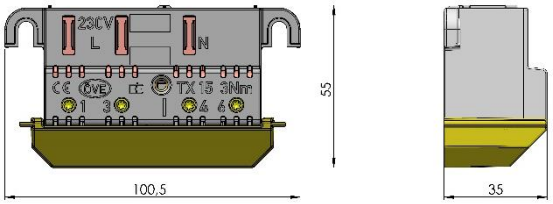
Klassifizierung	Zähleranschlussklemme nach ÖVE R21:2015	
Geeignet für Elektrizitätszähler mit Abmessungen nach	DIN 43857	
Bemessungsstromstärke nach VDE 0603 Teil 3	63A	
Max. zulässige Vorsicherung gegen Kurzschluss	100A gG (gL)	
Max. Nennstrom der Überlastschutzeinrichtung		
gemäß ÖVE R21:2015	3-polig+N	1-polig+N
mit **A-DOCK Systemstift**	**50 A gG (gL)**	**63 A gG (gL)**
mit Standard-Zählerstift (CuZn39Pb3)	40 A gG (gL)	40 A gG (gL)
Polzahlen	3-polig+(2)N, 1-polig+2N	
Isolierteile Kunststoff:	halogen-, phosphor-, und silikonfrei	
Brandklasse / Kriechstromfestigkeit	UL94/V0, Glühdrahtprüfung 960°C	
Temperaturbeständigkeit	150° C	
Kriechstromfestigkeit	CTI600	
Schutzart	IP2XC (mit Zählerklemmenabdeckung)	
Bemessungsspannung	400V~ (3P+N); 230V~ (1P+N)	
Bedingter Bemessungskurzschlussstrom I_{cc}	10kA$_{eff}$	
Überspannungskategorie	IV	
Verschmutzungsgrad	3	
Bemessungsstoßspannungsfestigkeit U_{imp}	6000V	
Anschlusstechnik – Edelstahlklemmen	6...25mm²	
Schraube / Anzugsdrehmoment	TX15 / 3Nm	

A-DOCK® Bügel

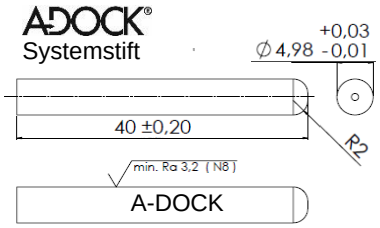
Klassifizierung	Überbrückungsvorrichtung
Max. Nennstrom der Überlastschutzeinrichtung	63 A gG (gL)
Max. Einsatzdauer	30min
Bemessungsspannung	400V~ 3-polig; 230V~ 1-polig

Abmessungen [mm]

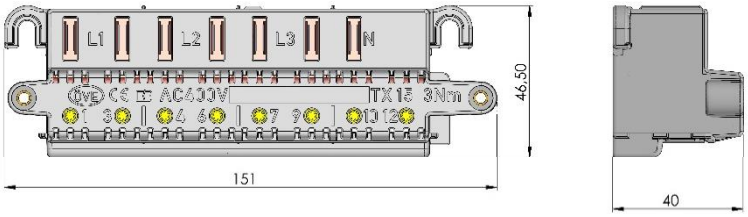
1002



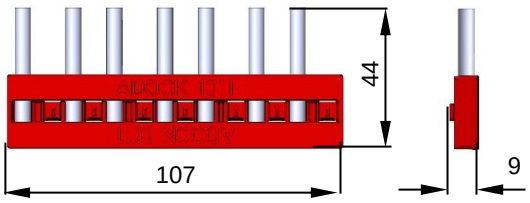
A-DOCK® Systemstift



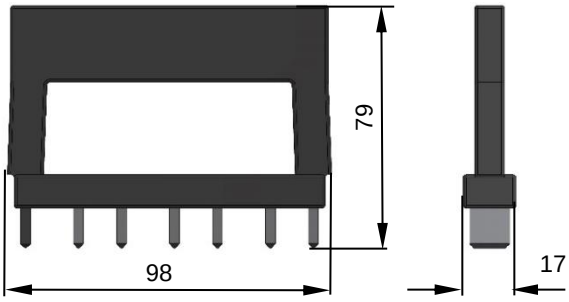
1018, 1019



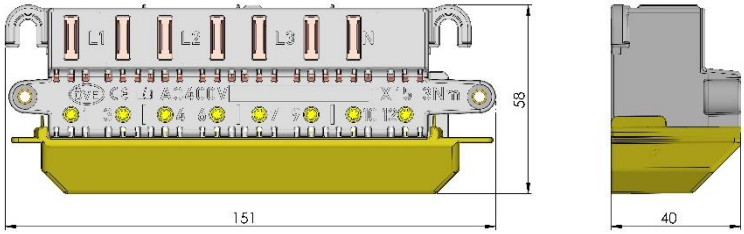
1011



1004, 1008



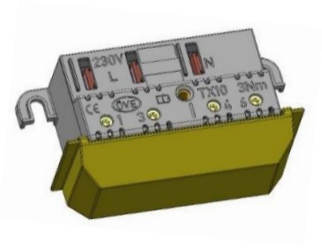
1005, 1006, 1007, 1015, 1016



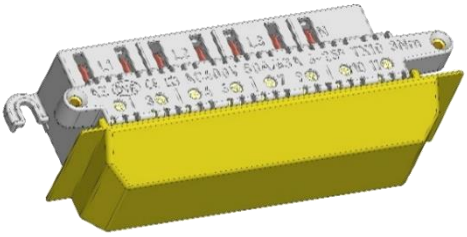
ADOCK® der Energiesparer

ADOCK® Steckleiste

mit Anschlussraum-Abdeckung für Elektrizitätszähler nach DIN 43857
Bemessungsspannung 2-polig 230V AC oder 4-polig 400V AC
Bemessungsstromstärke 63A* nach VDE 0603 Teil 3 mit **ADOCK® Systemstift**
mit zweiter N-Klemme für Weiterverdrahtung.



2-polig (1P+N); Wechselstrom	Art.-Nr.	VE	g/Stk.
- 63A gG, Anschluss unten	1002	1	123



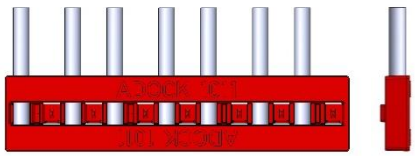
4-polig (3P+N); Drehstrom	Art.-Nr.	VE	g/Stk.
- 50A gG, DUO-Anschluss (Bild 1 u. 2)	1005	1	326
- 50A gG, Anschluss unten (Bild 1, 3)	1007	1	248
- 50A gG, Anschluss hinten (Bild 2)	1006	1	252

*Nach einer Sonderprüfung mit den verwendeten Zählern und Vereinbarung mit dem jeweiligen Verteilnetzbetreiber bis 63A einsetzbar.

Exklusiv für die Verteilnetzbetreiber

ADOCK® Systemstift

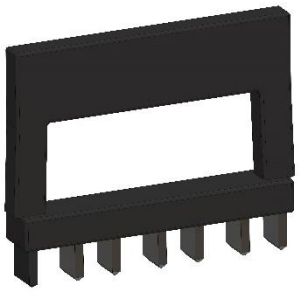
Hochleitende E-Legierung, versilbert im Magazin.
Für Zähler bis 60A oder 100A Grenzstrom einsetzbar - max. Nennstrom der Überlastschutzeinrichtung 63A gG (gL)
Das Magazin ist Montagehilfe und Schutz:
Es bildet den Abstandhalter für die Einschraubtiefe im Zähler und fixiert die Parallelität der Stifte passend für die Schraubklemmen des Zählers.
Gleichzeitig schützt es die versilberten Kontakte steckseitig vor Fingerabdrücken und Verschmutzung.



		Art.-Nr.	VE	g/Stk.
2-polig	3 Stifte	1010	10	25
4-polig	Magazin mit 7 Stiften	1011	10	55

ADOCK® Bügel

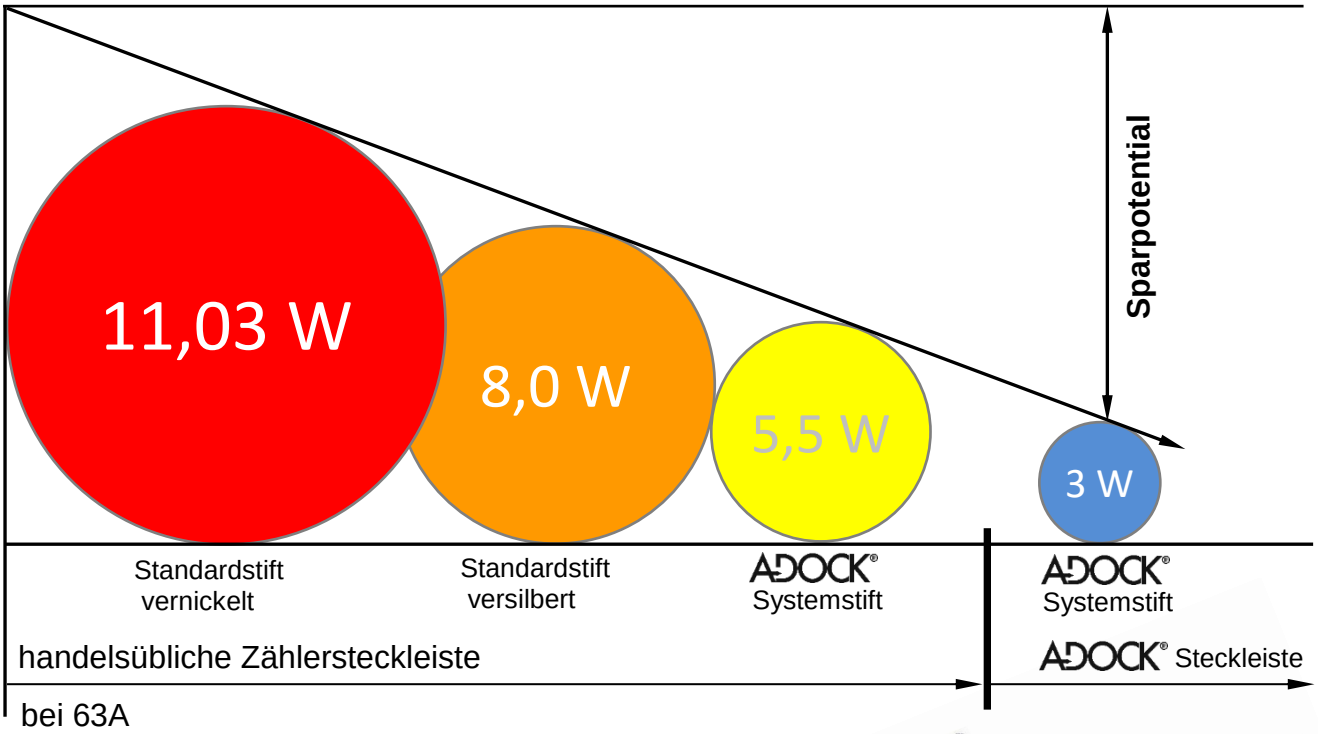
Max. Nennstrom der Überlastschutzeinrichtung 63A gG, zum kraftlosen, unterbrechungsfreien Zählertausch. Entlastet die Steckleisten-Kontakte beim Steckvorgang.



	Art.-Nr.	VE	g/Stk.
2-polig (1P+N)	1004	1	44
4-polig (3P+N)	1008	1	76

ADOCK® der Energiesparer

Energie-Spardiagramm



ADOCK® Steckleiste
2-polig und 4-polig mit Anschlussraum-Abdeckung
für Elektrizitätszähler nach DIN 43857

Kompakte Bauform
Die ADOCK® Steckleiste kann in der Regel mit dem **Standard-Zähler-Klemmendeckel** abgedeckt werden.

DUO-Anschluss
Zählerschleifen bis 25mm² Querschnitt können auch nach hinten (Bild 2) angeschlossen werden.
Dies erleichtert die Montage und reduziert die mechanischen Kräfte. Weniger Lagerkosten, eine Steckleiste für alle Anwendungen.

Antimagnetische Edelstahlklemmen
vermeiden gefahrbringende Überhitzung bei Oberwellen.

50% Zeitersparnis beim Anklemmen der Zählerschleife
Nur 1 Schraube pro Klemmstelle in der ADOCK® Steckleiste.
Kraftsparendes Anschrauben – nur 3Nm Anzugsdrehmoment!
Robuste Schrauben TX15 aus hochfestem Stahl.

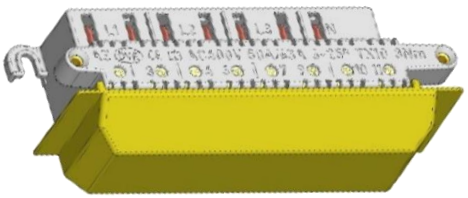


Bild Anschlussraum-Abdeckung

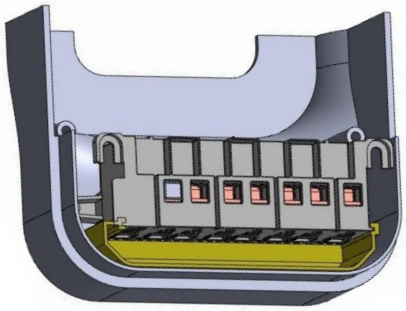


Bild Zähler-Klemmendeckel

Mit Anschlussraumabdeckung

6-10mm²

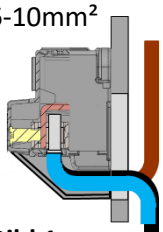


Bild 1
Anschluss unten

6-25mm²

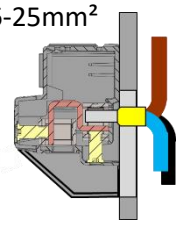


Bild 2
Anschluss hinten

Ohne Anschlussraumabdeckung

6-25mm²

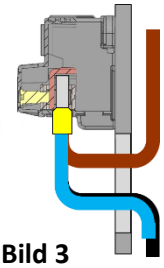


Bild 3
Anschluss unten

ADOCK®

der Energiesparer

Austria Docktechnologie für Smart Meter

sichert die Zukunft, erfüllt **ÖVE R21**

A-DOCK® der Energiesparer

Technische Daten

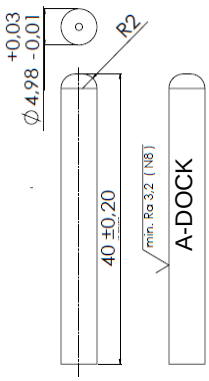
A-DOCK® Steckleiste

Klassifizierung	Zähleranschlussklemme nach ÖVE R21:2015
Geeignet für Elektrizitätszähler mit Abmessungen nach	DIN 43857
Bemessungsstromstärke nach VDE 0603 Teil 3	63A
Max. zulässige Vorsicherung gegen Kurzschluss	100A gG (gL)
Max. Nennstrom der Überlastschutzeinrichtung	
gemäß ÖVE R21:2015	3-polig+N 1-polig+N
mit **A-DOCK Systemstift**	**63 A gG (gL) 63 A gG (gL)**
mit Standard-Zählerstift (CuZn39Pb3)	50 A gG (gL)
Polzahlen	3-polig+(2)N, 1-polig+(2)N
Isolierteile Kunststoff:	halogen-, phosphor-, und silikonfrei
Brandklasse / Kriechstromfestigkeit	UL94/V0, Glühdrahtprüfung 960°C
Temperaturbeständigkeit	150° C
Kriechstromfestigkeit	CTI600
Schutzart	IP2XC (mit Zählerklemmenabdeckung)
Bemessungsspannung	400V~ (3P+N); 230V~ (1P+N)
Bedingter Bemessungskurzschlussstrom I_{cc}	10kA$_{eff}$
Überspannungskategorie	IV
Verschmutzungsgrad	3
Bemessungsstoßspannungsfestigkeit U_{imp}	6000V
Anschlusstechnik – Edelstahlklemmen	6...25mm²
Schraube / Anzugsdrehmoment	TX15 / 3Nm

A-DOCK® Bügel

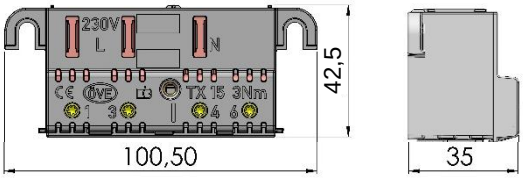
Klassifizierung	Überbrückungsvorrichtung
Max. Nennstrom der Überlastschutzeinrichtung	63 A gG (gL)
Max. Einsatzdauer	30min
Bemessungsspannung	400V~ 3-polig; 230V~ 1-polig

A-DOCK®
Systemstift

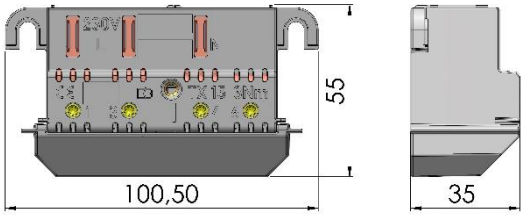


Abmessungen [mm]

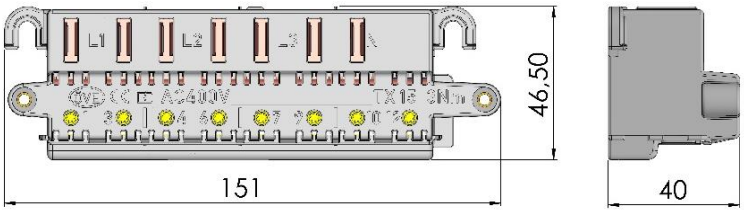
1002-T



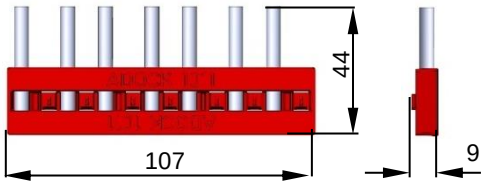
1002



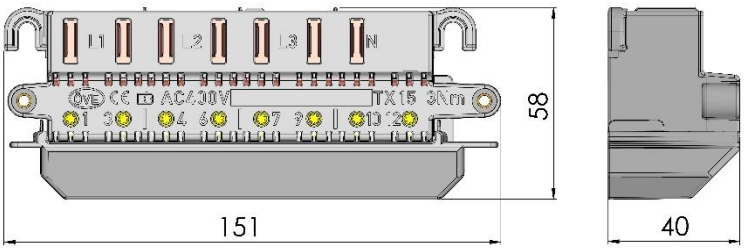
1007-T (Ausführung ohne Anschlussraum-Abdeckung)



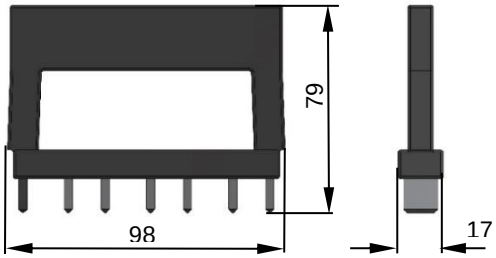
1011



1005 (Ausführung mit Anschlussraumabdeckung)



1004, 1008



Technische Änderungen vorbehalten

ADOCK® der Energiesparer

ADOCK® Steckleiste
für Elektrizitätszähler nach DIN 43857
Bemessungsspannung 2-polig 230V AC oder 4-polig 400V AC
Bemessungsstromstärke 63A nach VDE 0603 Teil 3 mit **ADOCK® Systemstift**
mit zweiter N-Klemme für Weiterverdrahtung.

Versorgungsgebiet der Elektrizitätsunternehmen OBERÖSTERREICH

mit Anschlussraum-Abdeckung

2-polig (1P+N); Wechselstrom	Art.-Nr.	VE	g/Stk.
- 63A gG, Anschluss unten	1002	1	123

4-polig (3P+N); Drehstrom	Art.-Nr.	VE	g/Stk.
- 63A gG, DUO-Anschluss (Bild 1 u. 2)	1005	1	372

SET: DUO-Anschluss Steckleiste mit Zählerschleife
4-polig (3P+N); Drehstrom

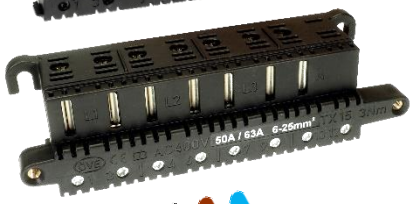
		N	ZU	AB	Art.-Nr.	VE	g/Stk
- 40A	10mm²	1x	1,0m	1,0m	1005-10-1N-1010	1	1112
- 40A	10mm²	1x	1,5m	1,5m	1005-10-1N-1515	1	1482
- 40A	10mm²	1x	2,0m	2,0m	1005-10-1N-2020	1	1852
- 63A	25mm²	1x	1,0m	1,0m	1005-25-1N-1010	1	2122
- 63A	25mm²	1x	1,5m	1,5m	1005-25-1N-1515	1	2992
- 63A	25mm²	1x	2,0m	2,0m	1005-25-1N-2020	1	3922

ZU… Aderleiter schwarz, blau
AB… Aderleiter braun

Versorgungsgebiet der Elektrizitätsunternehmen TIROL

ohne Anschlussraum-Abdeckung

2-polig (1P+N); Wechselstrom	Art.-Nr.	VE	g/Stk.
- 63A gG, Anschluss unten	1002-T	1	115



4-polig (3P+N); Drehstrom	Art.-Nr.	VE	g/Stk.
- 63A gG Anschluss unten (Bild 3)	1007-T	1	273

SET: ADOCK Steckleiste 1007-T mit Zählerschleife
4-polig (3P+N); Drehstrom

		N	ZU	AB	Art.-Nr.	VE	g/Stk
- 40A	10mm²	1x	1,0m	1,0m	1007-T-10-1N-1010	1	1013
- 40A	10mm²	1x	1,5m	1,5m	1007-T-10-1N-1515	1	1383
- 40A	10mm²	1x	2,0m	2,0m	1007-T-10-1N-2020	1	1753
- 50A	16mm²	1x	1,0m	1,0m	1007-T-16-1N-1010	1	2023
- 50A	16mm²	1x	1,5m	1,5m	1007-T-16-1N-1515	1	2893
- 50A	16mm²	1x	2,0m	2,0m	1007-T-16-1N-2020	1	3823

ZU… Aderleiter schwarz, blau
AB… Aderleiter braun

DECKEL - Berührungsschutz mit Plombiereinrichtung

2-polig (1P+N); Wechselstrom	Art.-Nr.	VE	g/Stk.
- für ADOCK 1002-T	1013	2	156

4-polig (3P+N); Drehstrom	Art.-Nr.	VE	g/Stk.
- für ADOCK 1007-T	1012	2	138

Technische Änderungen vorbehalten

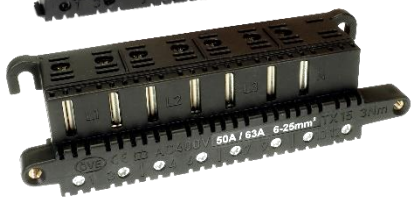
ADOCK® der Energiesparer

ADOCK® Steckleiste

Versorgungsgebiet der Energienetze STEIERMARK

ohne Anschlussraum-Abdeckung

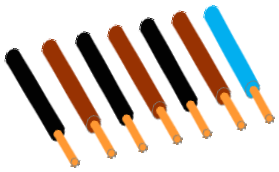
2-polig (1P+N); Wechselstrom	Art.-Nr.	VE	g/Stk.
- 63A gG, Anschluss unten	1002-T	1	115



4-polig (3P+N); Drehstrom	Art.-Nr.	VE	g/Stk.
- 63A gG Anschluss unten (Bild 3)	1007-T	1	273

SET: ADOCK Steckleiste 1007-T mit Zählerschleife
4-polig (3P+N); Drehstrom

		N	ZU	AB	Art.-Nr.	VE	g/Stk
- 32A	10mm²	1x	1,0m	1,0m	1007-T-10-1N-1010	1	1013
- 32A	10mm²	1x	1,5m	1,5m	1007-T-10-1N-1515	1	1383
- 32A	10mm²	1x	2,0m	2,0m	1007-T-10-1N-2020	1	1753
- 50A	16mm²	1x	1,0m	1,0m	1007-T-16-1N-1010	1	2023
- 50A	16mm²	1x	1,5m	1,5m	1007-T-16-1N-1515	1	2893
- 50A	16mm²	1x	2,0m	2,0m	1007-T-16-1N-2020	1	3823



ZU… Aderleiter schwarz, blau
AB… Aderleiter braun

DECKEL - Berührungsschutz mit Plombiereinrichtung

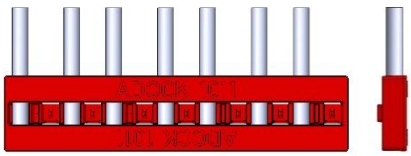
2-polig (1P+N); Wechselstrom	Art.-Nr.	VE	g/Stk.
- für ADOCK 1002-T	1013	2	156

4-polig (3P+N); Drehstrom	Art.-Nr.	VE	g/Stk.
- für ADOCK 1007-T	1012	2	138

Exklusiv für die Verteilnetzbetreiber

ADOCK® Systemstift

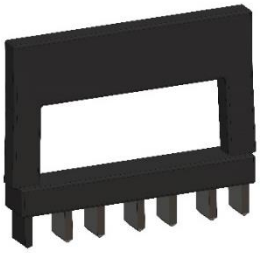
Hochleitende E-Legierung, versilbert im Magazin. Für Zähler bis 60A oder 100A Grenzstrom einsetzbar - max. Nennstrom der Überlastschutzeinrichtung 63A gG (gL)
Das Magazin ist Montagehilfe und Schutz:
Es bildet den Abstandhalter für die Einschraubtiefe im Zähler und fixiert die Parallelität der Stifte passend für die Schraubklemmen des Zählers. Gleichzeitig schützt es die versilberten Kontakte steckseitig vor Fingerabdrücken und Verschmutzung.



		Art.-Nr.	VE	g/Stk.
2-polig	3 Stifte	1010	30	21
4-polig	Magazin mit 7 Stiften 40mm	1011	10	55
4-polig	Magazin mit 7 Stiften 44mm	1011-44	10	60

ADOCK® Bügel

Max. Nennstrom der Überlastschutzeinrichtung 63A gG, zum kraftlosen, unterbrechungsfreien Zählertausch. Entlastet die Steckleisten-Kontakte beim Steckvorgang.



	Art.-Nr.	VE	g/Stk.
2-polig (1P+N)	1004	1	44
4-polig (3P+N)	1008	1	76

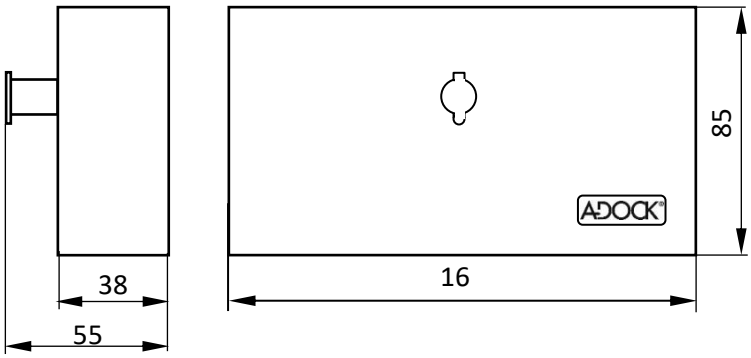
ADOCK® der Energiesparer

ADOCK® Deckel
Berührungsschutz für ADOCK® **Steckleisten** mit Plombiereinrichtung

Abmessungen [mm]

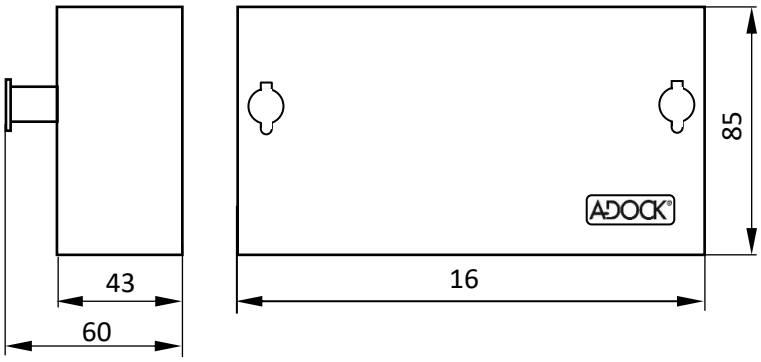
1013

Deckel für
Wechselstromklemme
1002-T



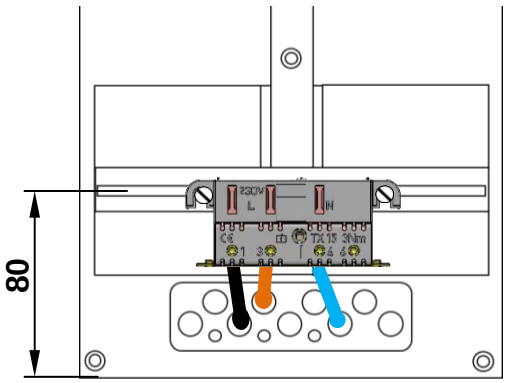
1012

Deckel für
Drehstromklemme
1007-T

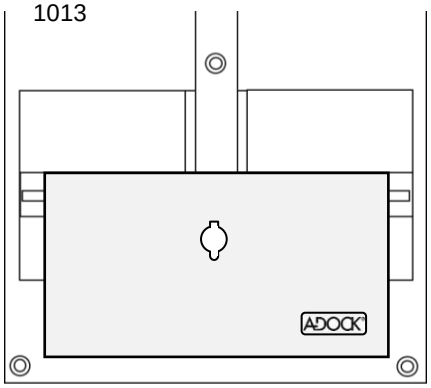


Montage

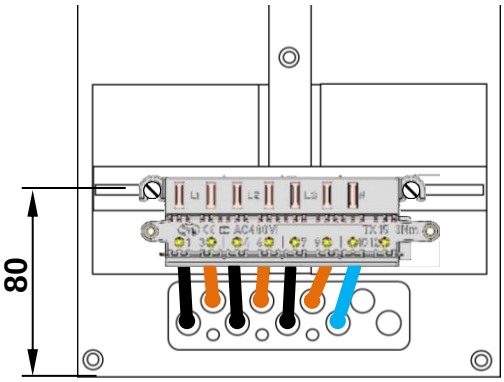
1002-T



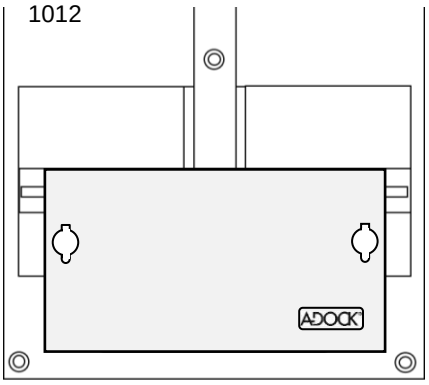
1013



1007-T



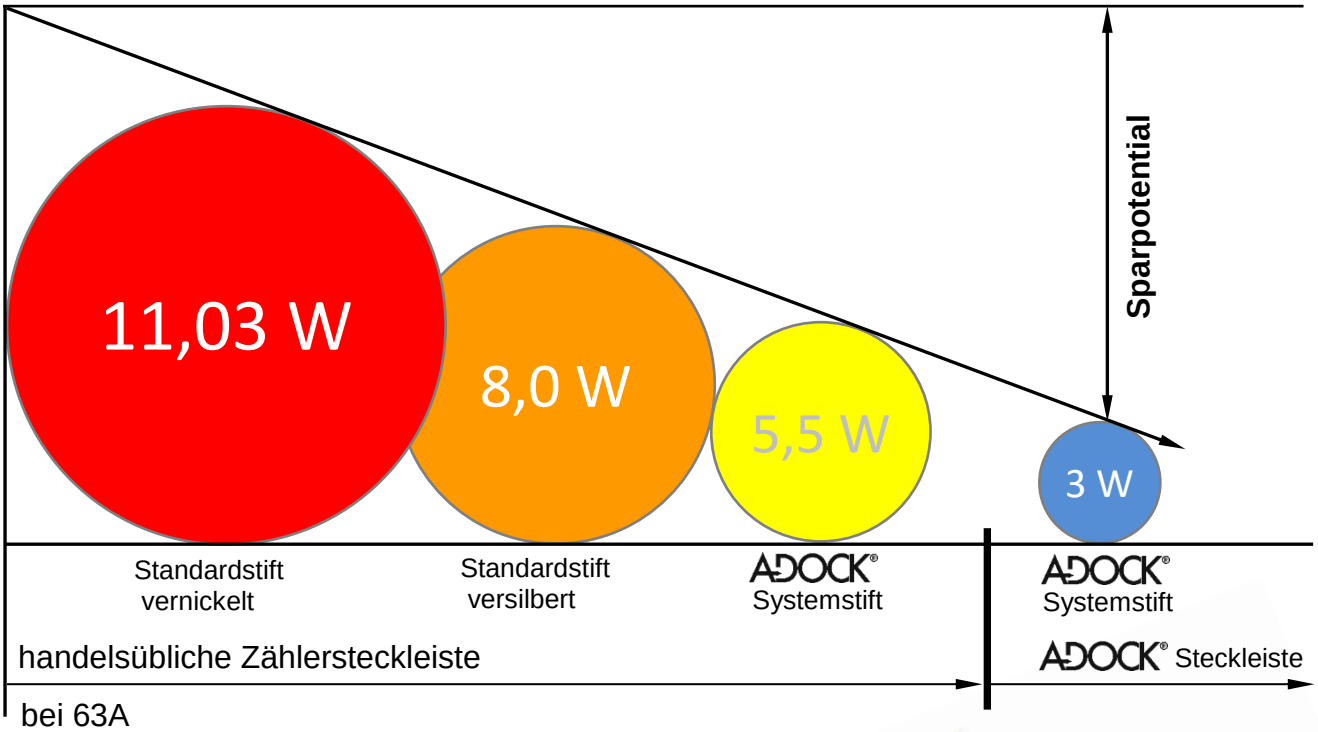
1012



Technische Änderungen vorbehalten

ADOCK® der Energiesparer

Energie-Spardiagramm



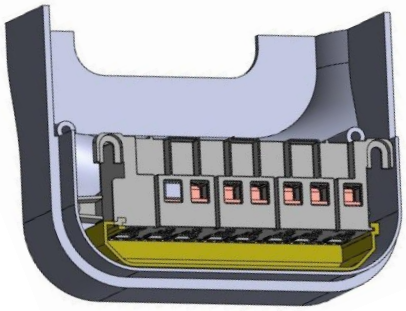


Bild Zähler-Klemmendeckel

ADOCK® Steckleiste 63A
2-polig und 4-polig für Elektrizitätszähler nach DIN 43857
Version mit Anschlussraum-Abdeckung erhältlich

Kompakte Bauform
Die ADOCK® Steckleiste kann in der Regel mit dem **Standard-Zähler-Klemmendeckel** abgedeckt werden.

DUO-Anschluss
Zählerschleifen bis 25mm² Querschnitt können auch nach hinten (Bild 2) angeschlossen werden.
Dies erleichtert die Montage und reduziert die mechanischen Kräfte. Weniger Lagerkosten, eine Steckleiste für alle Anwendungen.

Antimagnetische Edelstahlklemmen
vermeiden gefahrbringende Überhitzung bei Oberwellen.

50% Zeitersparnis beim Anklemmen der Zählerschleife
Nur 1 Schraube pro Klemmstelle in der ADOCK® Steckleiste.
Kraftsparendes Anschrauben – nur 3Nm Anzugsdrehmoment!
Robuste Schrauben TX15 aus hochfestem Stahl.

Mit Anschlussraumabdeckung

6-10mm²

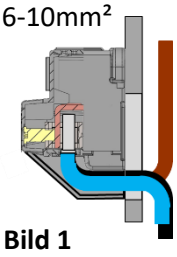


Bild 1
Anschluss unten

6-25mm²

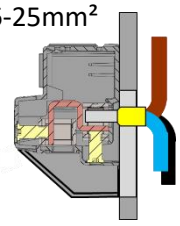


Bild 2
Anschluss hinten

Ohne Anschlussraumabdeckung

6-25mm²

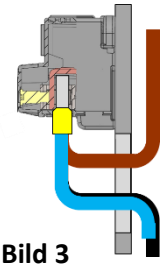


Bild 3
Anschluss unten

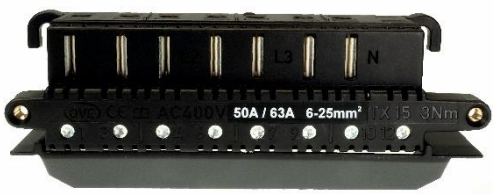


Bild Anschlussraum-Abdeckung

Klaus Bruchmann GmbH
Obere Dorfstraße 33
4616 Weißkirchen
Tel.: +43 699 17185619
E-Mail: gs@tytan.at

Druck-Nr.:0720/18-1005

Technische Änderungen vorbehalten

Stand 29.08.2018

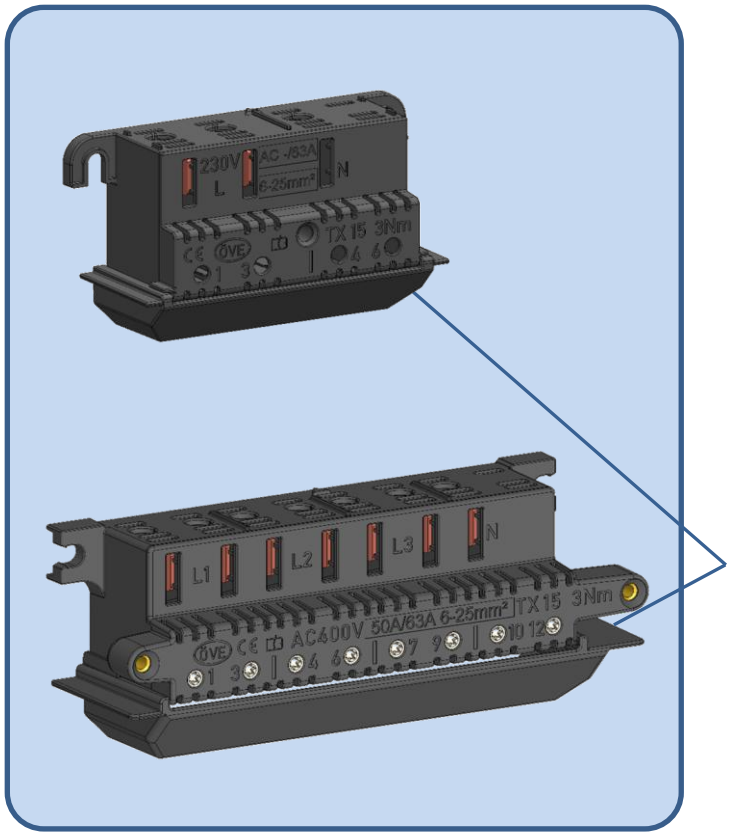
DATENBLATT / DATA SHEET

ADOCK

Version: 22.10.2025

Zähleranschlussklemmen und Zubehör
Meter connection terminal and accessories

FOTO



INFO

Für Elektrizitätszähler
nach DIN 43857
- Versionen mit Anschlussraumabdeckung
- Mit Standard Zähler-Klemmendeckel abdeckbar
- Entlastung der Kontakte ermöglicht eine kraftlose Steck-Montage des Zählers
- DUO-Version mit Anschlusswahlmöglichkeit (nach unten oder hinten)

For energy meter
according to DIN 43857
- Versions with wiring space cover
- To be covered with standard meter terminal cover
- Relieving the contacts makes it possible to mount the meter without force
- DUO-Version with choice of connection (at bottom or back)

HANDELSMARKE / TRADE MARK

ADOCK®

VERSIONEN / VERSIONS

Steckleiste für Wechselstromzähler
- Anschluss nach unten

Plug-in terminal block for Single-phase meters
- Connection at the bottom

Steckleiste für Drehstromzähler
- DUO-Anschluss (nach unten oder hinten)
- Anschluss nach unten
- Anschluss nach hinten
- Mit Anschlussleitern nach unten

Plug-in terminal block for Three-phase meters
- DUO-Connection (at bottom or back)
- Connection at bottom
- Connection at back
- With connection wires at bottom

DATENBLATT / DATA SHEET

ADOCK

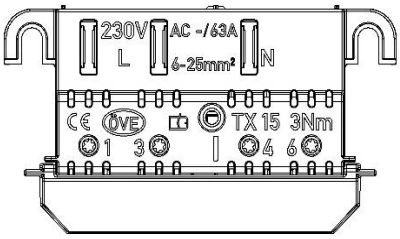
Version: 22.10.2025

TYPENSPEKTRUM / TYPE RANGE

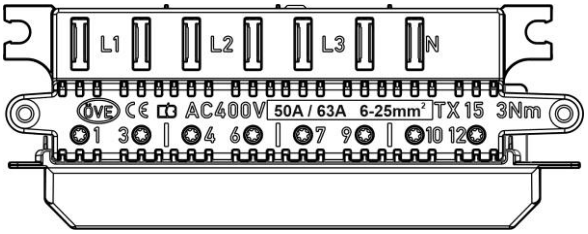
ADOCK Steckleiste / ADOCK Plug-in terminal block

Beschreibung / Description		Artikelnummer / Article no.	
WECHSELSTROM Type / SINGLE-PHASE type			
Bemessungsbetriebsspannung / Rated operational voltage		230 VAC 50Hz	
Max. zulässiger Nennstrom der Überlastschutzeinrichtung Maximum permissible rated current of overload protective device			
Mit Anschlussraumabdeckung / With wiring space cover			
1 polig + 2N / 1 pole + 2N	Anschluss unten / Connection at bottom	63A gG	**1002**
Ohne Anschlussraumabdeckung / Without wiring space cover			
1 polig + 2N / 1 pole + 2N	Anschluss unten / Connection at bottom	63A gG	**1002-T**
DREHSTROM Type / THREE-PHASE type			
Bemessungsbetriebsspannung / Rated operational voltage		400 VAC 50Hz	
Max. zulässiger Nennstrom der Überlastschutzeinrichtung Maximum permissible rated current of overload protective device			
Mit Anschlussraumabdeckung / With wiring space cover			
3 polig + 2N / 3 pole + 2N	DUO-Anschluss / DUO-Connection	63A gG	**1005**
Ohne Anschlussraumabdeckung / Without wiring space cover			
3 polig + 2N / 3 pole + 2N	Anschluss unten / Connection at bottom	63A gG	**1007-T**
3 polig + 2N / 3 pole + 2N	Anschluss unten / Connection at bottom	63A gG	**1007-W**

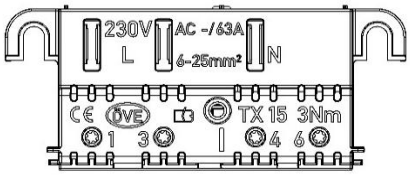
1002



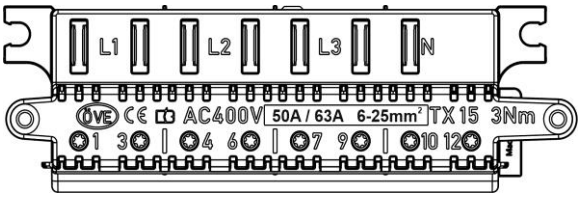
1005



1002-T



1007-T, 1007-W



DATENBLATT / DATA SHEET

ADOCK

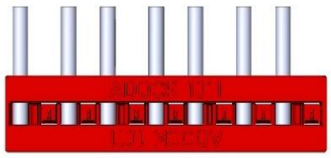
Version: 22.10.2025

TYPENSPEKTRUM / TYPE RANGE

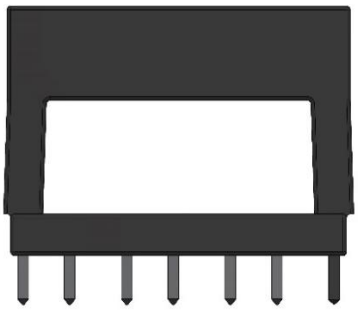
ZUBEHÖR / ACCESSORIES

Beschreibung / Description				Artikelnummer / Article no.
ADOCK Systemstift / ADOCK System pin				
*Im Montagemagazin / Inserted in a mounting magazine				
Bemessungsbetriebsspannung / Rated operational voltage		Länge	400 VAC 50Hz	
Max. zulässiger Nennstrom der Überlastschutzeinrichtung		Length		
Maximum permissible rated current of overload protective device				
1 polig + N / 1 pole + N	3 Systemstifte / 3 system pins	40mm	63A gG	**1010**
3 polig + N / 3 pole +N	7 Systemstifte / 7 system pins	40mm	63A gG	**1011***
3 polig + N / 3 pole +N	7 Systemstifte / 7 system pins	44mm	63A gG	**1011-44***
3 polig + N / 3 pole +N	7 Systemstifte / 7 system pins	50mm	63A gG	**1011-50***
Standardtift / Standard pin				
3 polig + N / 3 pole +N	7 Standardstifte / 7 standard pins	40mm	50A gG	**1011-S***
ADOCK Bügel / ADOCK Clamp				
Für unterbrechungsfreien Zählertausch / For uninterrupted meter exchange				
Einsatzdauer / Duration of use			60min	
Max. zulässiger Nennstrom der Überlastschutzeinrichtung				
Maximum permissible rated current of overload protective device				
1 polig / 1 pole	230 VAC 50Hz		63A gG	**1004**
3 polig / 3 pole	400 VAC 50Hz		63A gG	**1008**

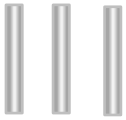
1011



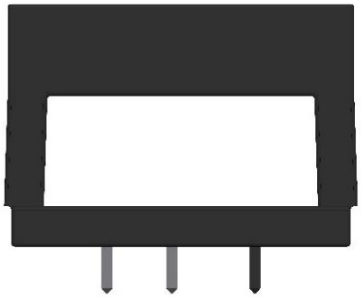
1008



1010



1004



DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

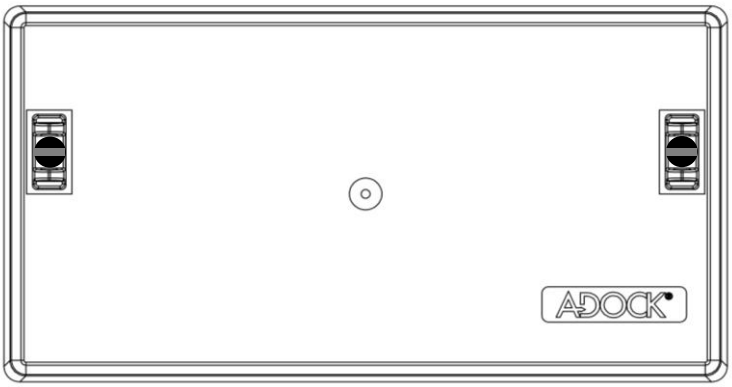
TYPENSPEKTRUM / TYPE RANGE

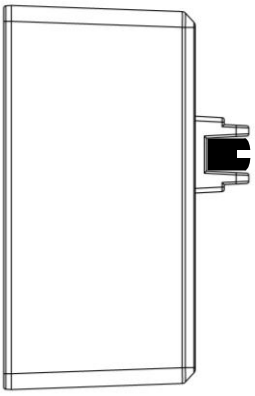
ZUBEHÖR / ACCESSORIES

Beschreibung / Description		Artikelnummer / Article no.
ADOCK Deckel / ADOCK Cover		
1 polig + N / 1 pole + N	160 x 85 x 38(55)mm	**1013**
3 polig + N / 3 pole +N	160 x 85 x 43(55)mm	**1012**

Berührungsschutz für / Touch protection for 1007-T
auf Zählerplatten aus Kunststoff nach / for Meter mounting boards made of plastic acc. to OVE E 8640

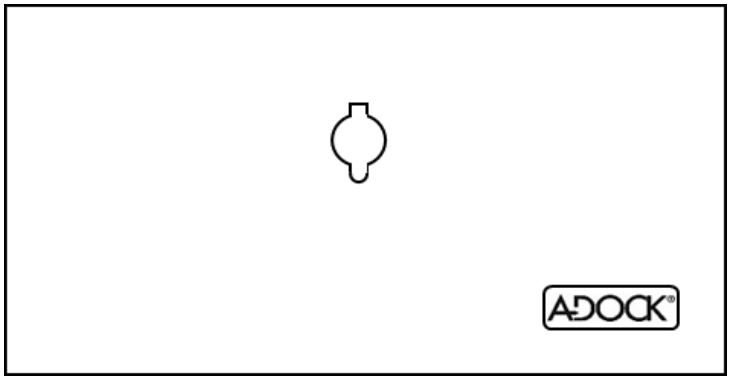
1012

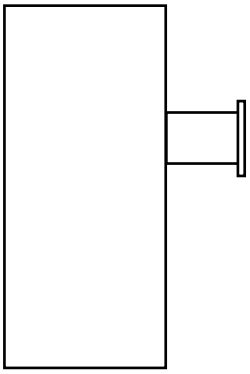




Berührungsschutz für / Touch protection for 1002-T
auf Zählerplatten aus Kunststoff nach / for Meter mounting boards made of plastic acc. to OVE E 8640

1013





DATENBLATT / DATA SHEET

ADOCK

Version: 22.10.2025

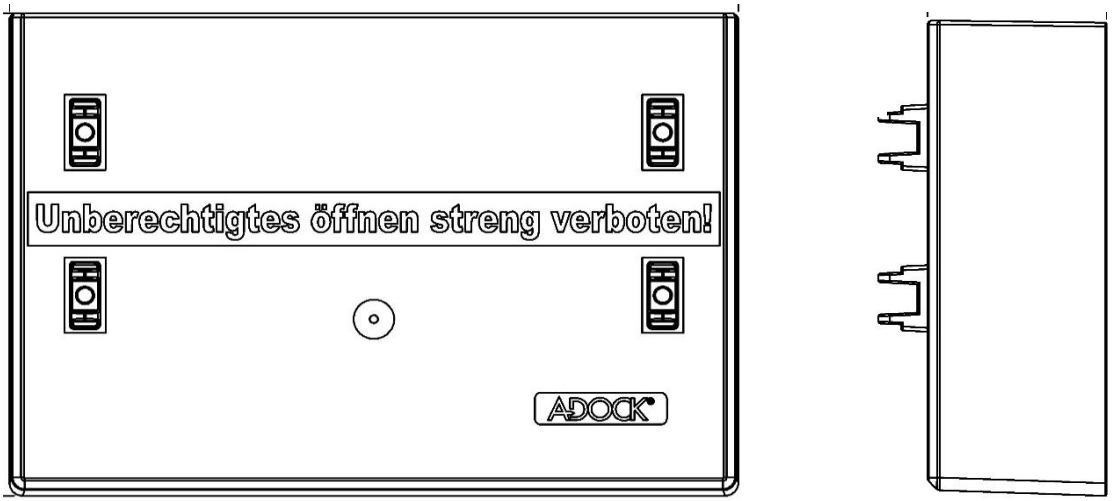
TYPENSPEKTRUM / TYPE RANGE

ZUBEHÖR / ACCESSORIES

Beschreibung / Description		Artikelnummer / Article no.
ADOCK Deckel / ADOCK Cover		
3 polig + N / 3 pole + N	177 x 122 x 43(55)mm	**1014**

Berührungsschutz für / Touch protection for 1007-T
auf Zählerplatten aus Kunststoff nach / for Meter mounting boards made of plastic acc. to OVE E 8640

1014



Auch verwendbar als Klemmenabdeckung für Elektrizitätszähler nach DIN 43857
Can also be used as a terminal cover for power meters according to DIN 43857

DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

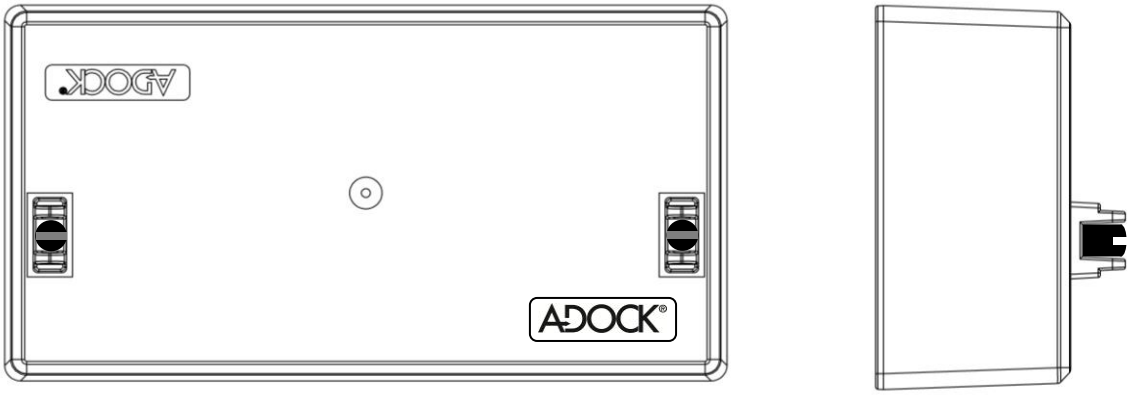
TYPENSPEKTRUM / TYPE RANGE

ZUBEHÖR / ACCESSORIES

Beschreibung / Description		Artikelnummer / Article no.
ADOCK Deckel / ADOCK Cover		
1 polig + N / 1 pole + N	160 x 85 x 38(47)mm	**1013-180**
3 polig + N / 3 pole +N	160 x 85 x 43(55)mm	**1012-180**

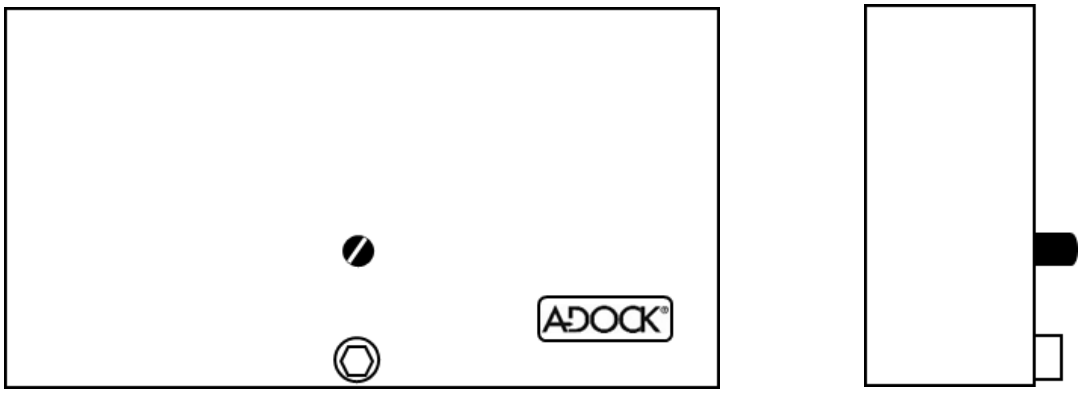
Berührungsschutz für / Touch protection for 1005
auf Zählerplatten aus Kunststoff nach / for Meter mounting boards made of plastic acc. to OVE E 8640

1012-180



Berührungsschutz für / Touch protection for 1002
auf Zählerplatten aus Kunststoff nach / for Meter mounting boards made of plastic acc. to OVE E 8640

1013-180



DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

ELEKTRISCH / ELECTRICAL PROPERTIES

ADOCK Steckleiste / ADOCK Plug-in terminal block				
Geprüft nach / approved acc. to		ÖVE-Richtlinie R 21:2019		
Standards		DIN 43857 OVE E 8640, ÖVE IM12 VDE 0603 Teil 3		
Bedienung durch Laien ist unzulässig **Not to be operated by ordinary persons**		**IEC/EN 61439-3**		
Polzahlen / Poles			1P+2N, 3P+2N	
Bemessungsbetriebsspannung Rated operational voltage	U_e	1P+2N 3P+2N	230 400	VAC VAC
Bemessungsstromstärke Rated current		**VDE 0603 Teil 3**	63	A
Max. zulässige Vorsicherung gegen Kurzschluss Max. permissible back-up fuse against short-circuit			100	A gG
Max. zulässige Sicherung gegen Überlast		**1002(-T)**	-*/**63**	A gG
mit Standardstiften* / ADOCK Systemstiften Max. permissible back-up fuse against overload with Standard pins* / ADOCK system pins		**1005, 1007-T, 1007-W**	50*/**63**	A gG
Bedingter Bemessungskurzschlussstrom Rated conditional short-circuit current	I_{cc}		10	kA_{eff} $kA_{r.m.s.}$
Bemessungsisolationsspannung Rated insulation voltage	U_i		500	V
Bemessungsstoßspannungsfestigkeit Rated impulse withstand voltage	U_{imp}		6	kV
Überspannungskatekorie Overvoltage category			IV	
Kriechstromfestigkeit Comparative tracking index	CTI		600	
Verlustleistung / Power loss	mit ADOCK Systemstiften / with ADOCK system pins			

Type / type	63A	50A	40A	35 A	25A		
1002(-T)	1	0,6	0,3	0,2	0,1	**2xL**	[W]
1005	2,6	1,5	0,8	0,6	0,2	**6xL**	
1007-T	2,6	1,5	0,8	0,6	0,2	**6xL**	
1007-W	2,6	1,5	0,8	0,6	0,2	**6xL**	
	0,4	0,2	0,1	0,07	0,02	**2N**	

DATENBLATT / DATA SHEET

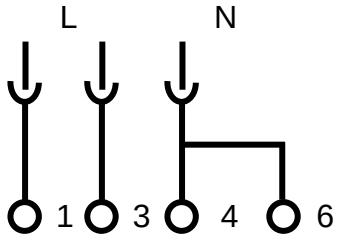
ADOCK Version: 22.10.2025

SCHALTBILDER / CIRCUIT DIAGRAM

ADOCK Steckleiste / ADOCK Plug-in terminal block

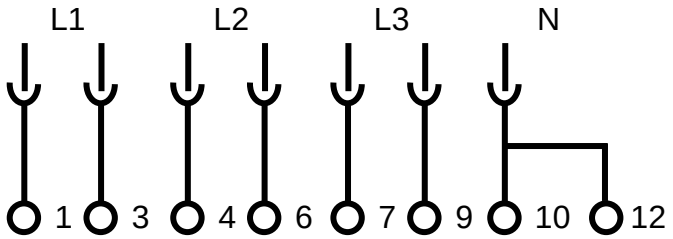
WECHSELSTROM Type / SINGLE-PHASE type

1002(-T)

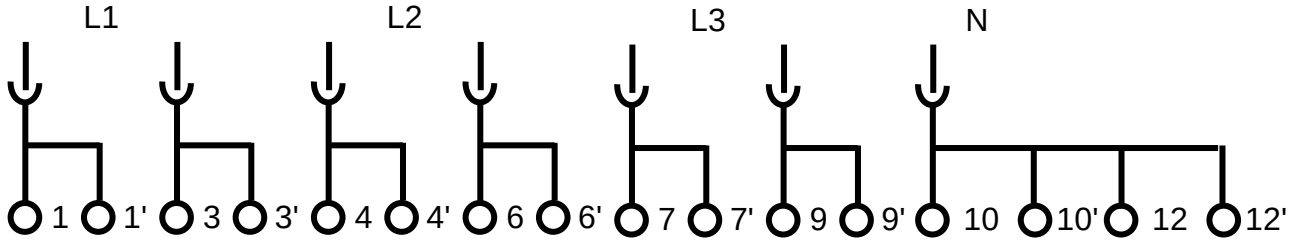


DREHSTROM Typen / THREE-PHASE types

1007-T, 1007-W



1005



DATENBLATT / DATA SHEET

ADOCK

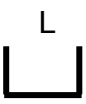
Version: 22.10.2025

ELEKTRISCH / ELECTRICAL PROPERTIES

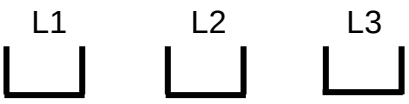
ADOCK Bügel / ADOCK Clamp				
Standards		ÖVE-Richtlinie R 21:2019		
Bedienung durch Laien ist unzulässig **Not to be operated by ordinary persons**		**IEC/EN 61439-3**		
Polzahlen / Poles				1P, 3P
Bemessungsbetriebsspannung Rated operational voltage	U_e	1P 3P	**1004** **1008**	230 VAC 400 VAC
Max. zulässiger Nennstrom der Überlastschutzeinrichtung Maximum permissible rated current of overload protective device				63 A gG
Max. zulässige Vorsicherung gegen Kurzschluss Max. permissible back-up fuse against short-circuit				100 A gG
Bemessungsisolationsspannung Rated insulation voltage	U_i			500 V
Bemessungsstoßspannungsfestigkeit Rated short-circuit making capacity	U_{imp}			6 kV
Überspannungskatekorie Overvoltage category				IV
Einsatzdauer Operating time				unbegrenzt unlimited

SCHALTBILDER / CIRCUIT DIAGRAM

1004



1008



DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

MECHANISCH / MECHANICAL PROPERTIES

ADOCK Steckleiste / ADOCK Plug-in terminal block

Gewicht Weight	1P+2N 3P+2N	**1002**	123	g
		1002-T	115	g
		1005	372	g
		1007-T	273	g
		1007-W	273	g

Klemme / Terminal		Liftklemmen Lift terminal	antimagnetischer Edelstahl stainless steel antimagnetic	
1002(-T)	Schraube / Screw	Torx	TX15	
1005	Anschlussquerschnitt / Cross section		6-25	mm²
1007-T	Anzugsdrehmoment M_n		3	Nm ±10%
1007-W	Tightening torque			

Schutzart (bei montiertem Standard-Zähler-Klemmendeckel) Degree of protection (with mounted standard meter terminal cover)			IP 20C	
Temperaturbereich Temperature range	IEC 61439	Umgebungsluft / Ambient air	-25 bis +40	°C
		24h Durchschnitt / Average	≤ +35	°C
		Lagerung / Storage	-25 bis +60	°C
Grenzübertemperaturen Temperature-rise limits	IEC 61439-1 Klemmen / Terminals		≤ +75	°K

Brandklasse / Flame class	nach UL94 / according to UL94	V0	
Glühdrahtprüfung / Glow wire test		960*	°C
Verschmutzungsgrad / Pollution degree		3	
Kunststoff Plastic	halogen-, phosphor-, silikonfrei Halogen-, silicone-, and phosphorfree		

* Isolierstoffteile, die stromführende Teile in Lage fixieren

* Parts of insulating material necessary to retain current-carrying parts in position

DATENBLATT / DATA SHEET

ADOCK

Version: 22.10.2025

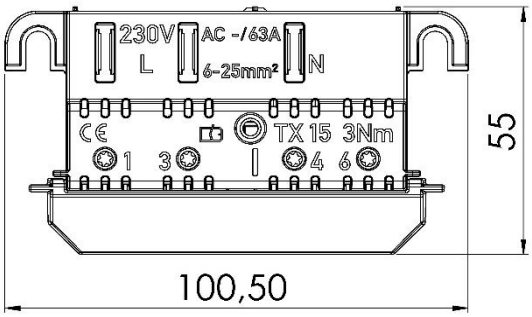
MECHANISCH / MECHANICAL PROPERTIES

ADOCK Steckleiste / ADOCK Plug-in terminal block

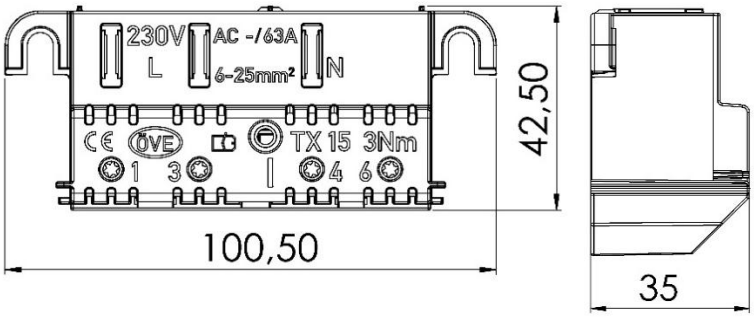
Abmessungen	B x H x T	**1002**	100,5 x 55 x 35	mm
Dimensions	W x H x D	**1002-T**	100,5 x 42,5 x 36	mm
		1005	151 x 58 x 40	mm
		1007-T, 1007-W	151 x 46,5 x 40	mm

WECHSELSTROM Type / SINGLE-PHASE type

1002

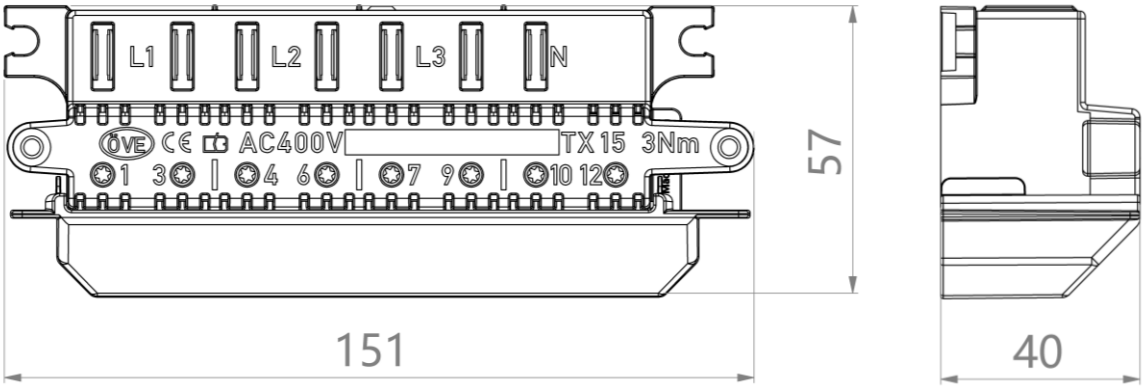


1002-T

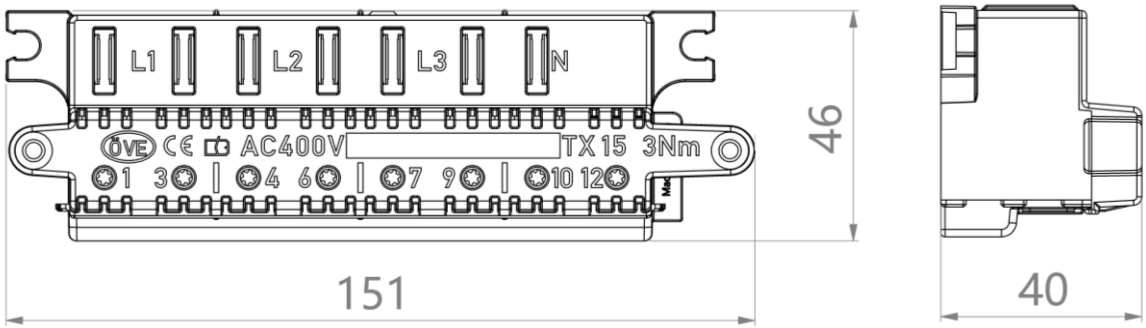


DREHSTROM Typen / THREE-PHASE types

1005



1007-T, 1007-W



DATENBLATT / DATA SHEET

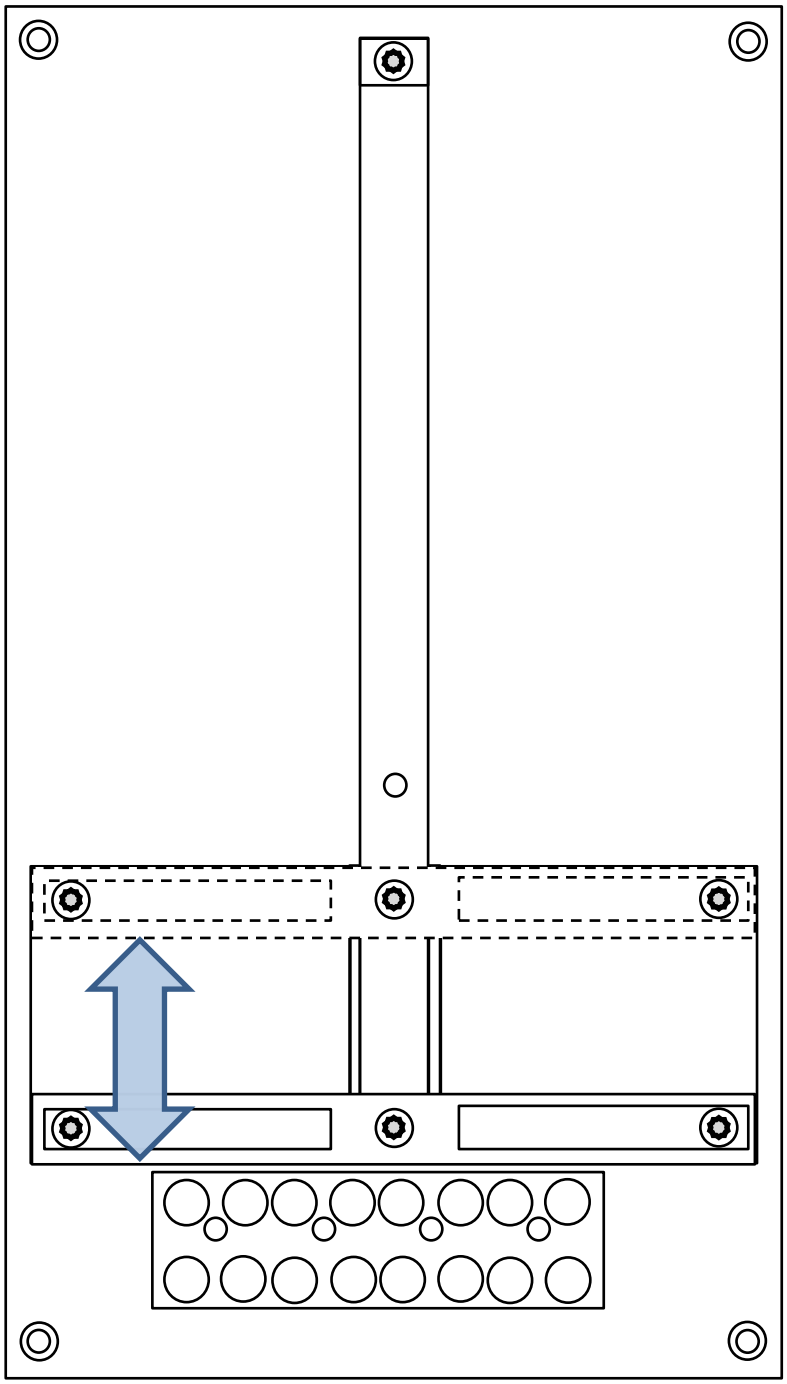
ADOCK Version: 22.10.2025

MECHANISCH / MECHANICAL PROPERTIES

ADOCK Steckleiste / ADOCK Plug-in terminal block

Montage Mounting	Auf Zählerplatten aus Kunststoff nach ÖNORM E 6570 oder auf, durch den lokalen Verteilnetzbetreiber, zugelassenen Isolierstoffplatten Onto meter mounting boards made of plastic according to ÖNORM E 6570 or onto insulation boards authorized by the local distribution system operator

ÖNORM E 6570



Einstellbereich
Adjustment range

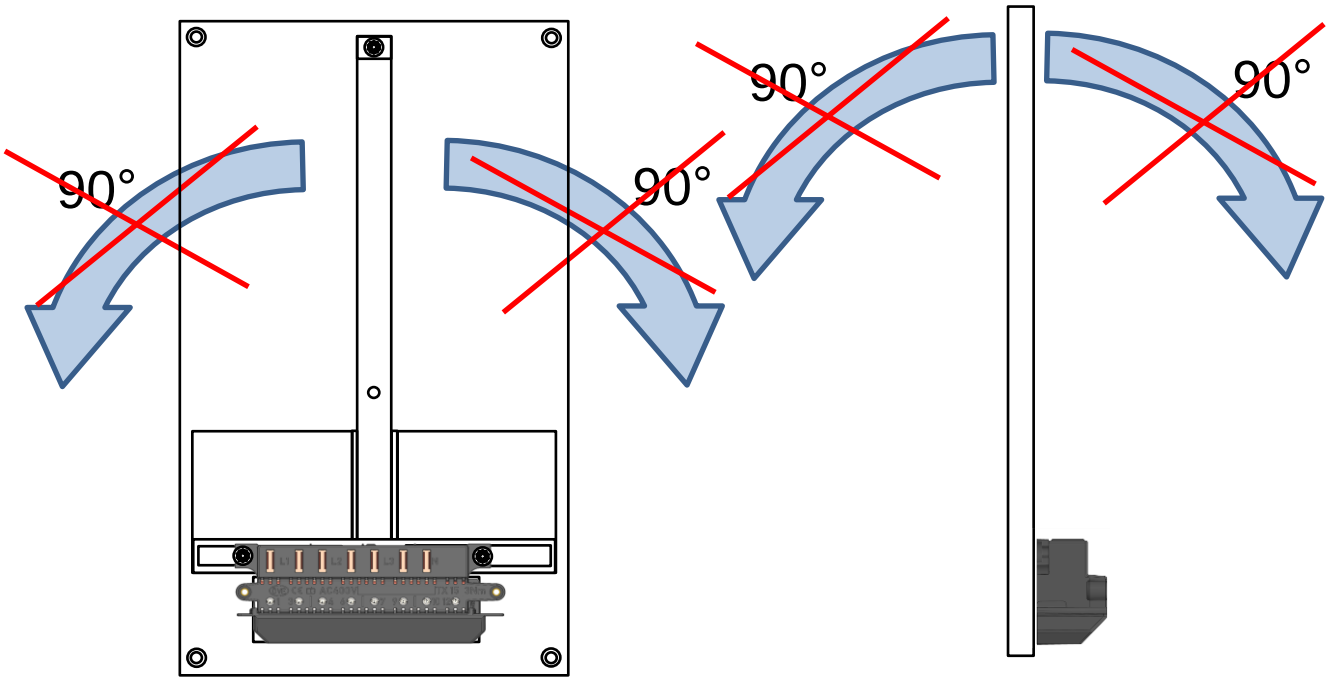
ADOCK Version: 22.10.2025

MECHANISCH / MECHANICAL PROPERTIES

ADOCK Steckleiste / ADOCK Plug-in terminal block

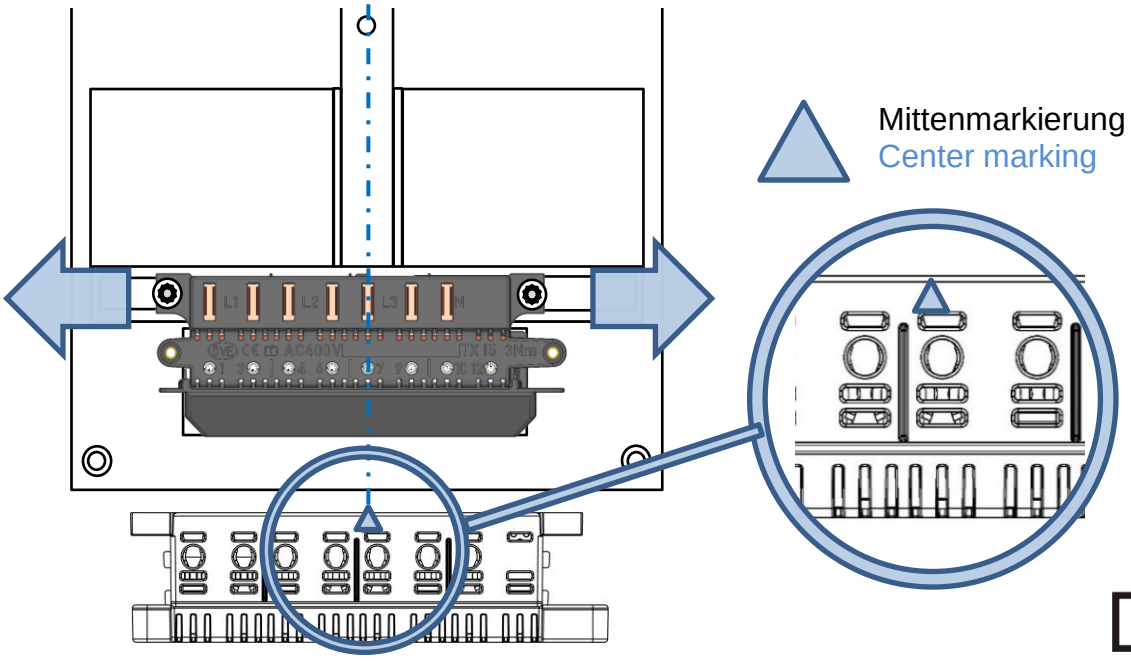
Einbaulage

Mounting position



Positionieren der ADOCK Steckleiste in der Zählermitte

Positioning of ADOCK Plug-in terminal block in the meter center



DATENBLATT / DATA SHEET

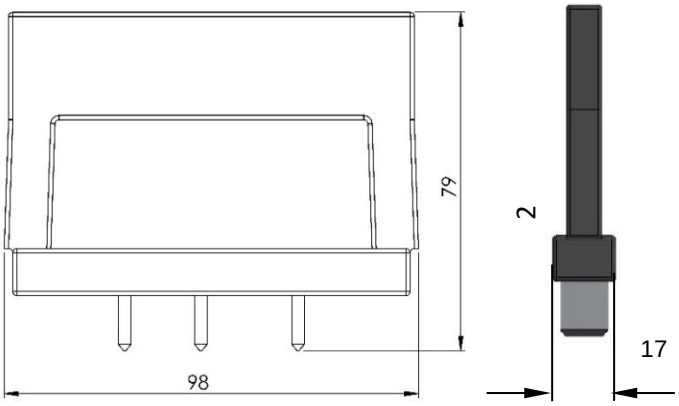
ADOCK

Version: 22.10.2025

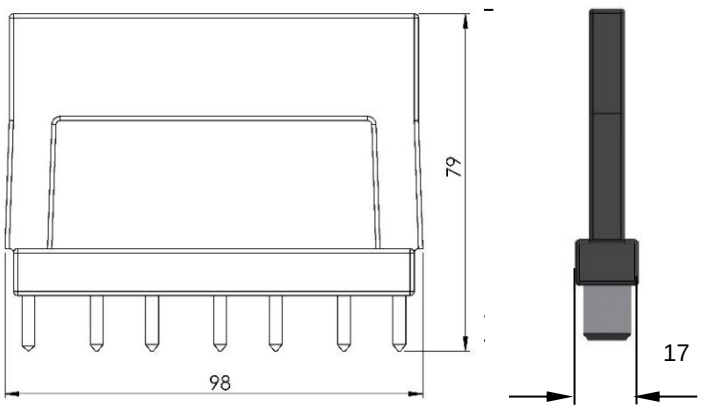
MECHANISCH / MECHANICAL PROPERTIES

ADOCK Bügel / ADOCK Clamp					
Gewicht	1P		**1004**	44	g
Weight	3P		**1008**	76	g
Schutzart				IP 00	
Degree of rotection					
Temperaturbereich		Lagerung / Storage		-25 bis +60	°C
Temperature range					
Grenzübertemperaturen	ÖVE R21			≤ +75	°K
Temperature-rise limits					
Glühdrahtprüfung / Glow wire test				960	°C
Abmessungen	B x H x T		1P	98 x 78 x 17	mm
Dimensions	W x H x D		3P	98 x 78 x 17	mm

1P



3P



DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

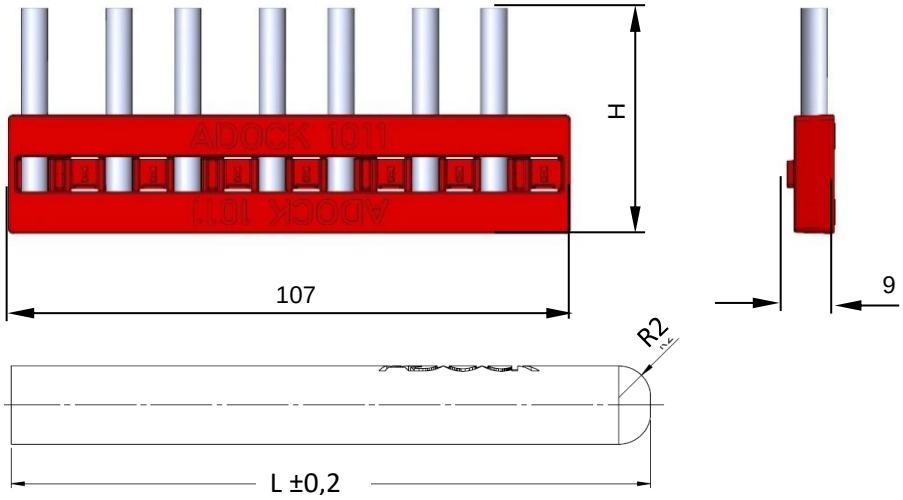
MECHANISCH / MECHANICAL PROPERTIES

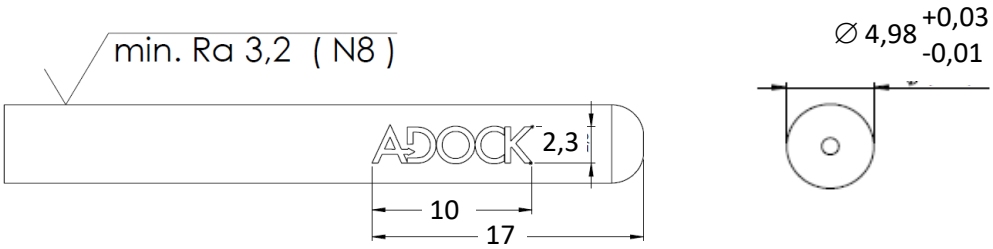
ADOCK Systemstift / ADOCK System pin

Gewicht Weight	3P+N	Magazin / Magazine	**1011**	55	g
			1011-44	60	g
			1011-50	69	g
	ADOCK Sytemstift / ADOCK System pin		**1011**	6,92	g
			1011-44	7,61	g
			1011-50	8,65	g
Grenzübertemperaturen Temperature-rise limits	ÖVE R21			≤ +75	°K
Ursprungszeichen Sign of origin	ÖVE R21			A-DOCK	
Typenbezeichnung Type designation	ÖVE R21			A-DOCK	
Oberflächenrauigkeit Surface finish	ÖVE R21		ÖNORM EN ISO 4287	N8	

Abmessungen Dimensions	B x H x T W x H x D	3P+N	Magazin Magazine	**1011**	107 x 45 x 9	mm
				1011-44	107 x 49 x 9	mm
				1011-50	107 x 54 x 9	mm
	Ø x L Ø x L	ADOCK Sytemstift ADOCK System pin		**1011**	4,99 x 40	mm
				1011-44	4,99 x 44	mm
				1011-50	4,99 x 50	mm

1011, 1011-44





DATENBLATT / DATA SHEET

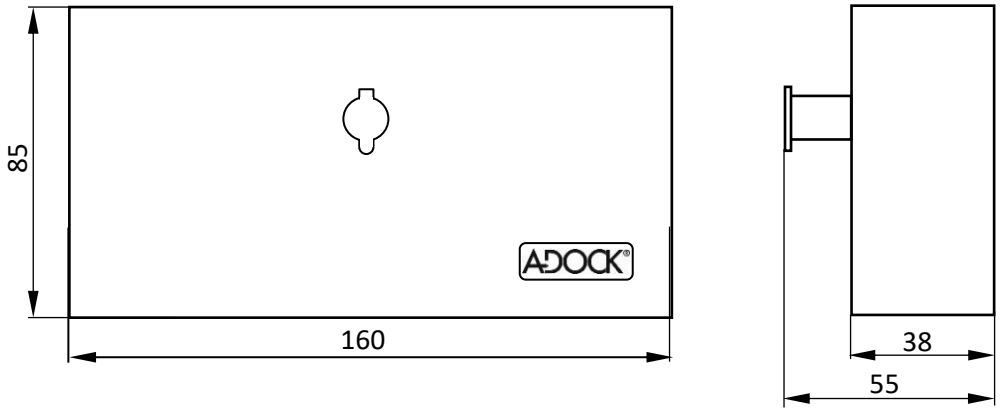
ADOCK Version: 22.10.2025

MECHANISCH / MECHANICAL PROPERTIES

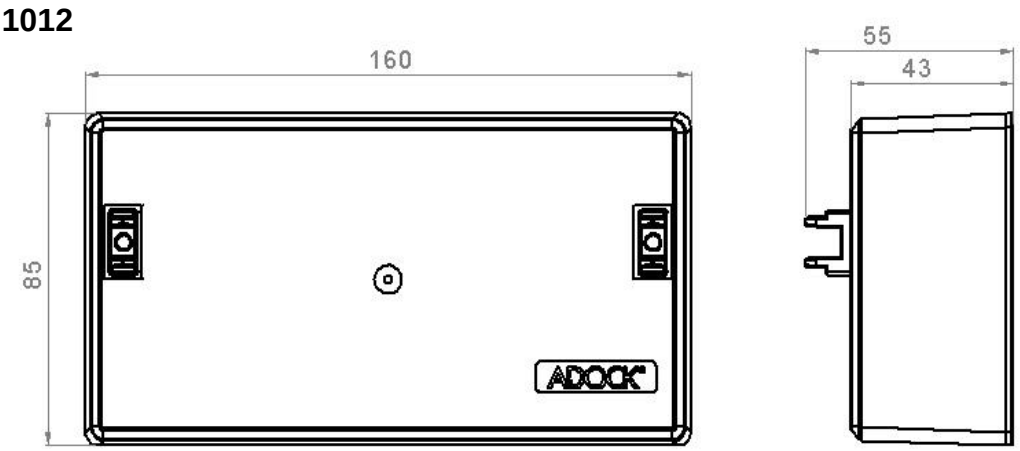
ADOCK Deckel / ADOCK Cover

Gewicht Weight	1P+N 3P+N	**1013** **1012**	156 70	g g
Schutzart Degree of rotection			IP 20C	
Temperaturbereich Temperature range		Lagerung / Storage	-25 bis +60	°C
Grenzübertemperaturen Temperature-rise limits	ÖVE R21		≤ +75	°K
Glühdrahtprüfung / Glow wire test			650	°C
Abmessungen Dimensions	B x H x T W x H x D	1P+N 3P+N	160 x 85 x 55 160 x 85 x 55	mm mm

1013



1012



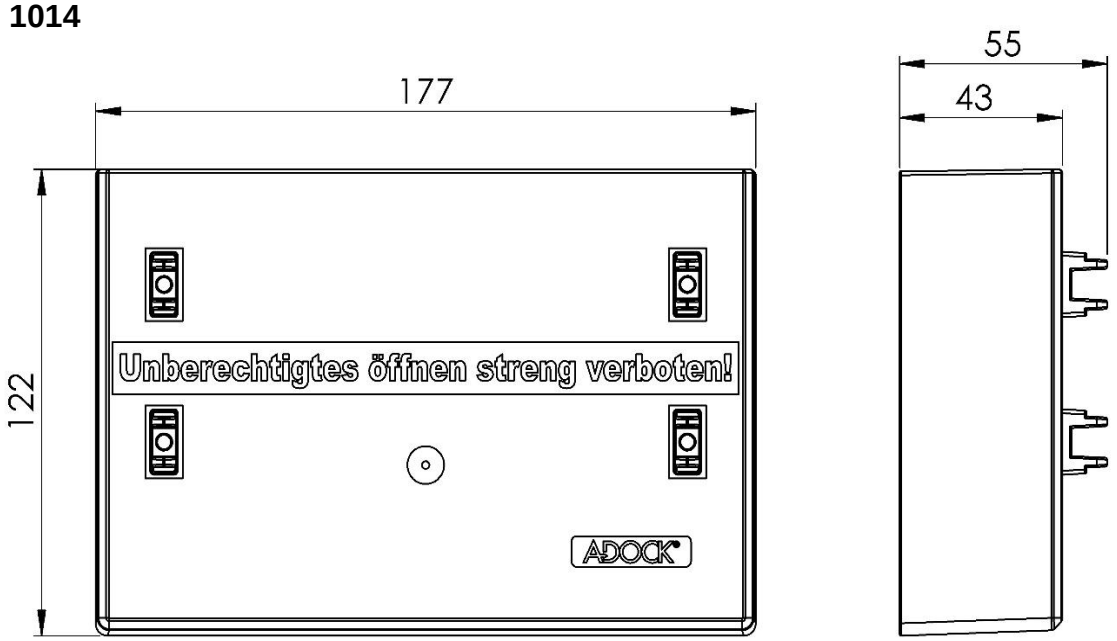
DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

MECHANISCH / MECHANICAL PROPERTIES

ADOCK Deckel / ADOCK Cover				
Gewicht Weight	3P+N	**1014**	124	g
Schutzart Degree of rotection			IP 20C	
Temperaturbereich Temperature range		Lagerung / Storage	-25 bis +60	°C
Grenzübertemperaturen Temperature-rise limits	ÖVE R21		≤ +75	°K
Glühdrahtprüfung / Glow wire test			650	°C
Abmessungen Dimensions	B x H x T W x H x D	3P+N	177 x 122 x 55	mm

1014



DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

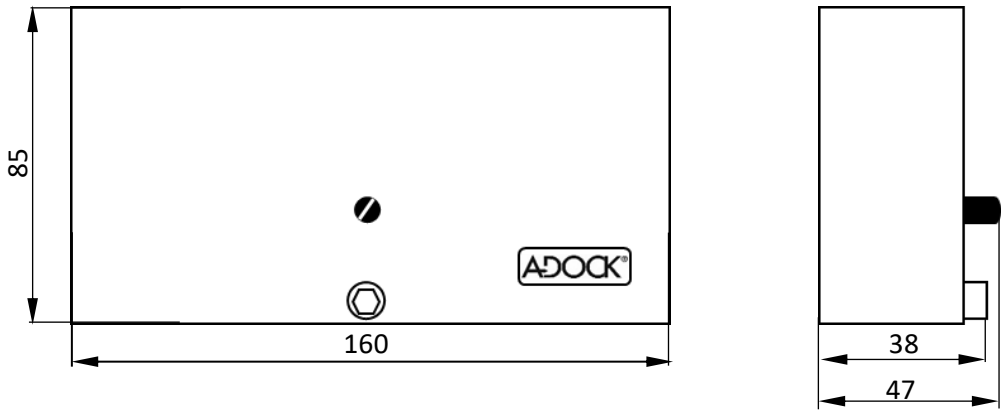
MECHANISCH / MECHANICAL PROPERTIES

ADOCK Deckel / ADOCK Cover

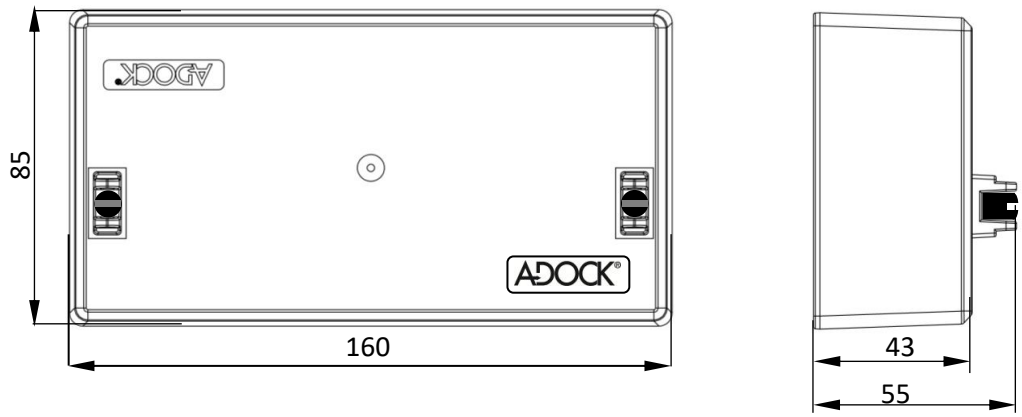
Gewicht Weight	1P+N 3P+N	**1013-180** **1012-180**	148 70	g g
Schutzart Degree of rotection			IP 20C	
Temperaturbereich Temperature range		Lagerung / Storage	-25 bis +60	°C
Grenzübertemperaturen Temperature-rise limits	ÖVE R21		≤ +75	°K
Glühdrahtprüfung / Glow wire test			650	°C

Abmessungen Dimensions	B x H x T W x H x D	1P+N 3P+N	160 x 85 x 47 160 x 85 x 55	mm mm

1013-180



1012-180



DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

LEITER ANSCHLIESSEN und MONTAGE / CONNECT WIRES and MOUNTING

Ausführungsbestimmungen des örtlichen Verteilnetzbetreibers sind zu beachten
Implementing regulations of local distribution system operator has to be considered

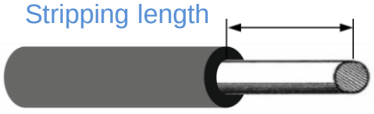
Installation nur durch Elektrofachkräfte
Installation by elctricians only

Vorschriftenkonforme Installation
Einhaltung der technischen Daten
Schutz von Personen und Sachwerten
Dokumentierte Unterweisung der Benutzer
Compliance with installation standards
Compliance with technical specifications
Protection of persons and property
Documented instruction of user

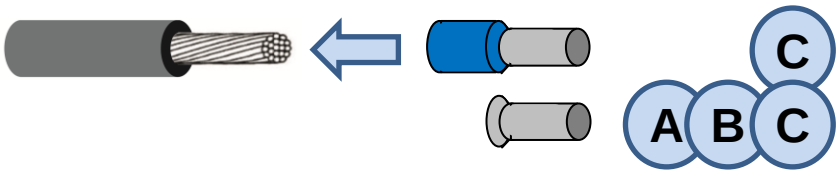
IEC 60417-6182
Installation, electrotechnical expertise

LEITERART / DESIGN OF WIRE	IEC 60288		
	Klasse / class	Type / type	Form / form
eindrähtig rigid	1	**H** xx xx **- U** x x xxx	rund round
mehrdrähtig stranded	2	**H** xx xx **- R** x x xxx	rund round
feindrähtig flexible	**5**	**H** xx xx **- F** x x xxx **H** xx xx **- K** x x xxx	rund round

Abisolierlänge 12mm
Stripping length



Bei feindrähtigen Leitern mit Aderendhülse nach DIN 46228
Use ferrules for flexible wires according DIN 46228



LEITERMATERIAL / WIRING MATERIAL Nur Kupfer / Only Copper

PRESSFORMEN / CRIMPING MOLDS

Vierkantpressung / Square crimping ≤ 16mm²
(z.B. Presswerkzeug / e.g. crimping tool Klauke K 30/4K)

Trapezpressung / Trapezoid crimping
(z.B. Presswerkzeug / e.g. crimping tool Klauke K 27/1 bzw. K28)

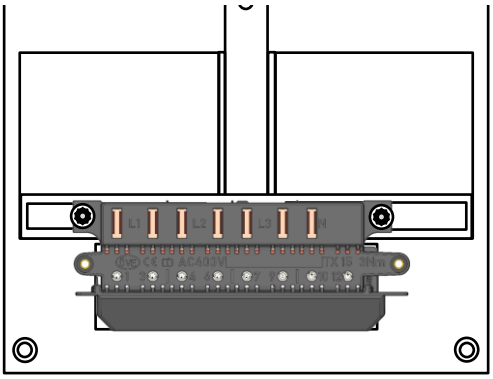
Sechskantpressung / Hexagonal crimping
(z.B. Presswerkzeug / e.g. crimping tool Klauke K 30/6K)

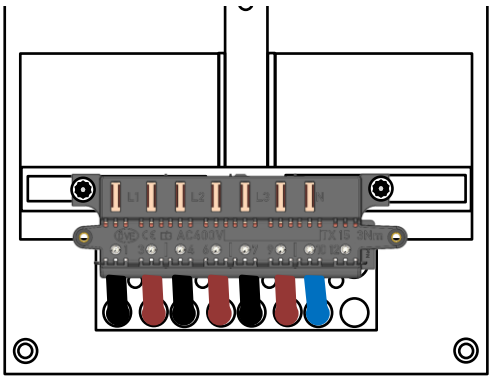
DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

ZÄHLERPLATTE/ METER MOUNTING BOARD

Montagemöglichkeiten / Mounting possibilities



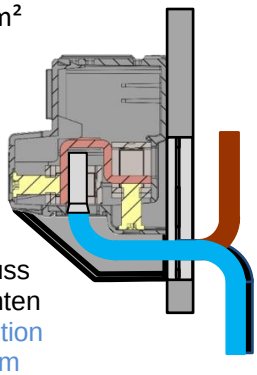


Anschlussmöglichkeiten / Wiring possibilities

Mit Anschlussraumabdeckung
With wiring space cover

6-10mm²

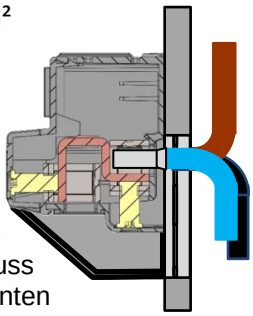
A



Anschluss nach unten
Connection at bottom

6-25mm²

B

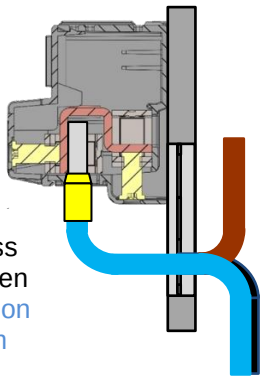


Anschluss nach hinten
Connection at back

Ohne Anschlussraumabdeckung
Without wiring space cover

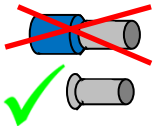
6-25mm²

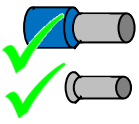
C



Anschluss nach unten
Connection at bottom

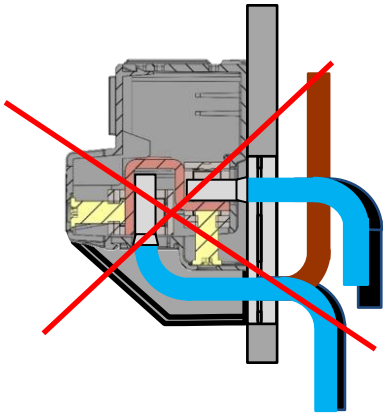
Artikelnummer / Article no.	A	B	C
1002	Ja / Yes	---	---
1005	Ja / Yes	Ja / Yes	---
1002-T	---	---	Ja / Yes
1007-T	---	---	Ja / Yes
1007-W	---	---	Ja / Yes





Weiterverdrahten ist nicht zulässig
Loop wiring is not permitted

1005

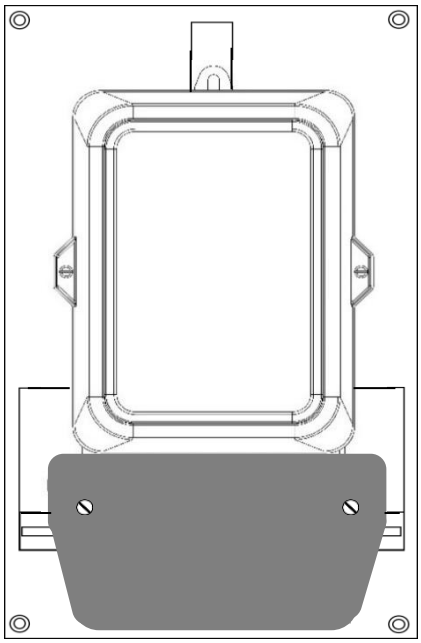


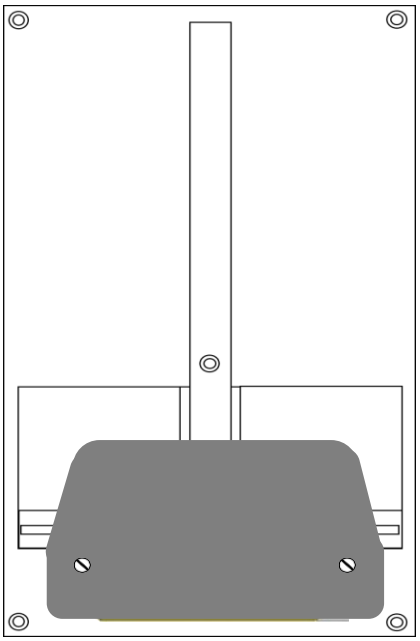
DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

SCHUTZART HERSTELLEN / DEGREE OF PROTECTION SET UP

1002, 1005	**IP2xC**
Standard Zähler-Klemmendeckel nach DIN 43857 Standard meter terminal cover acc. to DIN 43857	Standard Zähler-Klemmendeckel nach DIN 43857 Standard meter terminal cover acc. to DIN 43857



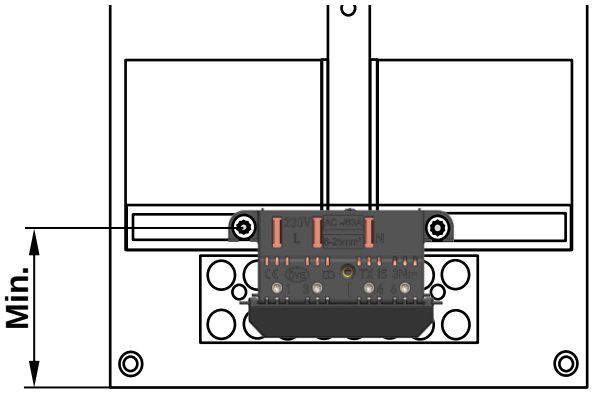


ADOCK Version: 22.10.2025

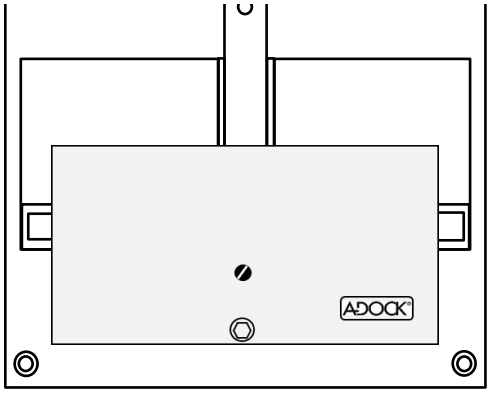
SCHUTZART HERSTELLEN / DEGREE OF PROTECTION SET UP

1002, 1005	IP2xC

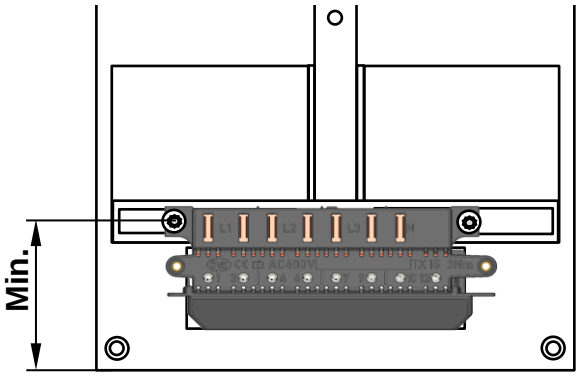
1002



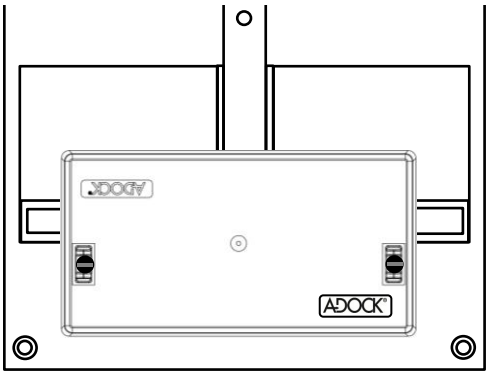
1013-180



1005



1012-180



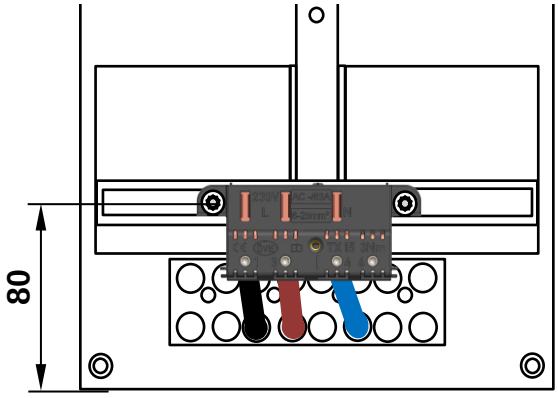
DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

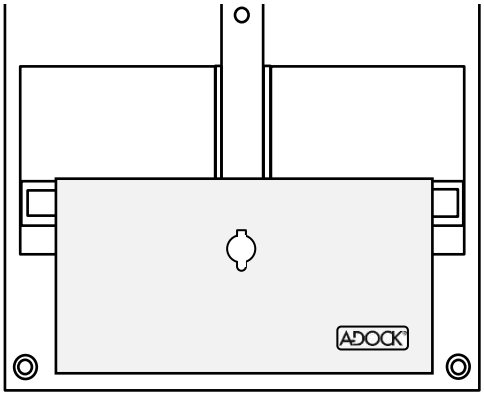
SCHUTZART HERSTELLEN / DEGREE OF PROTECTION SET UP

1002-T, 1007-T	IP2xC

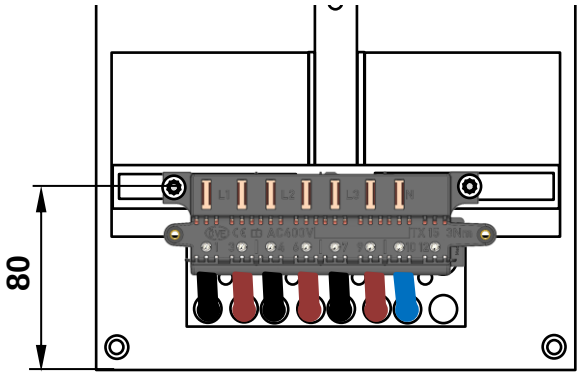
1002-T



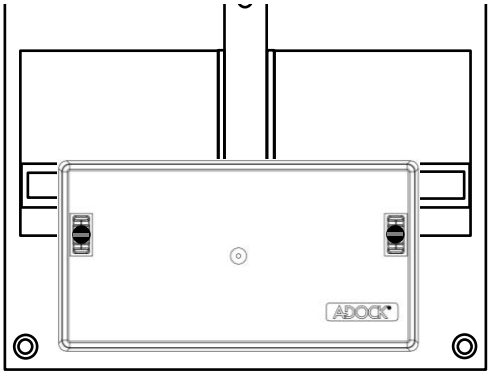
1013



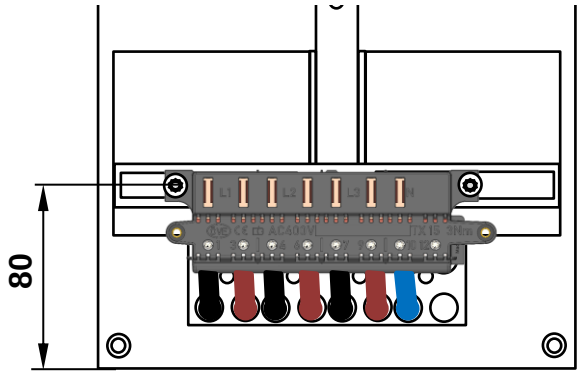
1007-T



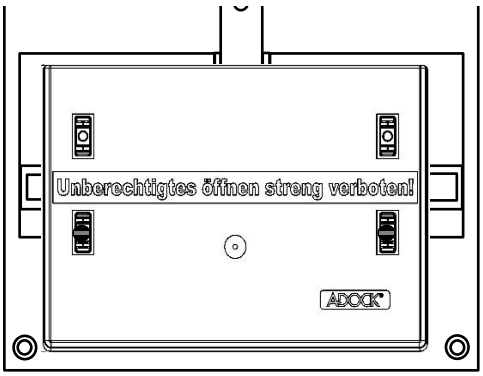
1012



1007-T



1014



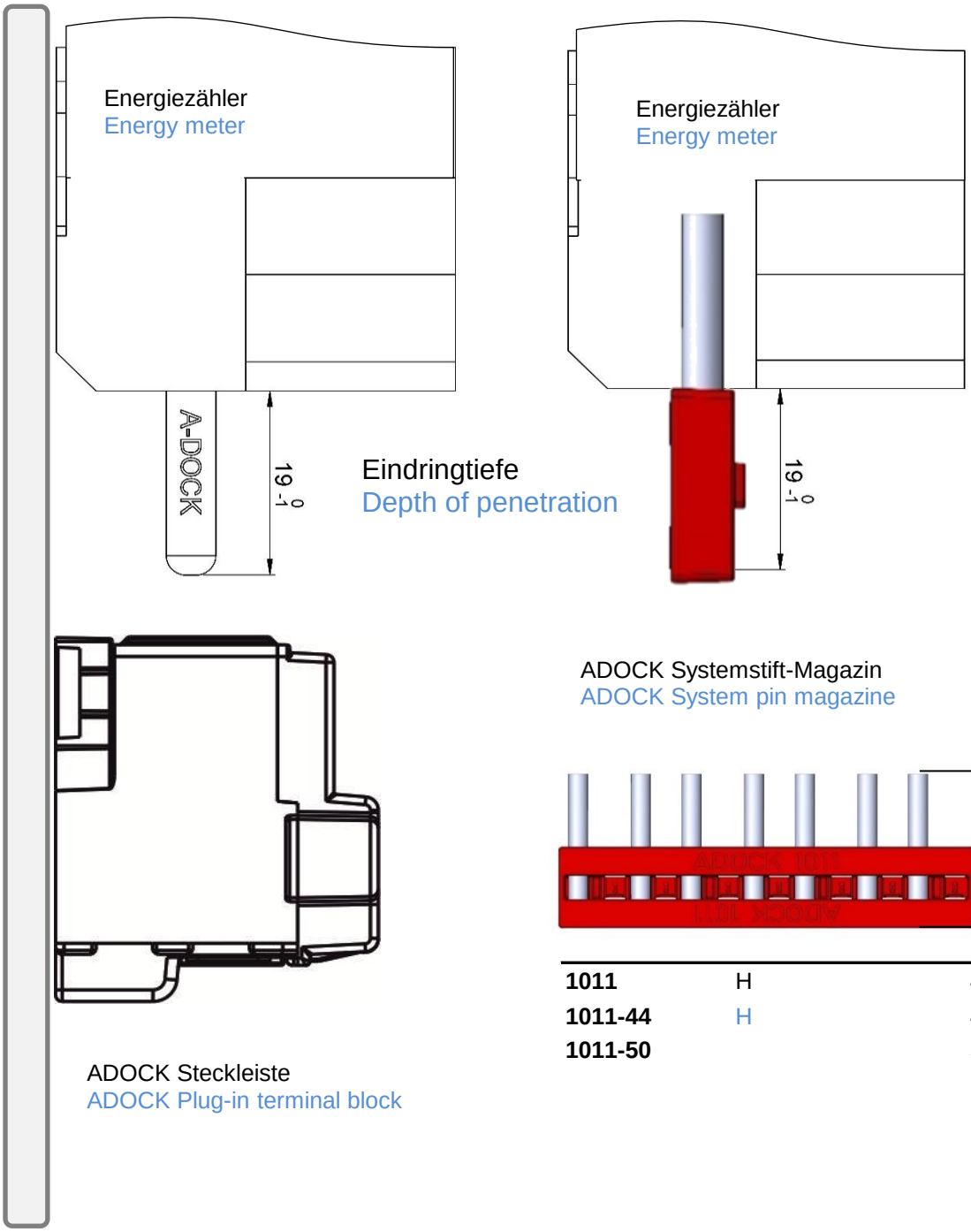
DATENBLATT / DATA SHEET

ADOCK Version: 22.10.2025

STIFTMONTAGE / MOUNTING OF PINS

1002(-T), 1005, 1007-T, 1007-W

STIFTLÄNGE / PIN LENGTH



1011	H	45	mm
1011-44	H	49	mm
1011-50		54	mm

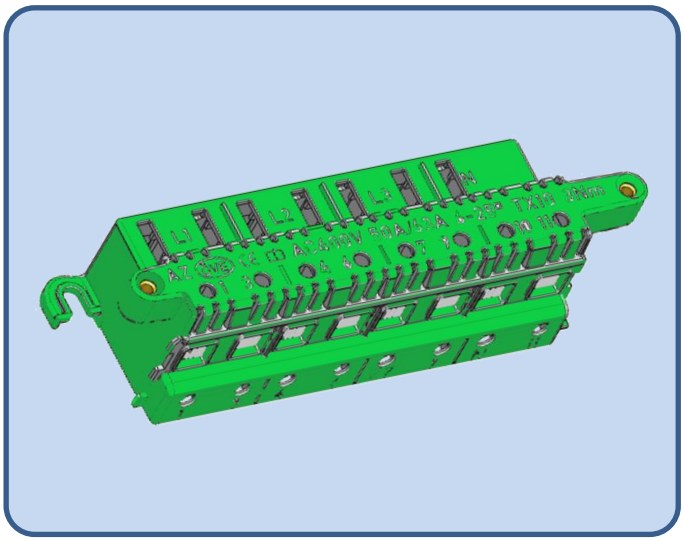
DATENBLATT / DATA SHEET

ZSL63/W

Version: 04.10.2021

Zähleranschlussklemmen und Zubehör
Meter connection terminal and accessories

FOTO



INFO

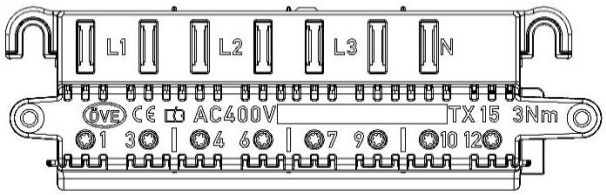
Für Elektrizitätszähler
nach DIN 43857
- Mit Standard Zähler-Klemmendeckel abdeckbar
- Entlastung der Kontakte ermöglicht eine kraftlose Steck-Montage des Zählers

For energy meter
according to DIN 43857
- To be covered with standard meter terminal cover
- Relieving the contacts makes it possible to mount the meter without force

TYPENSPEKTRUM / TYPE RANGE

Beschreibung / Description	Type / Type	Artikelnummer / Article no.
DREHSTROM Type / THREE-PHASE type		
Bemessungsbetriebsspannung / Rated operational voltage		400 VAC 50Hz
Max. zulässiger Nennstrom der Überlastschutzeinrichtung Maximum permissible rated current of overload protective device		63A gG
Anschluss unten / Connection at bottom		
3 polig + 2N / 3 pole + 2N	**ZSL63/W**	**310562**

ZSL63/W



DATENBLATT / DATA SHEET

ZSL63/W

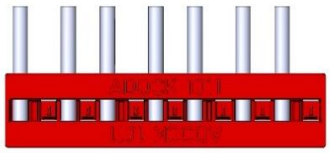
Version: 04.10.2021

TYPENSPEKTRUM / TYPE RANGE

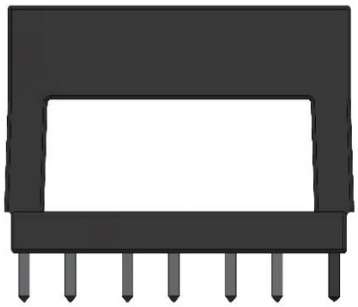
ZUBEHÖR / ACCESSORIES

Beschreibung / Description	Type / Type	Länge / Length	Artikelnummer / Article no.
Systemstift / System pin			
*Im Montagemagazin / Inserted in a mounting magazine			
Bemessungsbetriebsspannung / Rated operational voltage			400 VAC 50Hz
Max. zulässiger Nennstrom der Überlastschutzeinrichtung			63A gG
Maximum permissible rated current of overload protective device			
7 Systemstifte im Magazin / 7 system pins in a magazine			
3 polig + N / 3 pole +N	**ZSL Stift 40mm**		**310611**
3 polig + N / 3 pole +N	**ZSL Stift 44mm**		**310612**
Bügel / Clamp			
Für unterbrechungsfreien Zählertausch / For uninterrupted meter exchange			
Bemessungsbetriebsspannung / Rated operational voltage			400 VAC 50Hz
Einsatzdauer / Duration of use			60min
Max. zulässiger Nennstrom der Überlastschutzeinrichtung			63A gG
Maximum permissible rated current of overload protective device			
3 polig / 3 pole	**KSB63/W**		**310563**

ZSL Stift



KSB63/W



DATENBLATT / DATA SHEET

ZSL63/W

Version: 04.10.2021

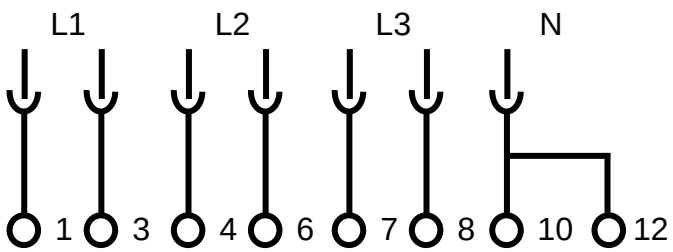
ELEKTRISCH / ELECTRICAL PROPERTIES

Steckleiste / Plug-in terminal block				
Standards		ÖVE-Richtlinie R 21:2019 DIN 43857 ÖNORM E 6570, ÖVE IM12 VDE 0603 Teil 3		
Bedienung durch Laien ist unzulässig **Not to be operated by ordinary persons**		**IEC/EN 61439-3**		
Polzahlen / Poles			3P+2N	
Bemessungsbetriebsspannung Rated operational voltage	U_e	3P+2N	400	VAC
Bemessungsstromstärke Rated current		**VDE 0603 Teil 3**	63	A
Max. zulässige Vorsicherung gegen Kurzschluss Max. permissible back-up fuse against short-circuit			100	A gG
Max. zulässige Sicherung gegen Überlast mit Standardstiften* / ADOCK Systemstiften Max. permissible back-up fuse against overload with Standard pins* / ADOCK system pins			50*/**63**	A gG
Bedingter Bemessungskurzschlussstrom Rated conditional short-circuit current	I_{cc}		10	kA_{eff} $kA_{r.m.s.}$
Bemessungsisolationsspannung Rated insulation voltage	U_i		500	V
Bemessungsstoßspannungsfestigkeit Rated impulse withstand voltage	U_{imp}		6	kV
Überspannungskatekorie Overvoltage category			IV	
Kriechstromfestigkeit Comparative tracking index	CTI		600	
Verlustleistung / Power loss	mit ADOCK Systemstiften / with ADOCK system pins			

Type / type	63A	50A	40A	35 A	25A		
ZSL63/W	2,6	1,5	0,8	0,6	0,2	**6xL**	[W]
	0,4	0,2	0,1	0,07	0,02	**2N**	

SCHALTBILDER / CIRCUIT DIAGRAM

ZSL63/W



DATENBLATT / DATA SHEET

KSB63/W

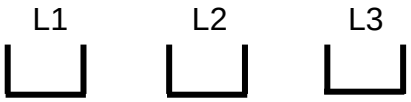
Version: 04.10.2021

ELEKTRISCH / ELECTRICAL PROPERTIES

Bügel / Clamp			
Standards		ÖVE-Richtlinie R 21:2015	
Bedienung durch Laien ist unzulässig **Not to be operated by ordinary persons**		**IEC/EN 61439-3**	
Polzahlen / Poles			3P
Bemessungsbetriebsspannung Rated operational voltage	U_e		400 VAC
Max. zulässiger Nennstrom der Überlastschutzeinrichtung Maximum permissible rated current of overload protective device			63 A gG
Max. zulässige Vorsicherung gegen Kurzschluss Max. permissible back-up fuse against short-circuit			100 A gG
Bemessungsisolationsspannung Rated insulation voltage	U_i		500 V
Bemessungsstoßspannungsfestigkeit Rated short-circuit making capacity	U_{imp}		6 kV
Überspannungskatekorie Overvoltage category			IV
Einsatzdauer Operating time		max.	60 min

SCHALTBILDER / CIRCUIT DIAGRAM

KSB63/W



DATENBLATT / DATA SHEET

ZSL63/W

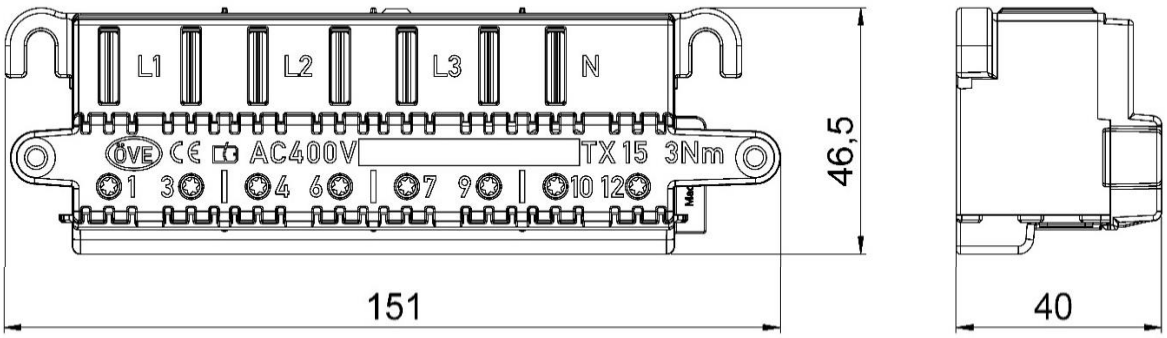
Version: 04.10.2021

MECHANISCH / MECHANICAL PROPERTIES

Steckleiste / Plug-in terminal block

Gewicht Weight	3P+2N		273	g
Klemme / Terminal		Liftklemmen Lift terminal	antimagnetischer Edelstahl stainless steel antimagnetic	
	Schraube / Screw	Torx	TX15	
	Anschlussquerschnitt / Cross section		6-25	mm²
	Anzugsdrehmoment Tightening torque	M_n	3	Nm ±10%
Schutzart (bei montiertem Standard-Zähler-Klemmendeckel) Degree of protection (with mounted standard meter terminal cover)			IP 20C	
Temperaturbereich Temperature range	IEC 61439	Umgebungsluft / Ambient air	-25 bis +40	°C
		24h Durchschnitt / Average	≤ +35	°C
		Lagerung / Storage	-25 bis +60	°C
Grenzübertemperaturen Temperature-rise limits	IEC 61439-1 Klemmen / Terminals		≤ +75	°K
Brandklasse / Flame class		nach UL94 / according to UL94	V0	
Glühdrahtprüfung / Glow wire test			960*	°C
Verschmutzungsgrad / Pollution degree			3	
Kunststoff Plastic		halogen-, phosphor-, silikonfrei Halogen-, silicone-, and phosphorfree		
Abmessungen Dimensions	B x H x T W x H x D		151 x 46,5 x 40	mm

ZSL63/W



* Isolierstoffteile, die stromführende Teile in Lage fixieren

* Parts of insulating material necessary to retain current-carrying parts in position

DATENBLATT / DATA SHEET

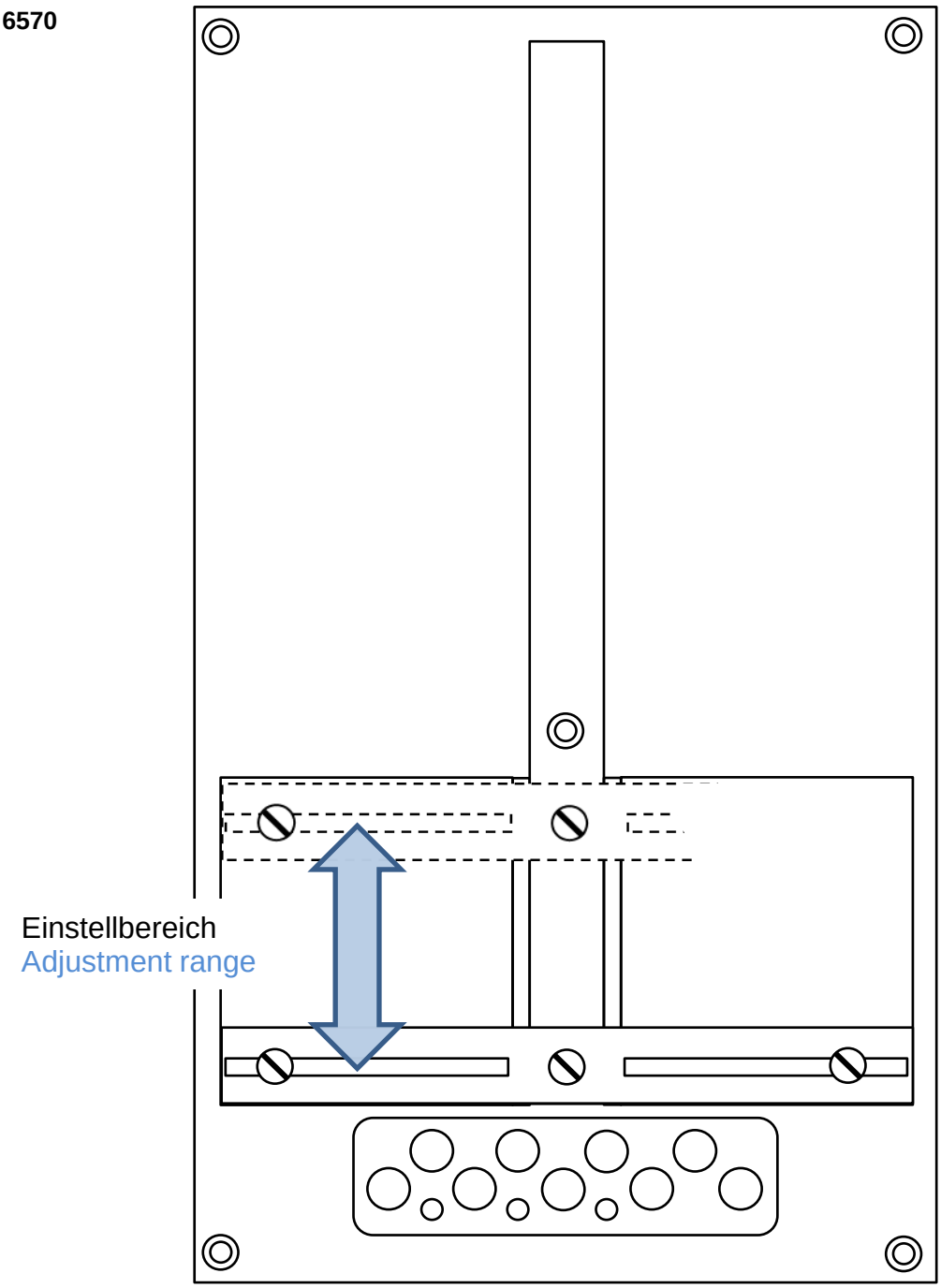
ZSL63/W Version: 04.10.2021

MECHANISCH / MECHANICAL PROPERTIES

Steckleiste / Plug-in terminal block

Montage Mounting	Auf Zählerplatten aus Kunststoff nach ÖNORM E 6570 oder auf, durch den lokalen Verteilnetzbetreiber, zugelassenen Isolierstoffplatten Onto meter mounting boards made of plastic according to ÖNORM E 6570 or onto insulation boards authorized by the local distribution system operator

ÖNORM E 6570



DATENBLATT / DATA SHEET

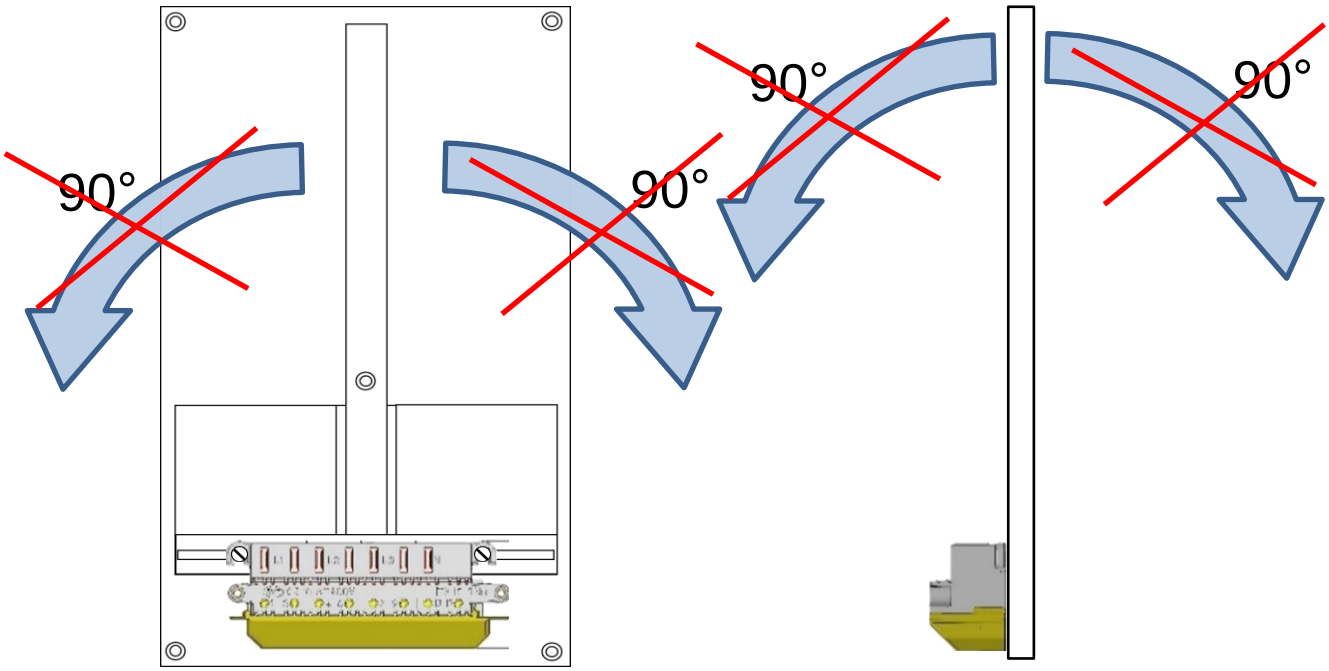
ZSL63/W Version: 04.10.2021

MECHANISCH / MECHANICAL PROPERTIES

Steckleiste / Plug-in terminal block

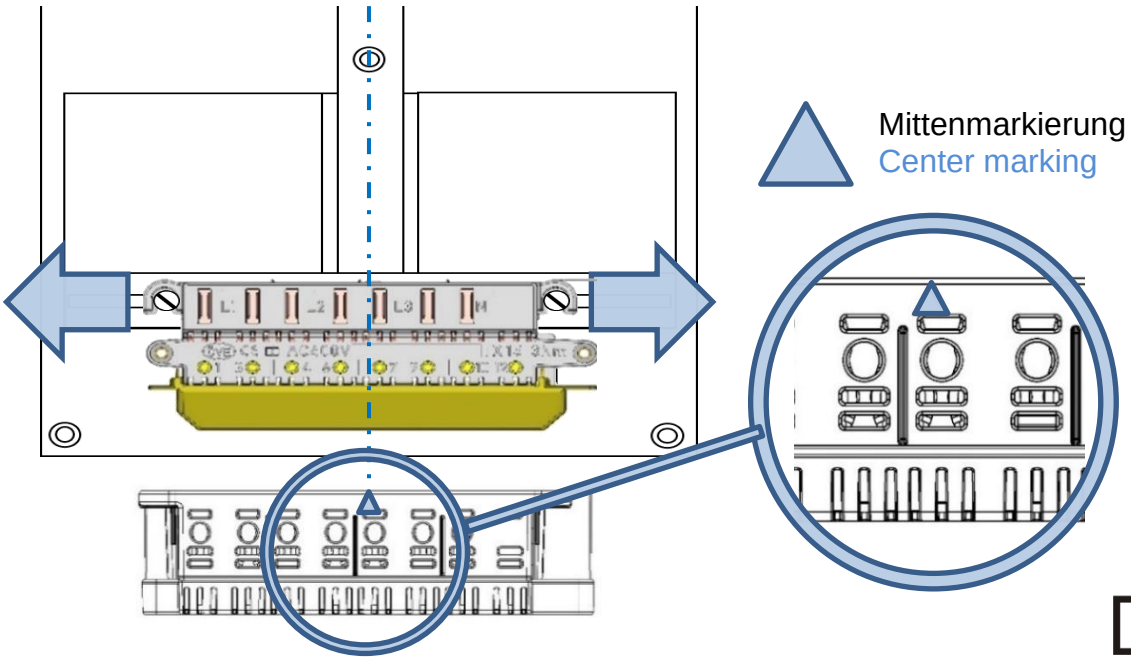
Einbaulage

Mounting position



Positionieren der Steckleiste in der Zählermitte

Positioning of Plug-in terminal block in the meter center



DATENBLATT / DATA SHEET

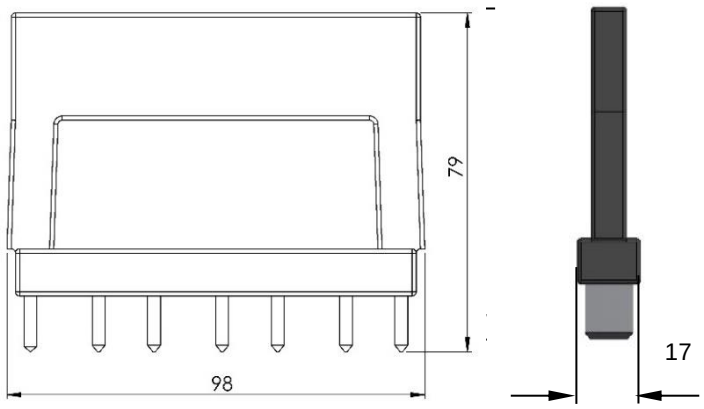
ZSL63/W Version: 04.10.2021

MECHANISCH / MECHANICAL PROPERTIES

Bügel / ADOCK Clamp				
Gewicht Weight	1P 3P		76	g
Schutzart Degree of rotection			IP 00	
Temperaturbereich Temperature range		Lagerung / Storage	-25 bis +60	°C
Grenzübertemperaturen Temperature-rise limits	ÖVE R21		≤ +75	°K
Glühdrahtprüfung / Glow wire test			960	°C

Abmessungen Dimensions	B x H x T W x H x D	1P 3P	98 x 78 x 17 98 x 78 x 17	mm mm

ZSL63/W



DATENBLATT / DATA SHEET

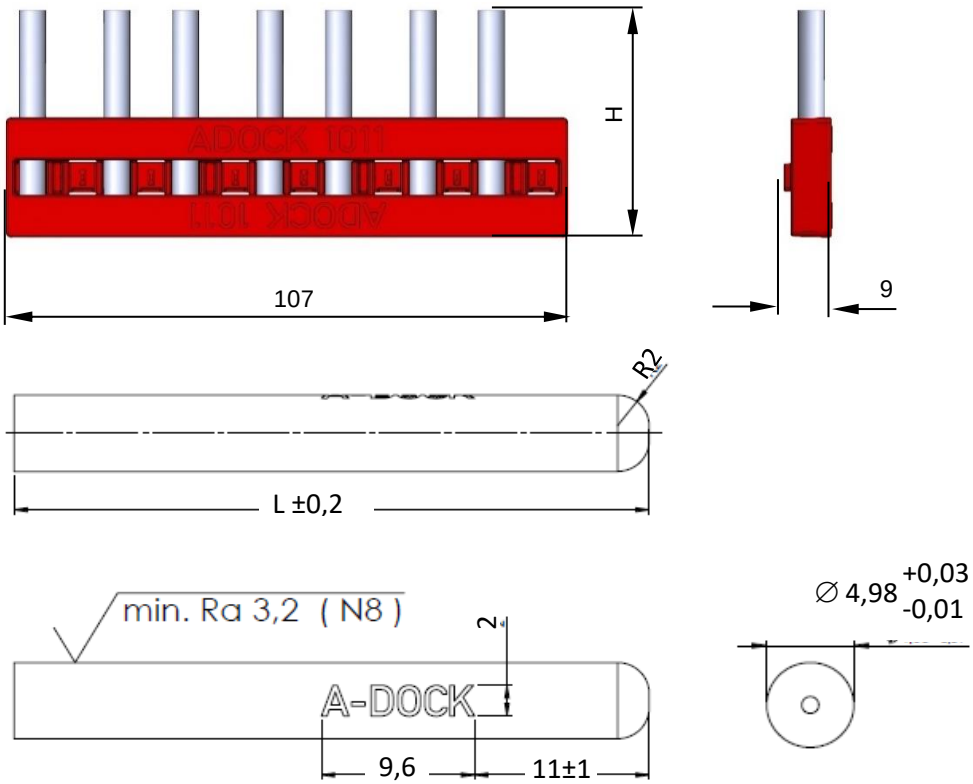
ZSL Stift

Version: 04.10.2021

MECHANISCH / MECHANICAL PROPERTIES

Systemstift / System pin

Gewicht Weight	3P+N	Magazin / Magazine		**310611**	40mm	55	g
				310612	44mm	59,83	g
		Sytemstift / System pin		**Stift**	40mm	6,92	g
				Stift	44mm	7,61	g
Temperaturbereich Temperature range	IEC 61439	Umgebungsluft / Ambient air				-25 bis +40	°C
		24h Durchschnitt / Average				≤ +35	°C
		Lagerung / Storage				-25 bis +60	°C
Grenzübertemperaturen Temperature-rise limits	ÖVE R21					≤ +75	°K
Ursprungszeichen Sign of origin	ÖVE R21					A-DOCK	
Typenbezeichnung Type designation	ÖVE R21					A-DOCK	
Oberflächenrauigkeit Surface finish	ÖVE R21		ÖNORM EN ISO 4287			N8	
Abmessungen Dimensions	B x H x T	3P+N	Magazin	**310611**		107 x 45 x 9	mm
	W x H x D	3P+N	Magazine	**310612**		107 x 49 x 9	mm
	Ø x L	Sytemstift		**40mm**		4,99 x 40	mm
ZSL Stift	Ø x L	System pin		**44mm**		4,99 x 44	mm



DATENBLATT / DATA SHEET

ZSL63/W Version: 04.10.2021

LEITER ANSCHLIESSEN und MONTAGE / CONNECT WIRES and MOUNTING

Ausführungsbestimmungen des örtlichen Verteilnetzbetreibers sind zu beachten
Implementing regulations of local distribution system operator has to be considered

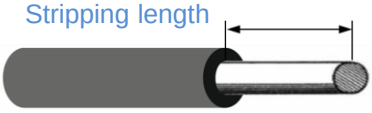
Installation nur durch Elektrofachkräfte
Installation by elctricians only

Vorschriftenkonforme Installation
Einhaltung der technischen Daten
Schutz von Personen und Sachwerten
Dokumentierte Unterweisung der Benutzer
Compliance with installation standards
Compliance with technical specifications
Protection of persons and property
Documented instruction of user

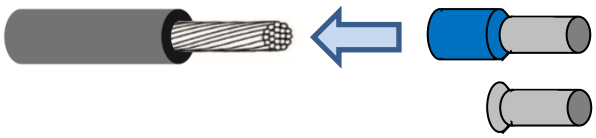
IEC 60417-6182
Installation, electrotechnical expertise

LEITERART / DESIGN OF WIRE	IEC 60288		
	Klasse / class	Type / type	Form / form
eindrähtig rigid	1	**H** xx xx **- U** x x xxx	rund round
mehrdrähtig stranded	2	**H** xx xx **- R** x x xxx	rund round
feindrähtig flexible	**5**	**H** xx xx **- F** x x xxx **H** xx xx **- K** x x xxx	rund round

Abisolierlänge 12mm
Stripping length



Bei feindrähtigen Leitern mit Aderendhülse nach DIN 46228
Use ferrules for flexible wires according DIN 46228



LEITERMATERIAL / WIRING MATERIAL Nur Kupfer / Only Copper

PRESSFORMEN / CRIMPING MOLDS

Vierkantpressung / Square crimping ≤ 16mm²
(z.B. Presswerkzeug / e.g. crimping tool Klauke K 30/4K)

Trapezpressung / Trapezoid crimping
(z.B. Presswerkzeug / e.g. crimping tool Klauke K 27/1 bzw. K28)

Sechskantpressung / Hexagonal crimping
(z.B. Presswerkzeug / e.g. crimping tool Klauke K 30/6K)

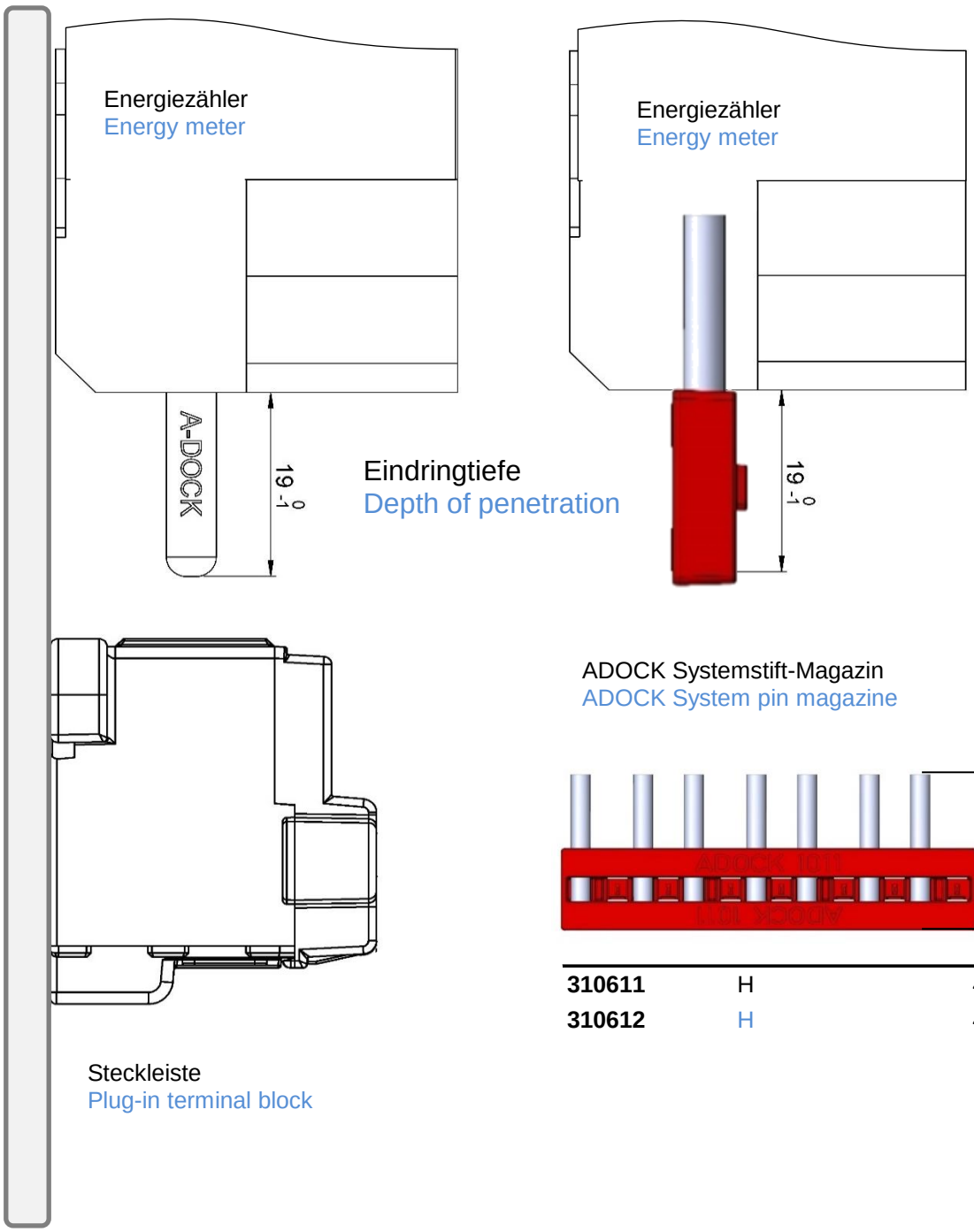
DATENBLATT / DATA SHEET

ZSL Stift Version: 04.10.2021

STIFTMONTAGE / MOUNTING OF PINS

ZSL63/W

STIFTLÄNGE / PIN LENGTH



310611	H	45	mm
310612	H	49	mm

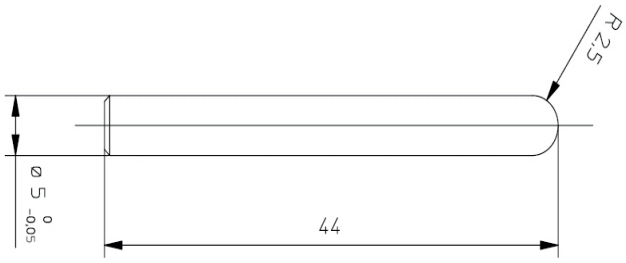
Datenblatt

Zubehör für Zählersteckleisten

Mat. Nr. 0061091 F8020/03 KONTAKTSTIFT-SET(3Stk) f. F802x
Mat. Nr. 0057312 F8040/07 KONTAKTSTIFT-SET(7Stk) f. F804x

Beschreibung: Dm 5x44mm, Leiterstücke, welche die elektrische Verbindung zwischen Zähler und Steckleisten herstellen, Stift versilbert

Kontaktstift
Abmessungen



Alle Angaben in [mm]

Material: CuZn39Pb3

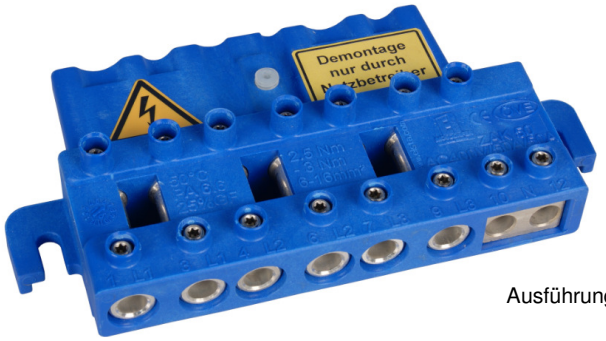
Oberflächenbehandlung: versilbert, Schichtdicke 6µ

Norm: ÖVE R21

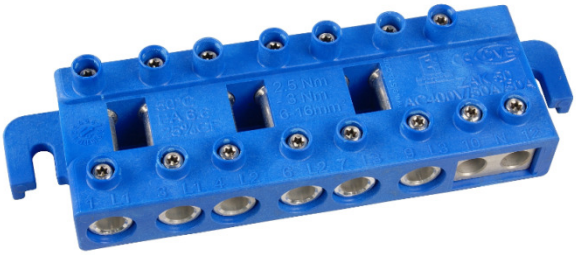
Alle Angaben sind Näherungswerte und beziehen sich auf genormte Prüfkörper unter Laborbedingungen; Änderungen vorbehalten. Informationen in diesem Datenblatt wurden nach bestem Wissen und Gewissen zusammengestellt. Dietzel GmbH übernimmt keinerlei Haftung für Schäden, die im Vertrauen hierauf entstehen.

ZÄHLERANSCHLUSSKLEMME 50A DREHSTROM

zur Verwendung mit Systemzählerstiften ELSTA Mosdorfer oder Standardzählerstiften



Ausführung ZK50N



Ausführung ZK50W

Beschreibung

Zähleranschlussklemme mit oder ohne fixe Zählerstifte
zur Montage auf allen gängigen Zählerplatten, Schraubanschluss.
Anschlussseitig einfach geschraubt (Verkürzung der Montagezeit),
zählerseitig mit fixen Zählerstiften (ZK50N) oder einfach geschraubt (ZK50W).
Bei der Ausführung mit fixen Zählerstiften sind die Stifte im Auslieferungszustand mit einer Berührungsschutzabdeckung abgedeckt, die mit einer Kunststoff-Torx-Schraube fixiert ist.

Hersteller

ELSTA Mosdorfer GmbH,
Bahnstraße 29, A-8430 Kaindorf / Sulm

Type

ZAK50 (ZAKD)

Art. Nr.

ZK50N	Zähleranschlussklemme 50A Drehstrom mit fixen Zählerstiften und Stiftabdeckung
ZK50W	Zähleranschlussklemme 50A Drehstrom

Normbezeichnung

ZAK 50 AC400V/50A/50A

Prüfströme

Normalbetriebsprüfung: 50A bis Beharrung; Überlastprüfung: 80A, 1 Stunde

Materialien

- Hülsen	Messing CW614N, verzinnt (Schichtdicke nominal 5µm)
- Kunststoffteile	Polyamid 6.6, glasfaserverstärkt
- Gewindestifte	A2-21H

REACH / RoHS

RoHS-konform
enthält keine Substanzen lt. Anhang XIV oder XVII nach REACH-VO (EG) Nr. 1907/2006

Schraubantrieb

Torx10

Prüfnorm

ÖVE-Richtlinie R21

Zertifikat

ÖVE 80-079

Zubehör

UB50	Kurzschlussbügel als Überbrückungsvorrichtung
SZS50	ELSTA Systemzählerstifte (siehe eigenes Datenblatt)

geeignete Überbrückungsvorrichtung Kurzschlussbügel UB50 oder z.B. Geiger KSB

34267 Zählerplatte ELSTA ZP-E (siehe eigenes Datenblatt)

108054 Drehmoment Schraubendreher DM-Set 1:
1000V Slim-Bits

ELSTA DM-Schrauben-dreherset

Maße und Gewichte		
Außenabmaße	**Ausführung mit fixen Zählerstiften**	**Ausführung ohne Stifte**
Länge	145mm	145mm
Höhe	72mm	42mm
Tiefe	33,5mm	31mm
Gewicht	340g	245g

Technische Daten	
Anzahl der Pole	4-polig (3P+N)
Maximaler zulässiger Nennstrom der Überstromschutzeinrichtung	50 A
Bemessungsspannung	AC 400 V
Bemessungsquerschnitte für starre und flexible Kupferleiter - eindrähtig - mehrdrähtig - feindrähtig (Nicht in jedem Netz zulässig!) - feindrähtig mit Aderendhülsen *	6 - 16 mm²
Anzahl der Neutralleiteranschlüsse	zwei
Schutzart	IP20C
Abgegebene Verlustleistung (bei 50 A) je Pol / bei dreiphasiger symmetrischer Belastung	0,21 W / 1,3 W
Umgebungstemperaturbereich im Betrieb	-25 bis +50 °C
Anzugsdrehmoment für die Leiter - mindestens - maximal	2,5 Nm 3,0 Nm
Anzugsdrehmoment zur Befestigung der Zähleranschlussklemme auf der Zählerplatte (Type ELSTA) - mindestens - maximal	1,0 Nm 1,5 Nm
Bemessungsisolationsspannung	630 V
Verschmutzungsgrad	2
Bemessungsstoßspannungsfestigkeit	4 kV
verwendbare Zählerstifte	Standardzählerstifte oder ELSTA Systemzählerstifte

* Wir empfehlen die Verwendung von isolierten Aderendhülsen Länge 15-18mm, z.B. Weitkowitz 51376 od. 51368

KJ10AT

Zählersteckklemme Wechselstrom 50A

Technische Merkmale

Elektrischer Strom	
Nennstrom	50 A

Leistung	
Gesamtverlustleistung unter Nennstrom	1,05 W

Architektur	
Polart	2P

Abmessungen	
Höhe	40 mm
Breite	90 mm
Tiefe	32 mm

Anschluss	
Anschlussquerschnitt Schraubklemme	25 mm²
Leiterquerschnitt	25 - 25 mm²
Anschlussquerschnitt flexibler Leiter mit Aderendhülse	4 - 16 mm²
Anschlussquerschnitt flexibler Leiter ohne Aderendhülse	4 - 25 mm²
Tarifanschluss	Nein

Werkstoff	
Transparent	Nein

Funktionen	
Geeignet für flexible Aderkabel	Ja

Konnektivität	
Anschlussart	Schraubanschluss

KJ30ATT

Zählersteckklemme Drehstrom 50A

Technische Merkmale

Elektrischer Strom	
Nennstrom	50 A

Leistung	
Gesamtverlustleistung unter Nennstrom	3,15 W

Architektur	
Polart	4P

Abmessungen	
Höhe	42 mm
Breite	130 mm
Tiefe	32 mm

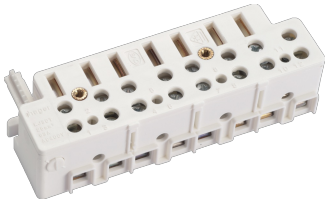
Anschluss	
Anschlussquerschnitt Schraubklemme	25 mm²
Leiterquerschnitt	25 - 25 mm²
Anschlussquerschnitt bei flexiblem Leiter	16 mm²
Anschlussquerschnitt bei starrem Leiter	25 mm²
Anschlussquerschnitt flexibler Leiter mit Aderendhülse	4 - 16 mm²
Anschlussquerschnitt flexibler Leiter ohne Aderendhülse	4 - 25 mm²
Tarifanschluss	Nein

Werkstoff	
Farbe	Reinweiß
RAL Nummer	9010
Transparent	Nein

Spannung	
Bemessungsbetriebsspannung Ue	400 - 400 V

Funktionen	
Geeignet für flexible Aderkabel	Ja

Konnektivität	
Anschlussart	Schraubanschluss



KJ30S

Zählersteckklemme, universZ, Drehstrom 63 A, sperrbar, mit TRE-Anschlussklemmen

Technische Merkmale

Elektrischer Strom

Nennstrom	63 A

Leistung

Gesamtverlustleistung unter Nennstrom	4,73 W

Architektur

Polart	4P

Abmessungen

Höhe	42 mm
Breite	130 mm
Tiefe	32 mm

Anschluss

Anschlussquerschnitt Schraubklemme	25 mm²
Leiterquerschnitt	25 - 25 mm²
Tarifanschluss	Nein

Werkstoff

Farbe	Lichtgrau
RAL Nummer	7035

Spannung

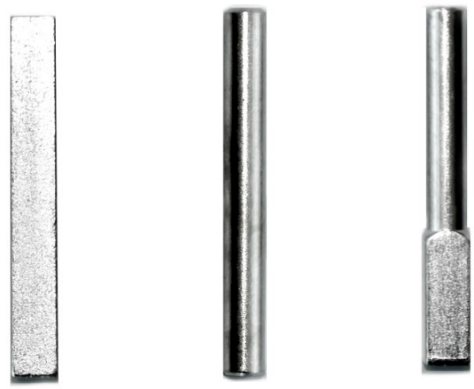
Bemessungsbetriebsspannung Ue	400 - 400 V

Konnektivität

Anschlussart	Schraubanschluss

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®



Zähleranschlussstifte

SL-...-5-...-...-Z

für die Baureihe der Zählersteckklemme SL-ZSK...,

Artikelnummer s. Tabelle
Datenblatt QM-PD-055 Index A
Erstellung 27.06.25 von SB
Prüfung SKZ
Freigabe SKZ

1. Zweck:

Die hochleistungsfähigen Seidl Zähleranschlussstifte für Zählersteckklemmen mit vierkantiger (V), runder (R), rund-vierkantiger (RV) und vierkantiger-runder (VR) Form ermöglichen die Anschlusskontaktierung mit Smartmetern / Energiezählern.

2. Funktion:

Die Zähleranschlussstifte ermöglichen die Verbindung vom Smartmeter / Energiezähler mit der Zählersteckklemme.

3. Sicherheit:

Die Zähleranschlussstifte, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter / Energiezählertausch.

Die Montage ist durch eine Elektrofachkraft oder eine hierfür unterwiesene Person durchzuführen!

4. Technische Daten:

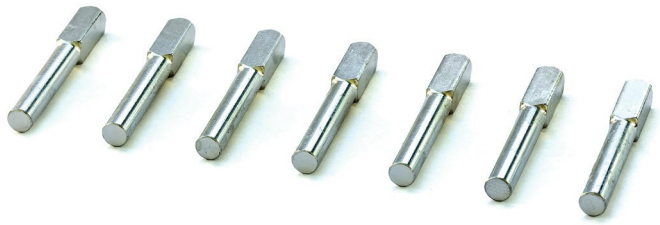
Artikel-Nummer	Bezeichnung	Variante	Stifttype / Abmessung Zähler	Stifttype / Abmessung Klemme	Stiftlänge	VPE-Gewicht	Anzahl
1030356	SL-5-5-37-RR-Z-Set-7	VDE 63A	rund / 5mm	rund / 5mm	37mm	14 g	7
1030344	SL-5-5-44-VV-Z-Set-7	S+ 80A	vierkant / 5mm	vierkant / 5mm	44mm	21 g	7
1001037	SL-5-5-44-R-Z-Set-7-C	VDE 63A	rund / 5mm	rund / 5mm	44mm	17 g	7
1030101	SL-5-5-44-R-Z-Set-7-D	ÖVE 50(80)A	rund / 5mm	rund / 5mm	44mm	17 g	7
1030196	SL-5-5-44-RV-Z-Set-7	S+ 80A	rund / 5mm	vierkant / 5mm	44mm	20 g	7
1030194	SL-6-5-44-RR-Z-Set-7	ÖVE 50(80)A	rund / 6mm	rund Halbkugel / 4,97mm	44mm	19 g	7
1001038	SL-6-5-44-VR-Z-Set-7-C	VDE 63A	vierkant / 6mm	rund / 5mm	44mm	23 g	7
1030102	SL-6-5-44-VR-Z-Set-7-D	ÖVE 50(80)A	vierkant / 6mm	rund / 5mm	44mm	23 g	7

SL-5-5-... SL-6-5-...	Zähleranschlussstifte SL für Zählersteckklemmen SL-ZSK...
Nennstrom:	bis 80A unter Berücksichtigung der Systemkomponenten des Zähleranschlusssystems, siehe auch Spalte Variante
Prüf- Überlaststrom:	80A / 1h (geprüft mit 1,6-fachem Nennstrom), für Variante ÖVE
Material:	AL^{EF} Aluminiumcompositewerkstoff, verzinnt
Leitfähigkeit:	>31mS/m
Betriebsspannung:	AC 400V, 50Hz
Anzugsdrehmoment Zählerstifte:	max. 5,35Nm

5. Zertifizierungen und Konformitäten:
OVE R21:2019; DIN VDE 0603-3-3:2020; Niederspannungsrichtlinie LVD Directive 2014/35/EU; RoHS III Directive 2015/863/EU

6. Besonderheiten und Montagehinweise:
Die Zähleranschlussstifte sind gleichwertig zu versilberten Standard-Zählerstiften gemäß OVE R21 (TGM-Gutachten VA EE 38624-1).

7. Kompatibilitätshinweis:
Die Zähleranschlussstifte, welche in der o.a. Tabelle angeführt sind, sind für die Baureihen der Zählersteckklemme SL-ZSK... vorgesehen. Durch die Gleichwertigkeit mit Standard-Zählerstiften gemäß OVE R21 ist der Einsatz in anderen zertifizierten Zähleranschlussklemmen möglich.



VDE REG F551

Die hochleistungsfähigen Zähleranschlussstifte SL für Smartmeter/Zähler mit **runder/eckiger Anschlusskontaktierung**. Der Zähleranschlussstift ermöglicht die Verbindung von Smartmeter/Zähler mit der SL-AKS/Z Zähleranschlussklemme. Die Stifte, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und spannungsunterbrechungsfreien Smartmeter-/Energiezählertausch. Die Montage ist durch eine Elektrofachkraft durchzuführen.

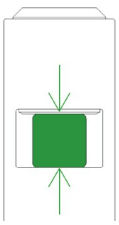
Technische Daten:

SL-6-6-45-RV-Z-Set-3 SL-6-6-45-RV-Z-Set-7 SL-6-6-45-RV-Z-Set-100	System-Standard-Zähleranschlussstift SL, Dauerstrom 100A, Überlaststrom 2h 128A
Nennstrom:	100A (abhängig von der Auslösecharakteristik der zugehörigen Überlastschutzeinrichtung) [a)]
Prüf- Überlaststrom:	128A / 2h (geprüft mit 1,6-fachem Nennstrom)
Betriebsspannung:	AC 400V, 50Hz
Anzugsmoment Zählerstifte:	5 Nm [b)]
Material:	Aluminiumcompositewerkstoff
Leitfähigkeit:	> 31 mS/m
Korrosionsbeständigkeit:	geprüft nach EN 60068 / EN 61439-3:2012 / EN 60998-1:2004
Höhe/ Breite/ Tiefe:	6 mm / 6 mm / 45 mm
VPE - Gewicht 3 Stück:	0,0105 kg
VPE - Gewicht 7 Stück:	0,0245 kg
VPE - Gewicht 100 Stück:	0,3500 kg
VPE - Gewicht 3.500 Stück:	12,244 kg

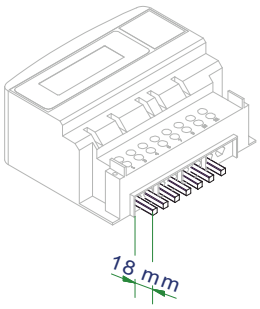
[a)] NH 80A Leistungsschalter bzw. Leistungsschutzschalter - max. Auslösestrom 128A
[b)] nur bei SL-AKS/Z - andere Klemmen nach Herstellerangaben

Besondere Merkmale:

Durch das einzigartige Design des Stiftes ist eine Flächenauflage anstatt einer herkömmlichen Linienauflage gegeben.



Flächenauflage



Bei der Montage der Stifte ist darauf zu achten, das sie 18,00 mm ± 0,5 mm hervorstehen.

Stifte dürfen je Seite des Vierkantes max. 1 mal verschraubt werden!

Kompatibilitätshinweis:

SL-ZAKD 80 (128)A-1N, SL-ZAKD (128)A-2N, SL-ZAKD 80 (128)A-1N + TRE, SL-ZAKD 80 (128)A-2N + TRE, ZIKD63A-x-x-, ZIKD100A-x-x-
SL-AKS/Z 80 (128)A-1N, SL-AKS/Z 80 (128)A-2N, SL-AKS/Z 80 (128)A-1N + TRE, SL-AKS/Z 80 (128)A-2N + TRE,
SL-AKS/Z 63 (100)A-1N, SL-AKS/Z 63 (100)A-2N, SL-AKS/Z 63 (100)A-1N + TRE, SL-AKS/Z 63 (100)A-2N + TRE,
SL-ZAKW 63 (100)A-2N, SL-ZAKW 63 (100)A-2N + TRE, SL-AKS/Z 63 (100)A-EVN

Zertifizierungen und Konformitäten:

ÖVE R21:2015; Niederspannungsrichtlinie LVD Directive 2014/35/EU
RoHS III Directive 2015/863/EU

Stand 01-2022 - Technische Änderungen vorbehalten - Symbolbilder

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®

Zähleranschlussklemme

SL-AKS/Z 63(100)A 1N-EVN

Artikelnummer 1030142
Datenblatt QM-PD-006 Index B
Erstellt 29.02.24 von PM
Prüfung SZ
Freigabe AH

ÖVE-Zertifikatsnummer:
85145-003

AlEF®

1. Zweck:
Die Klemme mit Inserts aus der Speziallegierung AlEF für den Anschluss von Smartmeter/Energiezähler ermöglicht den spannungsunterbrechungsfreien Gerätetausch.

2. Funktion:
Die Funktion der Anschlussklemme erfüllt die OVE R21:2019 und orientiert sich an den Sicherheitszielen der DIN VDE 0603-3-3. „Open Contact“ ermöglicht den Einsatz verschiedener Geräte unterschiedlicher Smartmeter/Zählerhersteller.

3. Sicherheit:
Die Klemme, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter-Energiezählertausch.
Die Montage ist durch eine Elektrofachkraft durchzuführen!

4. Technische Daten:

SL-AKS/Z 63(100)A 1N EVN o. TRE	Anschlussklemme Smartmeter / Zähler, Dauerstrom 63A Überlaststrom 1h 100,8A, Ausführung 1xN ohne Tarifanschluss inkl. fixierter (nicht wieder-anschließbarer) Stifte SL-6-6-45-RV-Z mit ADK
Nennstrom:	63A [a] (maximal zulässiger Nennstrom der zugehörigen Überlastschutzeinrichtung)
Prüf- Überlaststrom:	100,8A / 1h (geprüft mit 1,6-fachem Nennstrom)
Betriebsspannung:	400V AC, 50Hz
Steckzyklen Zähleranschlussklemme:	1.250
Steckzyklen Überbrückungsvorrichtung:	5.000
Leitermaterial / Leiterart:	Cu / 2,5 – 35 mm², starr, ein- und mehrdrahtig / flexible Leiter mit verpresster Aderendhülse [b] / mehrdrahtige und Sektorenleiter erfordern eine gesonderte Leiteranschlussvorbereitung mittels Presshülse [c]
Anschlüsse zählerseitig:	Fixierte (nicht wiederanschließbare) Stifte SL-6-6-45-RV-Z, rund/vierkant, Stiftabstand 13/16mm
Einstecktiefe Leiter:	18 mm
ADK:	Abdeckkappe vormontiert für Berührungsschutz
Anzugsmoment Leiter:	5,5 Nm (1 Klemmschraube je Zu- und Abgangsklemme) 6 Nm bei mehrdrahtigen Leitern
Anzugsmoment Zählerstifte:	Zählerspezifisch bis max. 5 Nm
Antriebswerkzeug Klemmschrauben:	Torx 25 - Zu- und Abgangsklemmen (Phasen + N)

[a] 63A / 100,8A mit fixierten (nicht wiederanschließbaren) System-Zählerstift
[b] DIN 46228-1, DIN 46228-4 oder gleichwertig
[c] Mehrdrahtige- und Sektorenleiter müssen mit Presshülsen sowie geeigneten Presswerkzeugen vorbereitet werden, um eine dauerhafte Kontaktierung zu gewährleisten.

Zählerstiftabstände:	gemäß DIN 43857, fixierte Zählerstifte, bei Bestellung ist eine Anpassung der Abstände möglich [d]
Verlustleistung bei 20 °C Raumtemperatur:	63A: 1,25W [e]
Umgebungstemperatur:	-30°C bis +65°C [f]
IP-Schutzart:	IP2XC (nach Montage aller Systemkomponenten inkl. Abdeckhaube)
Höhe/ Breite/ Tiefe:	74 mm / 135 mm / 35 mm
Gewicht:	1 Stück - 0,31 kg
VPE - Gewicht:	36 Stück - 11,16 kg
Kunststoff - Material:	PA 66 V0, halogenfrei

5. Zertifizierungen und Konformitäten:
OVE R21:2019; Niederspannungsrichtlinie LVD Directive 2014/35/EU
RoHS III Directive 2015/863/EU; IEC/EN 60998-2-1; IEC 61545

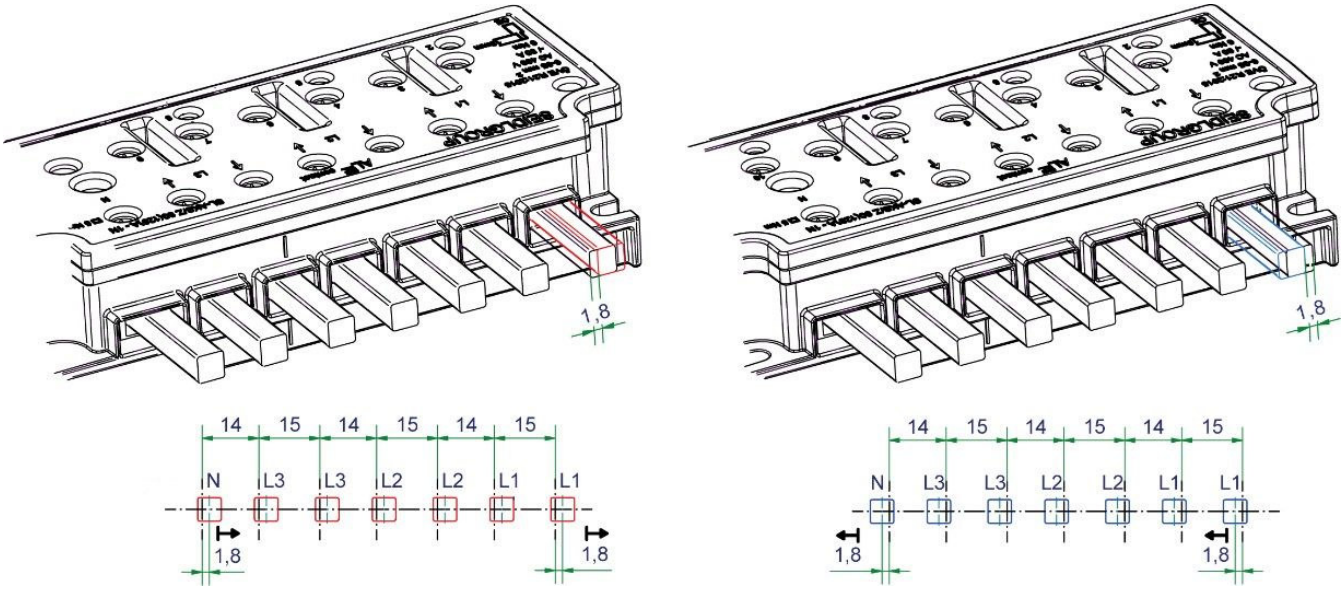
6. Verlustleistung:

Zu- und Abgang aller Phasenanschlüsse, durchschnittliche Verlustleistungsermittlung			
Systemstifte SL-....	Mittelwert Angabe in Watt		
Belastungsstrom	20°C	40°C	65°C
20A	0,18	0,18	0,19
40A	0,60	0,61	0,64
63A	1,25	1,51	1,62

Flächenauflage vs. Linienauflage

Durch die quadratische Ausführung der Stifte ist in Kombination mit der Anschlussklemme SL-AKS/Z eine Flächenauflage anstatt der herkömmlichen Linienauflage gegeben.

7. Mögliche Zählerstiftabstände durch seitlichen Versatz (Open Contact):



Das einzigartige und zugleich innovative Merkmal ist der seitliche Versatz der Zähleranschlussstifte von bis zu 3,6 mm (1,8 mm je Seite). Dadurch können alle derzeit verwendeten Energiezähler und Smartmeter angeschlossen werden.

8. Kompatibilitäts- und Montagehinweise
Die Klemme darf ausschließlich mit dem zugelassenen Überbrückungswerkzeug SL-AKS-Z-UEW-01-X-X-X temporär überbrückt werden.
Bei Schraubenbefestigung auf einer Zählertafel / Zählerplatte muss in Bezug auf die Montageschrauben die Befestigungslaschenhöhe von 6 mm berücksichtigt werden (inkl. Ausnehmung für Überstand der Gleitmuttern gem. OVE E 8640). Die Schraubenlänge ist derart zu wählen, dass die Montageschraube ausreichend Gewindegänge in die Gleitmutter der Zählerplatte, gemäß Herstellerspezifikation, aufweist.

[d] Open Contact s. Skizze, Punkt 7
[e] nach TGM-Gutachten TGM-VA EE 36844, s. Tabelle, Punkt 6
[f] Auswahl der entsprechenden Aderisolation (Temperaturbeständigkeit) für die zugeführten Leiter ist erforderlich

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®

ÖVE-Zertifikatsnummer:
85145-003

Zähleranschlussklemme

SL-AKS/Z 63(100)A 2N-EVN

Artikelnummer 1008229
Datenblatt QM-PD-007 Index B
Erstellt 29.02.24 von PM
Prüfung SZ
Freigabe AH

AlEF®

1. Zweck:
Die Klemme mit Inserts aus der Speziallegierung AlEF für den Anschluss von Smartmeter/Energiezähler ermöglicht den spannungsunterbrechungsfreien Gerätetausch.

2. Funktion:
Die Funktion der Anschlussklemme erfüllt die OVE R21:2019 und orientiert sich an den Sicherheitszielen der DIN VDE 0603-3-3. „Open Contact“ ermöglicht den Einsatz verschiedener Geräte unterschiedlicher Smartmeter/Zählerhersteller.

3. Sicherheit:
Die Klemme, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter-Energiezählertausch.
Die Montage ist durch eine Elektrofachkraft durchzuführen!

4. Technische Daten:

SL-AKS/Z 63(100)A 2N EVN o. TRE	Anschlussklemme Smartmeter / Zähler, Dauerstrom 63A Überlaststrom 1h 100,8A, Ausführung 2xN ohne Tarifanschluss inkl. fixierter (nicht wieder-anschließbarer) Stifte SL-6-6-45-RV-Z mit ADK
Nennstrom:	63A [a] (maximal zulässiger Nennstrom der zugehörigen Überlastschutzeinrichtung)
Prüf- Überlaststrom:	100,8A / 1h (geprüft mit 1,6-fachem Nennstrom)
Betriebsspannung:	400V AC, 50Hz
Steckzyklen Zähleranschlussklemme:	1.250
Steckzyklen Überbrückungsvorrichtung:	5.000
Leitermaterial / Leiterart:	Cu / 2,5 – 35 mm², starr, ein- und mehrdrahtig / flexible Leiter mit verpresster Aderendhülse [b] / mehrdrahtige und Sektorenleiter erfordern eine gesonderte Leiteranschlussvorbereitung mittels Presshülse [c]
Anschlüsse zählerseitig:	Fixierte (nicht wiederanschließbare) Stifte SL-6-6-45-RV-Z, rund/vierkant, Stiftabstand 13/16mm
Einstecktiefe Leiter:	18 mm
ADK:	Abdeckkappe vormontiert für Berührungsschutz
Anzugsmoment Leiter:	5,5 Nm (1 Klemmschraube je Zu- und Abgangsklemme) 6 Nm bei mehrdrahtigen Leitern
Anzugsmoment Zählerstifte:	Zählerspezifisch bis max. 5 Nm
Antriebswerkzeug Klemmschrauben:	Torx 25 - Zu- und Abgangsklemmen (Phasen + N)

[a] 63A / 100,8A mit fixierten (nicht wiederanschließbaren) System-Zählerstift
[b] DIN 46228-1, DIN 46228-4 oder gleichwertig
[c] Mehrdrahtige- und Sektorenleiter müssen mit Presshülsen sowie geeigneten Presswerkzeugen vorbereitet werden, um eine dauerhafte Kontaktierung zu gewährleisten.

Zählerstiftabstände:	gemäß DIN 43857, fixierte Zählerstifte, bei Bestellung ist eine Anpassung der Abstände möglich [d]
Verlustleistung bei 20 °C Raumtemperatur:	63A: 1,25W [e]
Umgebungstemperatur:	-30°C bis +65°C [f]
IP-Schutzart:	IP2XC (nach Montage aller Systemkomponenten inkl. Abdeckhaube)
Höhe/ Breite/ Tiefe:	74 mm / 135 mm / 35 mm
Gewicht:	1 Stück - 0,31 kg
VPE - Gewicht:	36 Stück - 11,16 kg
Kunststoff - Material:	PA 66 V0, halogenfrei

5. Zertifizierungen und Konformitäten:
OVE R21:2019; Niederspannungsrichtlinie LVD Directive 2014/35/EU
RoHS III Directive 2015/863/EU; IEC/EN 60998-2-1; IEC 61545

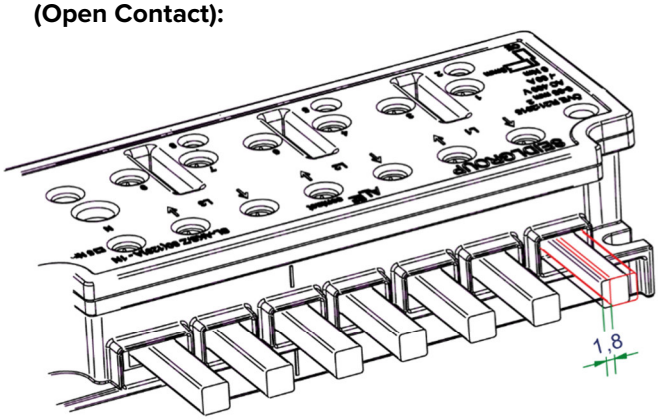
6. Verlustleistung:

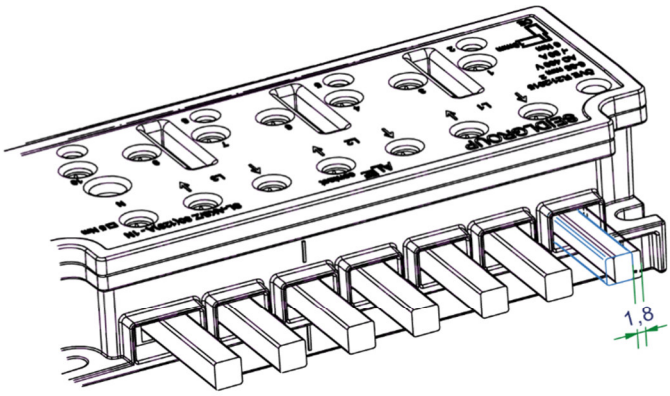
Zu- und Abgang aller Phasenanschlüsse, durchschnittliche Verlustleistungsermittlung			
Systemstifte SL-....	Mittelwert Angabe in Watt		
Belastungsstrom	20°C	40°C	65°C
20A	0,18	0,18	0,19
40A	0,60	0,61	0,64
63A	1,25	1,51	1,62

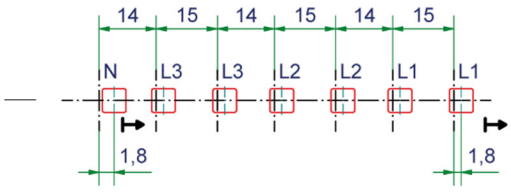
Flächenauflage vs. Linienauflage

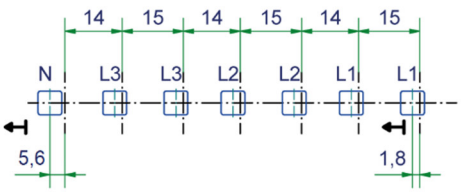
Durch die quadratische Ausführung der Stifte ist in Kombination mit der Anschlussklemme SL-AKS/Z eine Flächenauflage anstatt der herkömmlichen Linienauflage gegeben.

7. Mögliche Zählerstiftabstände durch seitlichen Versatz (Open Contact):









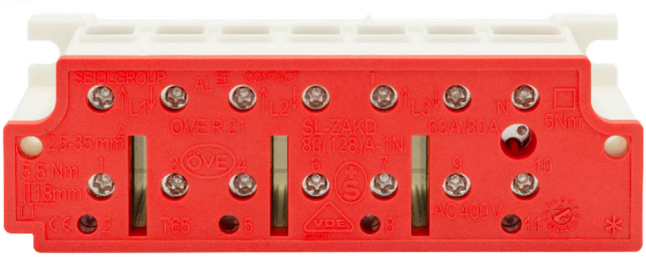
Das einzigartige und zugleich innovative Merkmal ist der seitliche Versatz der Zähleranschlussstifte von bis zu 3,6 mm (1,8 mm je Seite – N: 1,8 mm und 5,6 mm). Dadurch können alle derzeit verwendeten Energiezähler und Smartmeter angeschlossen werden.

8. Kompatibilitäts- und Montagehinweise
Die Klemme darf ausschließlich mit dem zugelassenen Überbrückungswerkzeug SL-AKS-Z-UEW-01-X-X-X temporär überbrückt werden.
Bei Schraubenbefestigung auf einer Zählertafel / Zählerplatte muss in Bezug auf die Montageschrauben die Befestigungslaschenhöhe von 6 mm berücksichtigt werden (inkl. Ausnehmung für Überstand der Gleitmuttern gem. OVE E 8640). Die Schraubenlänge ist derart zu wählen, dass die Montageschraube ausreichend Gewindegänge in die Gleitmutter der Zählerplatte, gemäß Herstellerspezifikation, aufweist.

[d] Open Contact s. Skizze, Punkt 7
[e] nach TGM-Gutachten TGM-VA EE 36844, s. Tabelle, Punkt 6
[f] Auswahl der entsprechenden Aderisolation (Temperaturbeständigkeit) für die zugeführten Leiter ist erforderlich

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®



Zähleranschlussklemme

SL-ZAKD 80(128)A-1N o. TRE

Artikelnummer 1006300
Datenblatt QM-PD-010 Index C
Erstellung 26.11.24, PM
Prüfung SZ
Freigabe SZ

ÖVE Zertifikat 85145-002

Bewilligung 23.0184

VDE REG F551 Ausweis 40048909

ÖVE IEC RoHS konform CE ISO 9001 EN

AlEF®

1. Zweck:
Die Klemme mit Inserts aus der Speziallegierung AlEF für den Anschluss von Smartmetern / Energiezählern ermöglicht den spannungsunterbrechungsfreien Gerätetausch.

2. Funktion:
Die Funktion der Anschlussklemme erfüllt die OVE R21:2019 und orientiert sich an den Sicherheitszielen der DIN VDE 0603-3-3. „Open Contact“ ermöglicht den Einsatz verschiedener Geräte unterschiedlicher Smartmeter/Zählerhersteller.

3. Sicherheit:
Die Klemme, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter-Energiezählertausch. **Die Montage ist durch eine Elektrofachkraft durchzuführen!**

4. Technische Daten:

SL-ZAKD 80(128)A-1N ohne TRE	Anschlussklemme Smartmeter / Zähler, Dauerstrom 80A Überlaststrom 2h 128A, Ausführung 1xN ohne Tarifanschluss
Nennstrom:	80A [a] (maximal zulässiger Nennstrom der zugehörigen Überlastschutzeinrichtung)
Prüf- Überlaststrom:	128A / 2h (geprüft mit 1,6-fachem Nennstrom)
Betriebsspannung:	400V AC, 50Hz
Steckzyklen Zähleranschlussklemme:	1.250
Steckzyklen Überbrückungsvorrichtung:	5.000
Leitermaterial / Leiterart:	Cu / 2,5 – 35 mm², starr, ein- und mehrdrähtig / flexible Leiter mit verpresster Aderendhülse [b] / mehrdrähtige und Sektorleiter erfordern eine gesonderte Leiteranschlussvorbereitung mittels Presshülse [c]
Anschlüsse zählerseitig:	Systemstifte SL-Stifte Vierkant und Rund, geeignet für Standard-Zählerstifte 63A und System-Zählerstifte 80A
Einstecktiefe Leiter:	18 mm
Anzugsdrehmoment Leiter:	5,5 Nm (1 Klemmschraube je Zu- und Abgangsklemme)
Anzugsdrehmoment Zählerstifte:	5 Nm (1 Klemmschraube je Zählerstiftanschluss)
Anzugsdrehmoment Befestigungsschrauben ADH:	max. 0,3 Nm
Antriebswerkzeug Klemmschrauben:	Torx 25 - Zu- und Abgangsklemmen (Phasen + N)

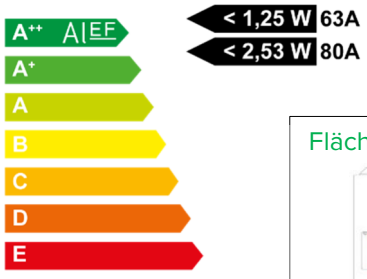
[a] 80A / 128A mit System-Zählerstift. 63A / 100A mit Standard-Zählerstift nach OVE Richtlinie R21:2019-02-01
[b] DIN 46228-1, DIN 46228-4 oder gleichwertig
[c] Mehrdrähtige- und Sektorleiter müssen mit Presshülsen sowie geeigneten Presswerkzeugen vorbereitet werden, um eine dauerhafte Kontaktierung zu gewährleisten. (s. auch unsere Technischen Hinweise QM-TH-001 Leiteranschluss SL-ZAKD_ZIKD_ZAKW-Baureihe)

Zählerstiftabstände:	gemäß DIN 43857 [d]
Verlustleistung bei 20 °C Raumtemperatur:	80A: 2,53W / 63A: 1,25W [e]
Umgebungstemperatur:	-30°C bis +65°C [f]
IP-Schutzart:	IP2XC (nach Montage aller Systemkomponenten inkl. Abdeckhaube)
Höhe/ Breite/ Tiefe:	44 mm / 135 mm / 35 mm
Gewicht:	1 Stück - 0,25 kg
VPE - Gewicht:	64 Stück - 16,00 kg
Kunststoff - Material:	PA 66 V0, halogenfrei

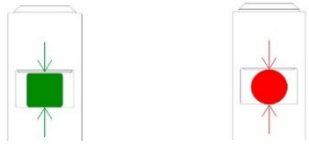
5. Zertifizierungen und Konformitäten:
OVE R21:2019; Niederspannungsrichtlinie LVD Directive 2014/35/EU
RoHS III Directive 2015/863/EU; IEC/EN 60998-2-1; IEC 61545

6. Verlustleistung:

Zu- und Abgang aller Phasenanschlüsse, durchschnittliche Verlustleistungsermittlung			
Systemstifte SL-....	Mittelwert Angabe in Watt		
Belastungsstrom	20°C	40°C	65°C
20A	0,18	0,18	0,19
40A	0,60	0,61	0,64
63A	1,25	1,51	1,62
80A	2,53	2,60	2,68

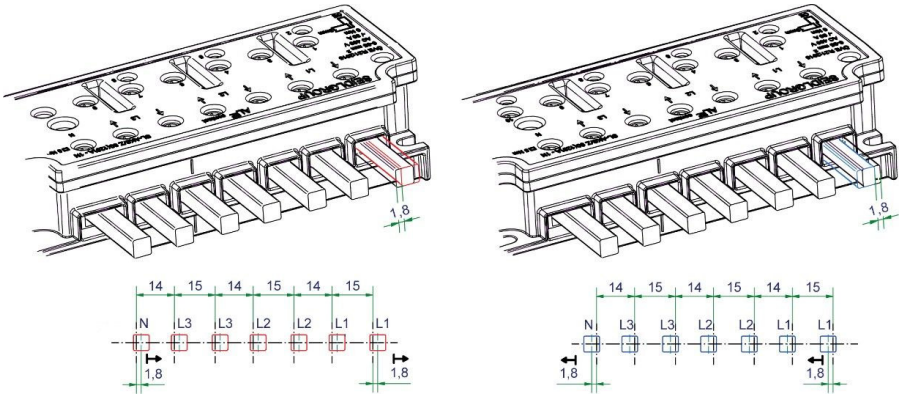


Flächenauflage vs. Linienauflage



Durch die quadratische Ausführung des Stiftes ist eine Flächenauflage anstatt einer herkömmlichen Linienauflage in Kombination mit der Anschlussklemme SL-ZAKD gegeben.

7. Mögliche Zählerstiftabstände durch seitlichen Versatz (Open Contact):



Einzigartig und innovativ ist der seitliche Versatz der Zähleranschlussstifte von bis zu 3,6 mm (1,8 mm je Seite). Dadurch können alle derzeit verwendeten Energiezähler und Smartmeter mit der Anschlussklemme SL-ZAKD angeschlossen werden.

8. Kompatibilitäts- und Montagehinweise:
Die Klemme darf ausschließlich mit dem zugelassenen Überbrückungswerkzeug SL-AKS/Z-UEW-01-X-X-X temporär und SL-AKS/Z-PUE-XX dauerhaft überbrückt werden.
Für den Anschluss von Smartmetern / Energiezählern sind ausschließlich folgende Stifte zugelassen:
- 80A / 128A - Anschluss mit System-Zählerstift der Reihe SL-6-6-XXX (alle nach OVE R21:2019)
- 63A / 100A - Anschluss mit Standard-Zählerstift nach OVE R21:2019

Bei Schraubenbefestigung auf einer Zählertafel / Zählerplatte muss in Bezug auf die Montageschrauben die Befestigungslaschenhöhe von 6 mm berücksichtigt werden (inkl. Ausnehmung für Überstand der Gleitmuttern gem. OVE E 8640). Die Schraubenlänge ist derart zu wählen, dass die Montageschraube ausreichend Gewindegänge in die Gleitmutter der Zählerplatte, gemäß Herstellerspezifikation, aufweist.

[d] Open Contact s. Skizze, Punkt 7
[e] nach TGM-Gutachten TGM-VA EE 36844, s. Tabelle, Punkt 6
[f] Auswahl der entsprechenden Aderisolation (Temperaturbeständigkeit) für die zugeführten Leiter ist erforderlich

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®

Zähleranschlussklemme

SL-ZAKD 80(128)A-2N m. TRE

Artikelnummer 1006303
Datenblatt QM-PD-013 Index A
Erstellung 26.11.24, PM
Prüfung SZ
Freigabe SZ

ÖVE Zertifikat 85145-002

Bewilligung 23.0184

VDE REG F551 Ausweis 40048909

ÖVE IEC RoHS konform CE ISO 9001 EN

AlEF®

1. Zweck:
Die Klemme mit Inserts aus der Speziallegierung AlEF für den Anschluss von Smartmetern / Energiezählern ermöglicht den spannungsunterbrechungsfreien Gerätetausch.

2. Funktion:
Die Funktion der Anschlussklemme erfüllt die OVE R21:2019 und orientiert sich an den Sicherheitszielen der DIN VDE 0603-3-3. „Open Contact“ ermöglicht den Einsatz verschiedener Geräte unterschiedlicher Smartmeter/Zählerhersteller.

3. Sicherheit:
Die Klemme, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter-Energiezählertausch. **Die Montage ist durch eine Elektrofachkraft durchzuführen!**

4. Technische Daten:

SL-ZAKD 80(128)A-2N mit TRE	Anschlussklemme Smartmeter / Zähler, Dauerstrom 80A Überlaststrom 2h 128A, Ausführung 2xN mit Tarifanschluss
Nennstrom:	80A [a] (maximal zulässiger Nennstrom der zugehörigen Überlastschutzeinrichtung)
Prüf- Überlaststrom:	128A / 2h (geprüft mit 1,6-fachem Nennstrom)
Betriebsspannung:	400V AC, 50Hz
Steckzyklen Zähleranschlussklemme:	1.250
Steckzyklen Überbrückungsvorrichtung:	5.000
Leitermaterial / Leiterart:	Cu / 2,5 – 35 mm², starr, ein- und mehrdrähtig / flexible Leiter mit verpresster Aderendhülse [b] / mehrdrähtige und Sektorleiter erfordern eine gesonderte Leiteranschlussvorbereitung mittels Presshülse [c]
Anschlüsse zählerseitig:	Systemstifte SL-Stifte Vierkant und Rund, geeignet für Standard-Zählerstifte 63A und System-Zählerstifte 80A
Einstecktiefe Leiter:	18 mm
Anzugsdrehmoment Leiter:	5,5 Nm (1 Klemmschraube je Zu- und Abgangsklemme)
Anzugsdrehmoment Zählerstifte:	5 Nm (1 Klemmschraube je Zählerstiftanschluss)
Anzugsdrehmoment Befestigungsschrauben ADH:	max. 0,3 Nm
Antriebswerkzeug Klemmschrauben:	Torx 25 - Zu- und Abgangsklemmen (Phasen + N) Torx 10 - Tarifanschluss

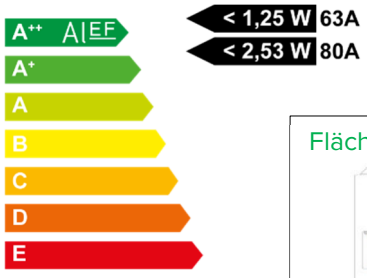
[a] 80A / 128A mit System-Zählerstift. 63A / 100A mit Standard-Zählerstift nach OVE Richtlinie R21:2019-02-01
[b] DIN 46228-1, DIN 46228-4 oder gleichwertig
[c] Mehrdrähtige- und Sektorleiter müssen mit Presshülsen sowie geeigneten Presswerkzeugen vorbereitet werden, um eine dauerhafte Kontaktierung zu gewährleisten. (s. auch unsere Technischen Hinweise QM-TH-001 Leiteranschluss SL-ZAKD_ZIKD_ZAKW-Baureihe)

Anschlussquerschnitt Tarifanschluss:	1,5 – 2,5 mm² starr-eindrähtig / flexible Leiter mit Aderendhülse [d]
Anzugsdrehmoment Tarifanschluss:	0,5 Nm
Zählerstiftabstände:	gemäß DIN 43857 [e]
Verlustleistung bei 20 °C Raumtemperatur:	80A: 2,53W / 63A: 1,25W [f]
Umgebungstemperatur:	-30°C bis +65°C [g]
IP-Schutzart:	IP2XC (nach Montage aller Systemkomponenten inkl. Abdeckhaube)
Höhe/ Breite/ Tiefe:	44 mm / 135 mm / 35 mm
Gewicht:	1 Stück - 0,26 kg
VPE - Gewicht:	64 Stück - 16,64 kg
Kunststoff - Material:	PA 66 V0, halogenfrei

5. Zertifizierungen und Konformitäten:
OVE R21:2019; Niederspannungsrichtlinie LVD Directive 2014/35/EU
RoHS III Directive 2015/863/EU; IEC/EN 60998-2-1; IEC 61545

6. Verlustleistung:

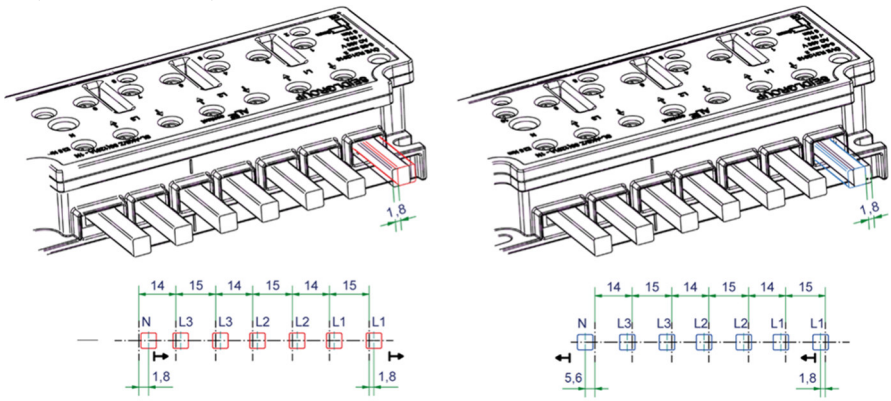
Zu- und Abgang aller Phasenanschlüsse, durchschnittliche Verlustleistungsermittlung			
Systemstifte SL-....	Mittelwert Angabe in Watt		
Belastungsstrom	20°C	40°C	65°C
20A	0,18	0,18	0,19
40A	0,60	0,61	0,64
63A	1,25	1,51	1,62
80A	2,53	2,60	2,68



Flächenauflage vs. Linienauflage

Durch die quadratische Ausführung des Stiftes ist eine Flächenauflage anstatt einer herkömmlichen Linienauflage in Kombination mit der Anschlussklemme SL-ZAKD gegeben.

7. Mögliche Zählerstiftabstände durch seitlichen Versatz (Open Contact):



Einzigartig und innovativ ist der seitliche Versatz der Zähleranschlussstifte von bis zu 3,6 mm (1,8 mm je Seite – N: 1,8 mm und 5,6 mm). Dadurch können alle derzeit verwendeten Energiezähler und Smartmeter mit der Anschlussklemme SL-ZAKD angeschlossen werden.

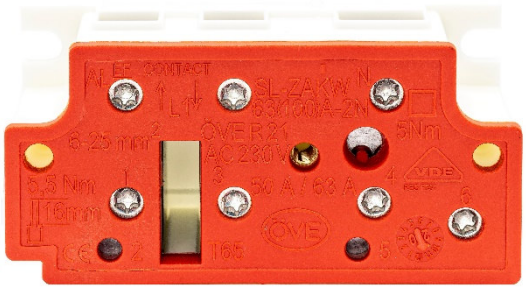
8. Kompatibilitäts- und Montagehinweise:
Die Klemme darf ausschließlich mit dem zugelassenen Überbrückungswerkzeug SL-AKS/Z-UEW-01-X-X-X temporär und SL-AKS/Z-PUE-XX dauerhaft überbrückt werden.
Für den Anschluss von Smartmetern / Energiezählern sind ausschließlich folgende Stifte zugelassen:
- 80A / 128A - Anschluss mit System-Zählerstift der Reihe SL-6-6-XXX (alle nach OVE R21:2019)
- 63A / 100A - Anschluss mit Standard-Zählerstift nach OVE R21:2019

Bei Schraubenbefestigung auf einer Zählertafel / Zählerplatte muss in Bezug auf die Montageschrauben die Befestigungslaschenhöhe von 6 mm berücksichtigt werden (inkl. Ausnehmung für Überstand der Gleitmuttern gem. OVE E 8640). Die Schraubenlänge ist derart zu wählen, dass die Montageschraube ausreichend Gewindegänge in die Gleitmutter der Zählerplatte, gemäß Herstellerspezifikation, aufweist.

[d] DIN 46228-1, DIN 46228-4 oder gleichwertig
[e] Open Contact s. Skizze, Punkt 7
[f] nach TGM-Gutachten TGM-VA EE 36844, s. Tabelle, Punkt 6
[g] Auswahl der entsprechenden Aderisolation (Temperaturbeständigkeit) für die zugeführten Leiter ist erforderlich

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®



Zähleranschlussklemme

SL-ZAKW 63(100)A-2N o. TRE

Artikelnummer 1011001
Datenblatt QM-PD-026 Index A
Erstellt 29.10.24 von PM
Prüfung SZ
Freigabe SZ

ÖVE-Zertifikatsnummer: 85145-004

VDE REG F551

VDE-Ausweisnummer: 40048909

ÖVE IEC RoHS konform CE ISO 9001 EN

AlEF®

1. Zweck:
Die Klemme mit Inserts aus der Speziallegierung AlEF für den Anschluss von Smartmeter/Energiezähler ermöglicht den spannungsunterbrechungsfreien Gerätetausch.

2. Funktion:
Die Funktion der Anschlussklemme erfüllt die OVE R21:2019 und orientiert sich an den Sicherheitszielen der DIN VDE 0603-3-3. „Open Contact“ ermöglicht den Einsatz verschiedener Geräte unterschiedlicher Smartmeter/Zählerhersteller.

3. Sicherheit:
Die Klemme, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter-Energiezählertausch. **Die Montage ist durch eine Elektrofachkraft durchzuführen!**

4. Technische Daten:

SL-ZAKW 63(100)A-2N ohne TRE	Anschlussklemme Wechselstrom Smartmeter / Zähler, Dauerstrom 63A, Überlaststrom 1h 100A, Ausführung 2xN ohne Tarifanschluss
Nennstrom:	63A [a] (maximal zulässiger Nennstrom der zugehörigen Überlastschutzeinrichtung)
Prüf- Überlaststrom:	100A / 1h (geprüft mit 1,6-fachem Nennstrom)
Betriebsspannung:	230V AC, 50Hz
Steckzyklen Zähleranschlussklemme:	1.250
Steckzyklen Überbrückungsvorrichtung:	4.000
Leitermaterial / Leiterart:	Cu / 6 – 25 mm², starr, ein- und mehrdrähtig / flexible Leiter mit verpresster Aderendhülse [b] / mehrdrähtige und Sektorleiter erfordern eine gesonderte Leiteranschlussvorbereitung mittels Presshülse [c]
Anschlüsse zählerseitig:	Systemstifte SL-Stifte Vierkant und Rund, geeignet für Standard-Zählerstifte 50A und System-Zählerstifte 63A
Einstecktiefe Leiter:	18 mm
Anzugsmoment Leiter:	5,5 Nm (1 Klemmschraube je Zu- und Abgangsklemme)
Anzugsmoment Zählerstifte:	5 Nm (1 Klemmschraube je Zählerstiftanschluss)
Antriebswerkzeug Klemmschrauben:	Torx 25 - Zu- und Abgangsklemmen (Phasen + N)

[a] 63A / 100A mit System-Zählerstift. 50A / 80A mit Standard-Zählerstift nach OVE Richtlinie R21:2019-02-01
[b] DIN 46228-1, DIN 46228-4 oder gleichwertig
[c] Mehrdrähtige- und Sektorleiter müssen mit Presshülsen sowie geeigneten Presswerkzeugen vorbereitet werden, um eine dauerhafte Kontaktierung zu gewährleisten (s. auch unsere Technischen Hinweise QM-TH-001 Leiteranschluss SL-ZAKD_ZIKD_ZAKW-Baureihe)

Zählerstiftabstände:	gemäß DIN 43857 [d]
Verlustleistungsangabe:	0,50 Watt bei 63A und 40°C Umgebungstemperatur
Umgebungstemperatur:	-30°C bis +65°C [e]
IP-Schutzart:	IP2XC (nach Montage aller Systemkomponenten)
Höhe/ Breite/ Tiefe:	35 mm / 88 mm / 44 mm
Gewicht:	1 Stück - 0,14 kg
VPE - Gewicht:	96 Stück - 13,44 kg
Kunststoff - Material:	PA 66 V0, halogenfrei

5. Zertifizierungen und Konformitäten:
OVE R21:2019; Niederspannungsrichtlinie LVD Directive 2014/35/EU
RoHS III Directive 2015/863/EU; IEC/EN 60998-2-1; IEC 61545

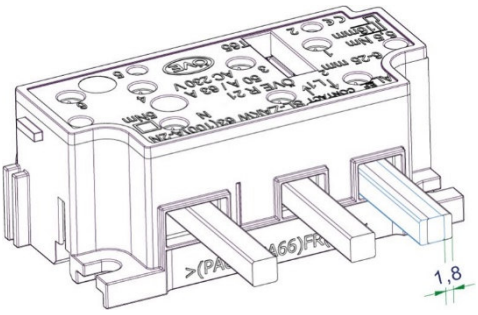
6. Verlustleistung:

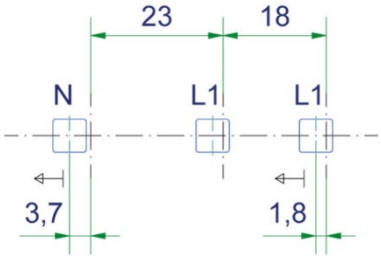
Zu- und Abgang der Phasenanschlüsse und Neutralleiteranschlüsse, durchschnittliche Verlustleistungsermittlung	
Systemstifte SL-....	Mittelwert Angabe in Watt
Belastungsstrom	40°C
63A	0,50

Flächenauflage vs. Linienauflage

Durch die quadratische Ausführung des Stiftes ist eine Flächenauflage anstatt einer herkömmlichen Linienauflage in Kombination mit der Anschlussklemme SL-ZAKW gegeben.

7. Mögliche Zählerstiftabstände durch seitlichen Versatz (Open Contact):





Einzigartig und innovativ ist der seitliche Versatz der Zähleranschlussstifte von bis zu 3,6 mm (1,8 mm je Seite – N: 1,8 mm und 3,7 mm). Dadurch können alle derzeit verwendeten Energiezähler und Smartmeter mit der Anschlussklemme SL-ZAKW angeschlossen werden.

8. Kompatibilitäts- und Montagehinweise
Die Klemme darf ausschließlich mit dem zugelassenen Überbrückungswerkzeug SL-ZAKW-UEW-01 temporär überbrückt werden.
Für den Anschluss von Smartmetern / Energiezählern sind ausschließlich folgende Stifte zugelassen:
- 63A - Anschluss mit System-Zählerstift der Reihe SL-6-6-XXX (alle nach OVE R21:2019)
- 50A - Anschluss mit Standard-Zählerstift nach OVE R21:2019

Bei Schraubenbefestigung auf einer Zählertafel / Zählerplatte muss in Bezug auf die Montageschrauben die Befestigungslaschenhöhe von 6 mm berücksichtigt werden (inkl. Ausnehmung für Überstand der Gleitmuttern gem. OVE E 8640). Die Schraubenlänge ist derart zu wählen, dass die Montageschraube ausreichend Gewindegänge in die Gleitmutter der Zählerplatte, gemäß Herstellerspezifikation, aufweist.

[d] Open Contact s. Skizze, Punkt 7
[e] Auswahl der entsprechenden Aderisolation (Temperaturbeständigkeit) für die zugeführten Leiter ist erforderlich

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®

ÖVE Zertifikatsnummer:
85145-006

Zähleranschlussklemme

SL-ZSK 50(80)A-2N m. TRE

Artikelnummer 1008600
Datenblatt QM-PD-001 Index F
Erstellt 18.10.24 von PM
Prüfung SZ
Freigabe SZ

1. Zweck:
Die Klemme mit Inserts aus versilbertem Kupfer für den Anschluss von Smartmeter/Energiezähler ermöglicht den spannungsunterbrechungsfreien Gerätetausch.

2. Funktion:
Die Funktion der Anschlussklemme erfüllt die OVE R21:2019 und orientiert sich an den Sicherheitszielen der DIN VDE 0603-3-3.

3. Sicherheit:
Die Klemme, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter-Energiezählertausch. **Die Montage ist durch eine Elektrofachkraft durchzuführen!**

4. Technische Daten:

SL-ZSK 50(80)A-2N mit TRE	Anschlussklemme Smartmeter / Zähler, Dauerstrom 50A, mit zweitem Anschluss für N-Leiter und Tarifanschluss
Nennstrom:	50A (maximal zulässiger Nennstrom der zugehörigen Überlastschutzeinrichtung)
Steckzyklen:	10.000
Prüf- Überlaststrom:	80A (geprüft mit 1,6-fachem Nennstrom) für 1h
Betriebsspannung:	400V AC, 50Hz
Anschlussquerschnitt / Leiterart:	2,5 - 16 mm^2, Cu-Leiter starr-eindrähtig / starr-mehrdrähtig / flexibel mit Aderendhülse [a], Einstecktiefe 18 – 22 mm
Anschlussquerschnitt Tarifanschluss:	0,5 - 2,5 mm^2, Cu-Leiter starr-eindrähtig / flexibel mit Aderendhülse [a], Einstecktiefe 12 mm
Anschlüsse zählerseitig:	Standard-Zählerstifte, Zählerstiftabstände gemäß DIN 43857-2
Antriebswerkzeug Klemmschrauben:	SL/PZ2 - Zu- und Abgangsklemmen (Phasen + N) SL/PZ1 - Tarifanschluss
Anzugsdrehmoment Klemmschrauben:	3 Nm - Zu- und Abgangsklemmen (Phasen + N) 0,5 Nm - Tarifanschluss
Anzugsdrehmoment Befestigungsschrauben ADH:	max. 0,3 Nm
Zählerstifte:	SL-6-5-44-RV-Z, SL-5-5-44-R-Z
Betriebsumgebungstemperatur:	max. 60°C
Lager-/Transportumgebungstemperatur:	0°C bis 35°C
IP-Schutzart:	IP2XC (nach Montage aller Systemkomponenten inkl. Abdeckhaube)
Höhe/ Breite/ Tiefe:	45 mm / 149 mm / 33 mm
Gewicht:	275 g
Verlustleistungsangabe:	3,3W bei 50A über alle drei Phasen bei Raumtemperatur
Kunststoff - Material:	PA 6.6

5. Zertifizierungen und Konformitäten:
OVE R21:2019; Niederspannungsrichtlinie LVD Directive 2014/35/EU; RoHS III Directive 2015/863/EU

[a] DIN 46228-1, DIN 46228-4 oder gleichwertig

Produkt-Datenblatt

SEIDL
MEMBER OF SEIDLGROUP®

VDE-Ausweisnummer:
40054501

Zähleranschlussklemme

SL-ZSK 63A-2N m.TRE

Artikelnummer 1030032
Datenblatt QM-PD-003 Index C
Erstellt 18.10.24 von PM
Prüfung SZ
Freigabe SZ

1. Zweck:
Die Klemme mit Inserts aus versilbertem Kupfer für den Anschluss von Smartmeter/Energiezähler ermöglicht den spannungsunterbrechungsfreien Gerätetausch.

2. Funktion:
Die Funktion der Anschlussklemme entspricht den Sicherheitszielen der DIN VDE 0603-3-3.

3. Sicherheit:
Die Klemme, sowie umfangreiche Systemkomponenten, gewährleisten optimale, sichere und zukunftsorientierte Montage, Dauerbetrieb und kundenfreundlichen Smartmeter-Energiezählertausch. **Die Montage ist durch eine Elektrofachkraft durchzuführen!**

4. Technische Daten:

SL-ZSK 63A-2N m. TRE	Anschlussklemme Smartmeter / Zähler, Dauerstrom 63A, mit zweitem Anschluss für N-Leiter und Tarifanschluss
Bemessungsstrom:	63A
Betriebsspannung:	400V AC, 50Hz
Anschlussquerschnitt / Leiterart:	6 - 16 mm^2, Cu-Leiter starr-eindrähtig / starr-mehrdrähtig / flexibel mit Aderendhülse[a], Einstecktiefe 18 – 22 mm
Anschlussquerschnitt Tarifanschluss:	0,5 - 2,5 mm^2, Cu-Leiter starr-eindrähtig / flexibel mit Aderendhülse [a], Einstecktiefe 12 mm
Anschlüsse zählerseitig:	Standard-Zählerstifte, Zählerstiftabstände gemäß DIN 43857-2
Antriebswerkzeug Klemmschrauben:	SL/PZ2 - Zu- und Abgangsklemmen (Phasen + N) SL/PZ1 - Tarifanschluss
Anzugsdrehmoment Klemmschrauben:	3 Nm - Zu- und Abgangsklemmen (Phasen + N) 0,5 Nm - Tarifanschluss
Anzugsdrehmoment Befestigungsschrauben ADH:	max. 0,3 Nm
Zählerstifte:	SL-6-5-44-RV-Z, SL-5-5-44-R-Z
Betriebsumgebungstemperatur:	max. 60°C
Lager-/Transportumgebungstemperatur:	0°C bis 35°C
IP-Schutzart:	IP2XC (nach Montage aller Systemkomponenten inkl. Abdeckhaube)
Höhe/ Breite/ Tiefe:	45 mm / 149 mm / 33 mm
Gewicht:	275 g
Verlustleistungsangabe:	4,2W bei 63A über alle drei Phasen bei Raumtemperatur
Kunststoff - Material:	PA 6.6

5. Zertifizierungen und Konformitäten:
DIN VDE 0603-1; DIN VDE 0603-3-3; Niederspannungsrichtlinie LVD Directive 2014/35/EU; RoHS III Directive 2015/863/EU

[a] DIN 46228-1, DIN 46228-4 oder gleichwertig