Leitfaden Systemkopplungen in der Energiewirtschaft Version 3.0, 11/2025

Empfehlung zu Errichtung und Betrieb von leit- und fernwirktechnischen Kopplungen

Herausgeber:
Oesterreichs Energie
Brahmsplatz 3, 1040 Wien, Österreich

Ansprechpartner:
Armin Selhofer (Österreichs E-Wirtschaft)

Autoren:
Projektgruppe „Systemkopplungen in der Energiewirtschaft“

Fachliche Beratung und Unterstützung:
Dr. Stephan Beirer, Dr. Derk Frerichs-Mihov (GAI NetConsult GmbH, Berlin/Deutschland)

Klassifizierung:
TLP-White

Version 3 vom 28.11.2025

Änderungshistorie:

Version	Datum	Beschreibung der Änderungen
1.0	16.09.2015	Initiale Version
2.0	12.04.2016	Einarbeitung von Kommentaren der GAI NetConsult GmbH und RWE AG
3.0	28.11.2025	Grundlegende Änderungen im gesamten Dokument (Ergänzung Abschnitte 2.1, 2.2, 2.3, 2.6, A.1, Kapitel 3, Überarbeitung Abschnitte 2.4, 2.5, A.2)

Inhalt

1. Einleitung

Im Mai 2013 ereignete sich eine Fernwirkstörung, die Auswirkungen auf mehrere Gas-/Strom-Netzbetreiber und Erzeuger in Österreich hatte. Die Ausbreitung der Störung zu mehreren Energieversorgungsunternehmen (EVU) erfolgte über die Systemkopplungen, die zum Datenaustausch zwischen den EVU errichtet worden waren.

Definition Systemkopplung:
Verbindung zwischen Netzwerken und Kommunikationsinfrastrukturen der Leit- und Fernwirktechnik, deren ordnungsgemäßer Betrieb unterschiedlichen Verantwortlichen („Partner“) zugeordnet ist. Leit- und fernwirktechnische Kopplungen zu Nicht-EVU gelten ebenfalls als Systemkopplungen.

Oesterreichs Energie hat über den Ausschuss IKT eine Projektgruppe installiert, um die Fernwirkstörung zu bearbeiten und Maßnahmen zur Verhinderung ähnlicher Probleme vorzuschlagen. Die Fach-Experten der Projektgruppe *Fernwirkstörung* haben daher einen Leitfaden entwickelt, der für Systemkopplungen den aktuellen Stand der Technik unter Berücksichtigung notwendiger Sicherheitsmaßnahmen spezifiziert. Dieser wurde 2025 von der Projektgruppe „Systemkopplungen in der Energiewirtschaft" überarbeitet und an aktuelle Entwicklungen angepasst.

Oesterreichs Energie empfiehlt, neue Kopplungen anhand des vorliegenden Leitfadens aufzusetzen. Bestehende Kopplungen sollen geprüft werden und in Abstimmung mit dem Partner gegebenenfalls angepasst werden. Dafür kann die angehängte Checkliste für Systemkopplungen zur Hilfe genommen werden.

An den entsprechenden Stellen des Leitfadens wird auf relevante Normanforderungen aus der ISO/IEC 27002:2022 und der ISO/IEC 27019:2024 sowie auf Best-Practice Empfehlungen des BDEW/OE/VSE Whitepapers *Anforderungen an sichere Steuerungs- und Telekommunikationssysteme* Version 3.0 09/2024 (kurz BDEW/OE/VSE Whitepaper 3.0:2024) verwiesen. Des Weiteren befindet sich im Anhang A.1 eine Mappingtabelle, die den Anforderungen der Netz- und Informationssystemsicherheitsverordnung vom 17. Juli 2019 die jeweiligen Abschnitte dieses Leitfadens zuordnet.

Dieser Leitfaden gilt sowohl für serielle als auch auf Ethernet basierende Systemkopplungen. Für Systemkopplungen werden die Fernwirkprotokolle IEC 60870-5-101 bzw. -104, TASE.2 und IEC 61850 empfohlen. Für andere Protokolle gelten die Empfehlungen sinngemäß.

Dieser Leitfaden beschränkt sich auf Übertragungsprotokolle der Leit- und Fernwirktechnik, Vorgaben für die unterlagerte IT-Infrastruktur mit WAN-, MAN-Strukturen und MPLS-Netzen sind nicht Teil dieser Empfehlungen.

In diesem Dokument werden die organisatorischen und technischen Maßnahmen festgelegt, die für die Planung, Errichtung und den Betrieb von Systemkopplungen eingehalten werden sollen. Auch wenn allgemeingültige Themen der Informationssicherheit in diesem Leitfaden nicht gesondert behandelt werden, müssen sie bei der Planung, der Errichtung und während des Betriebs von Systemkopplung stets mitgedacht und mit beachtet werden. Dazu zählen insbesondere

- ISO/IEC 27002:2022 und ISO/IEC 27019:2024 5.37 Dokumentierte Betriebsabläufe,
- ISO/IEC 27002:2022 und ISO/IEC 27019:2024 6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung,
- ISO/IEC 27002:2022 und ISO/IEC 27019:2024 7 Physische Maßnahmen,
- ISO/IEC 27002:2022 und ISO/IEC 27019:2024 8.32 Änderungssteuerung,
- BDEW/OE/VSE Whitepaper 3.0:2024 4.1.1 Sichere Systemarchitektur bis einschließlich 4.1.4 Support für eingesetzte Systemkomponenten,
- BDEW/OE/VSE Whitepaper 3.0:2024 4.1.8 Sichere Standard-Konfiguration.

Die in den Kapiteln 2 und 3 beschriebenen Anforderungen stützen sich auf die folgenden Formulierungen zur Klassifizierung der Verbindlichkeit der Maßnahmen:

- Eine „*muss/müssen*“-Anforderung gilt als verpflichtend umzusetzen.
- Von einer „*soll/sollte*“-Anforderung darf abgewichen werden, wenn der Umsetzung der Anforderung nachvollziehbare Gründe entgegenstehen. Dies muss nachvollziehbar begründet und dokumentiert werden.
- Die Umsetzung einer „*empfohlen*“-Anforderung obliegt den Partnern und von ihr darf nach Absprache der Partner auch ohne schriftliche Begründung abgewichen werden.
- Bei „*darf/dürfen*“-Anforderungen handelt es sich um erlaubte Ausnahmen, die keiner Begründung bedürfen. Diese Ausnahmen sind jedoch ggf. an Bedingungen geknüpft, die dafür erfüllt sein müssen.

Die angehängte Checkliste für Systemkopplungen listet die wesentlichen Anforderungen auf und kann zur Hilfe genommen werden, um einen ersten Überblick über den Stand jeder einzelnen Systemkopplung zu erhalten.

2. Organisatorische Maßnahmen

2.1 Vereinbarung zur Systemkopplung

ISO/IEC 27019:2024: 7.18 ENR, 8.38 ENR

Zu jeder Systemkopplung muss in Ergänzung zu den Richtlinien der Informationsübermittlung der Partner (vgl. ISO/IEC 27002:2022 5.14 Informationsübermittlung) eine zwischen den Partnern abgestimmte Vereinbarung vorliegen, welche die sicherheitsrelevanten Angaben beschreibt und verbindlich definiert.

Es muss dabei klar definiert werden, ob bzw. dass die Systemkopplung bei Störungen oder geplanten Wartungsarbeiten getrennt werden kann, wer dies anzuordnen befugt ist sowie welche Voraussetzungen und Bedingungen dafür gegeben sein müssen. Eine entsprechende Festlegung für den geregelten Wiederanlauf der Kopplungen nach einer Trennung sollte ebenfalls definiert werden. Beide Seiten müssen dafür die Kontaktmöglichkeiten der zuständigen Personen bereitstellen.

In der Vereinbarung muss festgelegt werden, welche Sicherheitsanforderungen für die Kopplung gelten und dass diese nach Stand der Technik gesichert wird. Weiterhin sollte basierend auf den möglichen Auswirkungen der Trennung der Kopplung festgelegt werden, ob bzw. welche Ausgleichsmaßnahmen im Falle der Trennung sinnvoll sind. Die konkrete Ausgestaltung der Sicherheits- und Ausgleichsmaßnahmen wird in einem Realisierungskonzept festgehalten, siehe 2.2 *Realisierungskonzept der Systemkopplung*, das der Vereinbarung anzuhängen ist.

Es sollte ebenfalls festgehalten werden, ob die Verbindung hohen Verfügbarkeitsanforderungen unterliegt und dementsprechend redundant realisiert werden muss, vgl. ISO/IEC 27002:2022 8.14 Redundanz von informationsverarbeitenden Einrichtungen.

Darüber hinaus sollte vereinbart werden, in welchem Umfang vor Inbetriebnahme von zur Kopplung genutzten Komponenten diese einer Sicherheitsprüfung unterliegen sollen. Dies gilt insbesondere auch beim Austausch von Komponenten.

2.2 Realisierungskonzept der Systemkopplung

BDEW/OE/VSE Whitepaper 3.0:2024: 4.1.11, 4.4.3

Zu jeder Systemkopplung muss in Ergänzung zu 2.1 *Vereinbarung zur Systemkopplung* ein Realisierungskonzept vorliegen, welches der Planung der Systemkopplung und der Abstimmung der Partner vor Inbetriebnahme der Kopplung dient. Es definiert die grundlegenden Rahmenbedingungen der Systemkopplung und wie diese technisch und organisatorisch realisiert werden soll.

Hinweis: Dieses Realisierungskonzept kann als Grundlage für die nach der Einrichtung der Kopplung anzufertigende Dokumentation dienen, vgl. 2.3 *Dokumentation der Systemkopplung*.

Folgende Punkte müssen in diesem Realisierungskonzept beschrieben werden:

- die verwendeten Protokolle zum Datenaustausch,
- die Liste der tatsächlich an einer Systemkopplung verwendeten Typkennungen,
- die Liste der umzusetzenden Sicherheitsmaßnahmen und insbesondere die zu nutzenden kryptographischen Verfahren und deren Parameter in Bezug auf Authentisierung, Integrität und Verschlüsselung, vgl. 2.1 *Vereinbarung zur Systemkopplung*,
- die Ausgestaltung der Ausgleichsmaßnahmen im Falle einer Trennung, wenn in der Vereinbarung der Partner festgeschrieben wurde, dass Ausgleichsmaßnahmen vorzunehmen sind, vgl. 2.1 *Vereinbarung zur Systemkopplung*,
- ob und wie die Netzwerkdienste überwacht werden,
- die Kopplungsarchitektur,
- die normale und maximal zu erwartende Datenübertragungsrate,
- die zur Zeitsynchronisation verwendete Zeitquelle bzw. die verwendeten Zeitquellen, wobei die Zeitsynchronisation über die gleiche Zeitquelle stattfinden sollte,
- ggf. Ersatzwege für die Notfallkommunikation, vgl. 2.4 *Incident Management*, und Meldewege zur Übermittlung ungewöhnlicher Ereignisse, vgl. 3.5 *Monitoring der Systemkomponenten und Perimeterüberwachung*.

Die Betreiber müssen das Realisierungskonzept bei allen relevanten Änderungen aktualisieren. Zusätzlich muss dieses Konzept zur Qualitätssicherung zyklisch – z. B. jährlich – auf Aktualität überprüft werden. Dabei muss insbesondere sichergestellt werden, dass es dem aktuellen Stand der Technik entspricht.

2.3 Dokumentation der Systemkopplung

ISO/IEC 27019:2024: 7.18 ENR
BDEW/OE/VSE Whitepaper 3.0:2024: 4.4.3

Während das Realisierungskonzept aus 2.2 *Realisierungskonzept der Systemkopplung* beschreibt, wie die Systemkopplung umzusetzen ist, beschreibt die Dokumentation der Systemkopplungen den aktuellen Ist-Zustand der Ausführung. Damit ist die Dokumentation insbesondere eine Grundvoraussetzung für die Ermöglichung eines sicheren Betriebs. Darüber hinaus muss die Dokumentation mit dem Ziel erstellt werden, bei Bedarf die Systemkopplungen schnellstmöglich trennen zu können und muss daher alle zur Erreichung dieses Ziels nötigen Informationen beinhalten sowie Anlagendetails und die technische Umsetzung möglichst exakt beschreiben.

Jeder Partner führt eine eigene Dokumentation. Diese sollte aufbauend auf dem Realisierungskonzept aus 2.2 *Realisierungskonzept der Systemkopplung* erstellt werden. Die Betreiber müssen diese Dokumentation bei allen relevanten Änderungen am System aktualisieren.

Mindestens muss die Dokumentation dabei folgenden Punkte behandeln:

- alle eingesetzten Komponenten und Systeme,
- alle physischen, logischen und virtuellen Netzwerkverbindungen der Komponenten/Systeme,
- IP-Adressen der Geräte,
- verwendete Protokolle zum Datenaustausch mit dem Partner
- verwendete Protokolle zur internen Prozessanbindung und zur Administration der Komponenten,
- die Liste der verwendeten Typkennungen,
- verwendete kryptographische Verfahren und deren Parameter,
- verwendete Ports,
- normale und maximal zu erwartende Datenübertragungsraten,
- eine regelmäßig gepflegte Adressliste mit technischen Ansprechpersonen von angrenzenden Partnern,
- die Konfigurationen und Parametrierungen der zur Kopplung genutzten Komponenten,
- die sichere Grundkonfiguration und die durchgeführten Härtungsmaßnahmen, vgl. 3.4 *Härtung*,

- die verwendete Zeitquelle oder Zeitquellen, ggf. inkl. der Konfiguration der Anbindung,
- ggf. die vereinbarten Ersatzwege für die Notfallkommunikation, vgl. 2.4 *Incident Management*, und Meldewege zur Übermittlung ungewöhnlicher Ereignisse, vgl. 3.5 *Monitoring der Systemkomponenten und Perimeterüberwachung*.

Darüber hinaus sollte die Dokumentation folgende Aspekte beachten:

- Es sollten Anlagen- bzw. Übersichtsbilder enthalten sein
- Die Dokumentation sollte Port-genau sein (Switch Port).
- Kabel sollten mit Kabelnummer und Ziel sowie Gegenziel beschriftet sein.
- Die Dokumentation sollte die maximal zulässige Netzwerkbelastung beinhalten, unterhalb der eine zuverlässige Funktion des Gesamtsystems und der Einzelkomponenten gewährleistet ist.

Die mit der Systemkopplung befassten Leit- und Fernwirktechniker müssen jederzeit Zugriff auf die Dokumentation haben. Außerdem muss die Dokumentation auch im Rahmen des Incident Managements zur Verfügung stehen und jederzeit aktuell gehalten werden, vgl. 2.4 *Incident Management.*

Zusätzlich muss die Dokumentation zur Qualitätssicherung zyklisch – z. B. jährlich – auf Aktualität überprüft werden. Dabei sollte außerdem festgestellt werden, ob veraltete Technologien („Legacy Systems“) genutzt werden. Diese sollten mittelfristig durch Systeme/Komponenten ersetzt werden, die dem Stand der Technik entsprechen, vgl. ISO/IEC 27019:2024 8.35 ENR – Treatment of legacy systems.

Technische Änderungen in den Systemkopplungen müssen zwischen den Partnern abgestimmt werden und dementsprechend die Dokumentation aktualisiert werden.

2.4 Incident Management

ISO/IEC 27002:2022: 5.24
ISO/IEC 27019:2024: 7.18 ENR

Jeder Partner muss die Kritikalität der Kopplung für die eigenen Betriebsprozesse analysieren und bewerten (Business Impact Analyse). Darauf aufbauend muss der Ablauf, wie leit- und fernwirktechnische Störungen größeren Ausmaßes behandelt werden, im Notfall- bzw. Krisenmanagement-Prozess des jeweiligen Unternehmens abgebildet sein. Für als kritisch eingestufte Kopplungen müssen Notfallpläne erstellt werden, in denen die Begrenzung der Folgen eines Ausfalls oder einer Kompromittierung der Kopplung behandelt wird und in denen aufgeführt ist, was im Falle eines Vorfalls zu tun ist. Dadurch sollten Störungen, Schäden und Folgeschäden minimiert werden und der Normalbetrieb zeitnah wiederhergestellt werden können. Es müssen die erforderlichen technischen und personellen Ressourcen für die vorgesehenen Notfallmaßnahmen vorgesehen werden.

Die Partner sollten im Rahmen der Notfallplanung prüfen, ob Ersatzwege für die Notfallkommunikation einzurichten sind, vgl. ISO/IEC 27019:2024 8.40 ENR – Emergency communication.

Die an einer Kopplung beteiligten Partner sollten sich auf einen Prozess einigen, wie Erkenntnisse aus Störungen oder Ausfälle wesentlicher Fernwirkdaten-Kopplungen gewonnen werden können und wie daraus für die Zukunft präventive Maßnahmen abgeleitet werden können („Lessons Learned“). Das Ziel des Prozesses muss sein, die aus aufgetretenen Störungen bzw. Ausfällen gewonnenen Erkenntnisse dafür zu nutzen, die Wahrscheinlichkeit für einen erneuten Ausfall bzw. dessen negative Auswirkungen in der Zukunft zu minimieren.

2.5 Schulung

ISO/IEC 27002:2022: 5.24, 6.3
ISO/IEC 27019:2024: 6.3

Die für die Kopplung zuständigen Personen müssen regelmäßig – in Abhängigkeit von der Kritikalität alle ein bis drei Jahre – geschult werden. Das Ziel der Schulung muss sein, die zuständigen Personen zu befähigen, eine ordnungsgemäße Isolierung sowie eine geregelte Wiederaufnahme der Kopplung durchführen zu können. Dafür sollten sie u.a. die Voraussetzungen für die Trennung der Systemkopplungen und die technische Dokumentation der Kopplung kennen sowie ein Verständnis für den Incident Managementprozess aus 2.4 *Incident Management* haben.

Es wird außerdem empfohlen, Störungen an der Systemkopplung in etwaigen Notfallübungen zu simulieren.

Das Personal sollte für die Reaktion auf etwaige Warnmeldungen automatisierter Überwachungssysteme vorgesehen und entsprechend geschult sein, um mögliche Vorfälle richtig zu interpretieren, vgl. 3.5 *Monitoring der Systemkomponenten und Perimeterüberwachung*.

2.6 Abnahme und Inbetriebnahmeprüfung

ISO/IEC 27019:2024: 8.2
BDEW/OE/VSE Whitepaper 3.0:2024: 4.2.2

Vor der Inbetriebnahme muss eine Prüfung der Systemkopplung stattfinden, wobei sich die Partner bezüglich des Umfangs der Prüfung abstimmen dürfen. Der Umfang der Prüfungen sollte im Verhältnis zur Bedeutung, zur Art des Systems und zur Kritikalität der Kopplung stehen. Mindestens muss ein Vergleich des Ist-Zustandes der Parametrierungen und Konfigurationen mit dem dokumentierten Soll-Zustand enthalten sein. Weiterhin sollte in einem Security-Abnahmetest

- die sichere Grundkonfiguration des Systems,
- die durchgeführten Härtungsmaßnahmen,
- die Umsetzung aller technischer Maßnahmen aus 3 *Technische Maßnahmen* und,
- ob das Realisierungskonzept aus 2.2 *Realisierungskonzept der Systemkopplung* umgesetzt wurde,

geprüft werden. Zusätzliche Prüfungen zur Sicherstellung, dass über die Systemkopplung keine Kompromittierung der jeweiligen Partnerumgebungen möglich sind, werden ebenfalls empfohlen.

Die Prüfung sollte nach Änderungen an der Architektur oder security-relevanten Einstellungen bzw. Parametrierungen wiederholt werden.

3. Technische Maßnahmen

Die folgenden technischen Maßnahmen müssen bei der Planung, Errichtung und dem Betrieb von Systemkopplungen von allen Partnern berücksichtigt werden. Die Einhaltung der Maßnahmen und ob die Umsetzung der Maßnahmen noch dem aktuellen Stand der Technik entspricht, muss zyklisch, z.B. jährlich, überprüft werden und ggf. die Dokumentation aus 2.3 *Dokumentation der Systemkopplung* aktualisiert werden.

In der Praxis können technische oder organisatorische Einschränkungen (z.B. durch die verwendete Fernwirktechnik) eine Umsetzung der Maßnahmen in einzelnen Punkten verhindern. Diese Abweichungen sollten technisch nachvollziehbar begründet, zwischen den Partnern abgestimmt und im Realisierungskonzept aus 2.2 *Realisierungskonzept der Systemkopplung* dokumentiert werden.

Zentrale Systemkopplungen, d.h. solche auf Leitsystemebene, sollten vorzugsweise über das TASE.2-Protokoll oder IEC-60870-5-104 realisiert werden. Dezentrale Systemkopplungen, d.h. Kopplungen, die in oder zwischen lokalen Anlagen stattfinden, sollten vorzugsweise auf IEC-60870-5-101 oder -104 basieren.

3.1 Netzwerksegmentierung

ISO/IEC 27019:2024: 8.22
BDEW/OE/VSE Whitepaper 3.0:2024: 4.4.2

Wo technisch umsetzbar, sollte für die Kopplung eine DMZ-Struktur realisiert werden, d.h. es soll eine separate getrennte Netzwerkzone geben, in der dedizierte Komponenten die Verbindung zum Partner terminieren. Darüber hinaus sollte eine physische Trennung zwischen den Netzwerken für den Datenaustausch mit dem Partner und den internen Systemen (interne Prozessdaten, Monitoring, Logging, Engineering, Administration etc.) eingerichtet werden. Alternativ ist auch eine logische Trennung zugelassen, wenn die physische Trennung technisch nicht möglich ist. Damit soll sichergestellt werden, dass der Datenverkehr von bzw. zum Partner über ein anderes (logisches), separates Netzwerk verläuft als der interne Datenverkehr, vgl. ISO/IEC 27019:2024 8.22 Segregation of networks.

Um den Zugang von außen zum eigenen Netzwerk einzuschränken, müssen von allen Partnern jeweils eigene filternde Komponenten wie Firewalls oder Gateways eingesetzt werden. Die Weiterleitung des Verkehrs beschränkt sich auf genau definierten und explizit erlaubten Verkehr vom Kopplungspartner, vgl. 3.2 *Zugelassener Datenverkehr*. Jeglicher darüber hinaus gehende Verkehr muss blockiert bzw. verworfen werden. Sofern der Einsatz von separaten, filternden Komponenten technisch nicht möglich ist, muss geprüft werden, ob die Kopplungskomponenten selbst entsprechende Filterfunktionen (Protokoll-Allowlisting) bieten. Diese müssen in diesem Fall als Ausgleichsmaßnahme aktiviert werden.

Für auf IP basierende Protokolle gilt, dass wenn möglich eine zu den filternden Komponenten ergänzende Filterung auf Applikationsebene realisiert sein sollte. Ist dies nicht möglich muss sie mindestens auf Port und IP-Adress-Ebene selektieren.

Weiterhin müssen Maßnahmen gegen ein uneingeschränktes Anfordern von Ressourcen wie z.B.

Netzwerkbandbreite implementiert werden, um z.B. Denial-of-Service-Ausfällen vorzubeugen. Die Datenübertragungsrate muss auf die in 2.2 *Realisierungskonzept der Systemkopplung* festgelegte maximale Rate begrenzt werden.

3.2 Zugelassener Datenverkehr und sichere Protokolle

ISO/IEC 27002:2022: 8.3
BDEW/OE/VSE Whitepaper 3.0:2024: 4.4.1

Der zugelassene Datenverkehr unterscheidet sich zwischen der Schnittstelle zum Partner und dem internen bzw. Management-Interface.

Der zugelassene Datenverkehr über die Schnittstelle zum Partner beschränkt sich ausschließlich auf die in 2.2 *Realisierungskonzept der Systemkopplung* festgelegten Protokolle und Typkennungen zum Datenaustausch sowie ggf. die in 2.3 *Dokumentation der Systemkopplung* dokumentierten verwendeten Ports. Weitere Protokolle, Ports oder Typkennungen, die über diese festgelegten hinaus gehen, sind nicht zulässig. Datenpunkte, die über die von den Partnern für den jeweiligen Zweck als notwendig identifizierten hinausgehen, müssen verworfen werden, d.h. ein automatischer Datenfluss ist untersagt.

Für IEC 60870-5-101/-104 gelten darüber hinaus die im Folgenden gelisteten Anforderungen:

- Für den Datenaustausch dürfen ausschließlich („muss“-Anforderung) die Standard-Typkennungen aus dem öffentlichen Bereich der IEC 60870-5-101/-104 Norm eingesetzt werden. Typkennungen aus dem privaten Bereich der IEC-Normen dürfen nicht („muss“-Anforderung) verwendet werden, weil hierdurch undokumentierte und sicherheitsrelevante Funktionen wie Fernparametrierung, Fernwartung, Firmwareupgrades und Debugging möglich sein können.
- Alle Systemtelegramme mit Ausnahme der Generalabfrage von Nutzdatenquellen müssen deaktiviert werden.

Die Fernparametrierung auf die Schnittstelle der Systemkopplung muss von Seiten des Partners unmöglich sein. Daher sollten die in 2.3 *Dokumentation der Systemkopplung* definierten Protokolle zur internen Prozessanbindung und zur Administration bzw. zum Management der Komponente nicht über die Schnittstelle zum Partner zugelassen sein. Diese müssen über das interne bzw. Management-Interface realisiert werden. Der Verbindungsaufbau über das interne Interface sollte immer in Richtung zur und nicht von der Kopplungskomponente aus geschehen. Dementsprechend muss der Datenaustausch mit dem Partner der im zweiten Absatz genannten Daten ausschließlich über das externe Interface zum Partner realisiert werden.

Für die Administration der Komponenten müssen sichere Protokolle wie z.B. SSH, SCP, SFTP, HTTPS in der jeweils aktuellen Version und mit aktivierten Sicherheitseinstellungen verwendet werden.

Weiterhin ist der Datenverkehr ausschließlich zulässig, wenn er den in 2.2 *Realisierungskonzept der Systemkopplung* vereinbarten und in 3.3 *Kryptographische Methoden* zugelassenen kryptographischen Maßnahmen entspricht. Datenverkehr, der diesen Maßnahmen nicht entspricht, muss blockiert bzw. verworfen werden. Darunter fallen insbesondere die Maßnahmen aus Tabelle 1.

3.3 Kryptographische Methoden

ISO/IEC 27019:2024: 8.24, 8.37 ENR
BDEW/OE/VSE Whitepaper 3.0:2024: 4.1.5, 4.1.6, 4.1.7

Die empfohlenen kryptographischen Methoden beziehen sich auf gegenseitige Authentifizierung, Integritätsprüfung und Verschlüsselung der übertragenen Daten. Sie unterscheiden sich abhängig von der topologischen Nähe der Partner, dem genutzten Netz und der Art der Verbindung, siehe Tabelle 1. Um das Monitoring der Verbindung zu ermöglichen, darf in Abhängigkeit von der Sensibilität der ausgetauschten Daten nach Einigung der Partner auf eine Verschlüsselung auf Transport-/Applikationsebene verzichtet werden (z.B. durch Verwendung von NULL-Ciphern), wenn die Verschlüsselung dem Monitoring entgegensteht, vgl. 3.5 *Monitoring der Systemkomponenten und Perimeterüberwachung*. In diesem Fall muss die Prüfung der Integrität der Nachrichten und die gegenseitige Authentifizierung weiterhin gewährleistet sein.

Wo möglich sollten in Abhängigkeit von der Kritikalität der Kopplung sicherheitserhöhende Einstellungen der genutzten Protokolle aktiviert werden. Die Standard-Protokolle IEC 60870-5-101 und -104, IEC 61850 sowie TASE.2 bieten ohne zusätzliche Maßnahmen keine sichere Integritätsüberprüfung, Authentifizierung und Verschlüsselung. Hier sollten die verfügbaren Erweiterungen gemäß IEC 62351 eingesetzt werden, d.h.

- IEC 62351-3 zur Sicherung der Transportschicht für TCP/IP-basierte Protokolle mittels TLS,
- IEC 62351-4 zur Sicherung der Anwendungsschicht für MMS-basierte Protokolle wie bspw. TASE.2 und

IEC 61850,
- IEC 62351-5 zur Sicherung der Anwendungsschicht für IEC 60870-5 basierte Protokolle und
- IEC 62351-6 zur Sicherung der Anwendungsschicht für IEC 61850-8-1 GOOSE und -9-2 Sampled Values.

Wo technisch möglich sollten unverschlüsselte Applikations-Protokolle durch Verschlüsselung auf den unteren Netzwerkebenen geschützt werden (z. B. durch verschlüsselte TLS/IPsec-VPN-Verbindungen).

Anforderung M.05_06 des „Sicherheitskonzept - SOGL Echtzeitdatenaustausch“ von Oesterreichs Energie zum Schutz vor Replay Angriffen muss umgesetzt werden, d.h.
- eine versuchte Wiedereinspielung von Nachrichten (message replay) muss erkannt und wiedereingespielte Nachrichten müssen verworfen werden,
- zum Schutz vor „Replay Angriffen“ sollten Protokolle (z.B. IPSec) und Verfahren verwendet werden, welche Mechanismen gegen diese implementiert haben (z.B. Verwendung von Zeitstempeln oder Sequenznummern, deren Authentizität von einem Message Authentication Code sichergestellt wird).

Bei der Auswahl der kryptographischen Verfahren müssen anerkannte Verfahren und Schlüsselmindestlängen benutzt werden, die nach aktuellem Stand der Technik auch in Zukunft als sicher gelten. Die Nutzung von selbstentwickelten kryptographischen Algorithmen ist nicht erlaubt. Als Stand der Technik von Verfahren für Hashbildung, Signaturen und Verschlüsselung und die zugehörigen Schlüssellängen werden insbesondere die BSI-Empfehlungen der TR-02102-Reihe „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ (Bundesamt für Sicherheit in der Informationstechnik, Deutschland) angesehen.

Sofern die Partner digitale Zertifikate einsetzen, müssen dafür PKIs etabliert sein. Die Nutzung von nicht-vertrauenswürdigen, selbst-signierten Zertifikaten ist nicht erlaubt. Alle kryptographischen Schlüssel und Zertifikate müssen ersetzbar sein. Wenn Auto-Enrollement-Mechanismen für das automatische Verteilen von X.509-Zertifikaten genutzt werden, müssen dafür sichere Verfahren wie z. B. SCEP oder EST genutzt werden. Vor der Nutzung von Zertifikaten ist deren Gültigkeit und Authentizität zu prüfen, beim Aufbau verschlüsselter Verbindungen ist dies durch beide Kommunikationspartner beidseitig zu prüfen. Als ungültig oder fehlerhaft erkannte Zertifikate und Zertifikatsketten müssen abgelehnt werden oder eine Alarm-Meldung auslösen. Beim Einsatz einer PKI bzw. von digitalen Zertifikaten müssen potenzielle Ausfall- und Notfallszenarien berücksichtigt werden, wie u. a. der Ausfall von PKI-Systemen oder die Ungültigkeit von digitalen Zertifikaten.

Bei Verwendung von kryptographischen Verfahren und Technologien zur Wahrung der Vertraulichkeit, Authentizität und Integrität von Informationen müssen die Partner ein Konzept zur Schlüsselverwaltung (Key-Management-Konzept) erstellen und umsetzen. Dieses muss den gesamten Schlüssellebenszyklus umspannen. Dabei sollten die Empfehlung und Umsetzungserläuterungen der Anforderung M.05_05 des „Sicherheitskonzept - SOGL Echtzeitdatenaustausch“ von Oesterreichs Energie umgesetzt werden, d.h.
- die Schlüsselverwaltung sollte entsprechend IEC 62351-9 (Schlüsselmanagement für Stromversorgungsanlagen) konzeptioniert und
- die folgenden generischen Vorgaben für kryptographisches Key-Management sollten umgesetzt werden:
    - Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen.
    - Für die Verschlüsselung sollten immer andere Schlüssel als für die Signaturbildung benutzt werden.
    - Die Verwendung von Shared keys (Verwendung ein und desselben Schlüssels auf mehreren Systemen und/oder Geräten über das technisch unbedingt nötige Ausmaß hinaus) sollte nur in Ausnahmefällen zugelassen werden. Die Schlüsselerzeugung sollte in einer sicheren Umgebung (d.h. physisch geschützt) und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen.
    - Schlüssel müssen unvorhersagbar und nicht vorausberechenbar sein, sondern auf Basis von kryptografischen Zufallszahlengeneratoren erzeugt werden.
    - Schlüssel müssen sicher (d.h. vertraulich, integer und authentisch) verteilt werden. Bei Verwendung von kryptographischen Schlüsselaustauschprotokollen sollten diese über die Eigenschaft „Perfect Forward Secrecy“ verfügen.
    - Alle kryptographischen Schlüssel müssen gegen (unbefugte) Veränderung und Verlust geschützt sein. Geheime und private Schlüssel müssen gegen unbefugte Benutzung und Offenlegung geschützt werden.
    - Der Schutzbedarf von kryptographischen Schlüsseln muss mindestens so hoch sein wie der Schutzbedarf der Daten, die damit geschützt werden. Die Zugriffsberechtigungen auf die Schlüssel müssen nach striktem Need-to-know Prinzip vergeben werden.
    - Systeme zur Speicherung und Archivierung von Schlüsseln sollten physisch geschützt sein.
    - Zur sicheren Speicherung von sensiblen bzw. kritischen Schlüsseln sollten spezielle Sicherheits- bzw. Kryptomodule mit einschlägigen Zertifizierungen (z.B. nach FIPS 140-2) eingesetzt werden.

- Im Zuge der Schlüsselinstallation muss die authentische Herkunft sowie die Integrität der Schlüsseldaten überprüft werden.
- Vor dem Einsatz von kryptographischen Schlüsseln muss ihre jeweilige Gültigkeitsdauer festgelegt und dokumentiert werden. Auf Basis letzterer müssen regelmäßig Schlüsselwechsel (rechtzeitig vor Ablauf der Gültigkeitsdauer) durchgeführt werden.
- Es muss sichergestellt werden, dass vor der Inbetriebnahme eines kryptographischen Verfahrens voreingestellte (Initial-)Schlüssel geändert werden.
- Kompromittierte Schlüssel (z.B. nach Diebstahl, Verlust oder unbefugter Offenlegung) müssen umgehend gewechselt werden (ein diesbezüglicher Verdacht reicht).
- Nicht mehr benötigte Schlüssel (z.B. Schlüssel, deren Gültigkeitsdauer abgelaufen ist) müssen auf sichere Art gelöscht bzw. vernichtet werden (z.B. durch mehrfaches Löschen/Überschreiben oder die mechanische Zerstörung des Datenträgers).

In der folgenden Tabelle sind die Anforderungen an die Erfüllung der gegenseitigen Authentifizierung, Integritätsprüfung und Verschlüsselung für verschiedene Szenarien aufgeführt:

Tabelle 1: Anforderungen an die Erfüllung gegenseitiger Authentifizierung, Integritätsprüfung und Verschlüsselung für verschiedene Szenarien.

Szenario	Gegenseitige Authentifizierung	Integritätsprüfung	Verschlüsselung
a) Anlagen-lokale Übertragung über eigenes Netz, direkte Verbindung	Empfohlen	Empfohlen	Empfohlen
b) Anlagen-übergreifende Übertragung über EVU-eigenes Netz, direkte Verbindung	Empfohlen	Empfohlen	Empfohlen
c) Anlagen-übergreifende Übertragung über EVU-eigenes Netz, geroutete Verbindung	Muss	Muss	Empfohlen
d) Anlagen-übergreifend, Übertragung über privates Provider-Netz, geroutete Verbindung	Muss	Muss	Muss*
e) Anlagen-übergreifend, Übertragung über öffentliches Netz, geroutete Verbindung	Muss	Muss	Muss*

* Eine Verschlüsselung auf Transport-/Applikationsebene darf in Abhängigkeit von der Sensibilität der ausgetauschten Daten nach Einigung der Partner entfallen, wenn die Verschlüsselung dem Monitoring entgegensteht, vgl. 3.5 *Monitoring der Systemkomponenten und Perimeterüberwachung*.

3.4 Härtung

ISO/IEC 27002:2022: 8.9
ISO/IEC 27019:2024: 8.39 ENR
BDEW/OE/VSE Whitepaper 3.0:2024: 4.3.1

Alle eingesetzten Komponenten müssen so weit wie technisch möglich gehärtet sein, mit aktuellen Sicherheits-Patches versehen sein und sofern technisch möglich mit einem aktuellen Schadsoftwareschutz versehen sein. Das sollte anhand anerkannter Best-Practice-Guides oder Hersteller-Guides geschehen.

Die Komponenten müssen so konfiguriert sein, dass ausschließlich die für die Kopplung benötigten Funktionen aktiviert sind. Nicht benötigte Funktionen, wie z.B. Software, Ports, unterstützte Protokolle, unnötige Benutzer, Default User müssen so weit wie möglich deaktiviert werden sowie gegen versehentliches Reaktivieren geschützt werden.

Zu den anzuwendenden Härtungsmaßnahmen zählen, sofern durch die jeweiligen Komponenten unterstützt u.a.:

- Deinstallation oder Deaktivierung nicht benötigter Software-Komponenten und Funktionen
- Deaktivierung unsicherer bzw. nicht benötigter System- und Kommunikationsdienste (z. B. Parametrierung und Engineering-Zugänge)
- Aktivierung lokaler Firewall-Funktionen
- Deaktivierung bzw. Löschung nicht benötigter Standardnutzer
- Änderung aller Standardpassworte
- Löschung von Installations- und temporären Dateien
- Aktivierung sicherheitserhöhender Konfigurationsoptionen
- Einschränkung der Rechte von Nutzern und Programmen auf das notwendige Minimum
- Deaktivierung nicht benötigter Kommunikations- und Datenträgerschnittstellen (CD/DVD, USB, Bluetooth, WLAN, usw.)
- Deaktivierung nicht benutzter Switch-Ports

- Aktivierung von Application-Allowlisting

Funk- bzw. internetbasierende Fernwartungs- oder Parametrierzugänge zu den für die Systemkopplung verwendeten Komponenten müssen deaktiviert sein.

Empfohlen wird weiterhin eine Adressumrechnung bei Systemkopplungen.

Die sichere Grundkonfiguration und die durchgeführten Härtungsmaßnahmen muss dokumentiert, vgl. 2.3 *Dokumentation der Systemkopplung*, und geprüft sein vgl. 2.6 *Abnahme und Inbetriebnahmeprüfung*. Die sichere Grundkonfiguration sollte wenn möglich automatisiert verifizierbar sein.

3.5 Monitoring der Systemkomponenten und Perimeterüberwachung

ISO/IEC 27002:2022: 8.9, 8.15, 8.16,
ISO/IEC 27019:2024: 8.15
BDEW/OE/VSE Whitepaper 3.0:2024: 4.1.13, 4.5.6

Das Monitoring wird unterschieden zwischen einem Monitoring der Parametrier- und Konfigurationseinstellungen der Komponenten und der Überwachung der Systemkopplung zur Anomalieerkennung.

Monitoring der Parametrier- und Konfigurationseinstellungen

Die aktuellen Konfigurationen und Parametrierungen sollten überwacht und regelmäßig auf Korrektheit bzw. Änderungen im Vergleich zur dokumentierten Konfiguration überprüft werden. Auf Abweichungen sollte reagiert werden, entweder durch automatische Durchsetzung der definierten Soll-Konfiguration oder durch manuelle Analyse der Abweichung und anschließende Korrekturmaßnahmen.

Monitoring der Systemkopplung

Wenn möglich, sollten die zur Kopplung genutzten Komponenten in die Überwachungssysteme der jeweiligen Partner integriert und das Verhalten der Komponenten protokolliert werden, um sie kontinuierlich auf anormales Verhalten zu überwachen. Das beinhaltet mindestens die folgenden Punkte:

- Überwachung, in welchem Zustand die Komponenten sind (z.B. An oder Aus).
- Überwachung der Auslastung der Komponenten sowie Datenübertragungsraten und Vergleich mit den dokumentierten Werten aus 2.3 *Dokumentation der Systemkopplung.*
- Protokollierung von sicherheitsrelevanten Ereignissen wie z.B. Änderung von Parametrierungen und Konfigurationen.

Wenn vorhanden, sollten die Protokolle in vorhandene Systeme zur Anomalieerkennung (z.B. SIEM) eingebunden werden. Ist dies technisch nicht möglich, sollten die Protokolle regelmäßig, z.B. monatlich, manuell geprüft werden. Die Protokolle müssen dabei gegen unbefugte Veränderungen geschützt sein und sollten in die Protokollierungsumgebung der jeweiligen Betreiber eingebunden sein.

Automatisierte Überwachungssoftware sollte dabei so konfiguriert sein, dass sie Warnmeldungen auf der Grundlage vordefinierter Schwellenwerte erzeugt. Das Warnsystem sollte auf die Ausgangsbasis (vgl. Auflistung unter ISO/IEC 27002:2022 8.16 Überwachung von Aktivitäten auf Seite 143) der Organisation abgestimmt und optimiert werden, um Fehlalarme zu minimieren.

Weiterhin werden die folgenden Punkte empfohlen:

- Überwachung der Inhalte des Netzwerkverkehrs auf Anomalien und Einbindung in ein Intrusion Detection bzw. Intrusion Prevention System. Wenn die Verschlüsselung dem entgegenspricht, darf in Abhängigkeit von der Sensibilität der ausgetauschten Daten nach Einigung der Partner auf eine Verschlüsselung auf Transport-/Applikationsebene verzichtet werden (z.B. durch Verwendung von NULL-Ciphern), vgl. 3.3 *Kryptographische Methoden.* In diesem Fall muss die Prüfung der Integrität der Nachrichten und die gegenseitige Authentifizierung weiterhin gewährleistet sein.
- Meldung von ungewöhnlichen Ereignissen an den Partner. In diesem Fall sollten sich die Partner bezüglich des Meldeprozesses abstimmen und im Realisierungskonzept festhalten, vgl. 2.2 *Realisierungskonzept der Systemkopplung*. Der Meldeweg sollte jeweils dokumentiert werden, vgl. 2.3 *Dokumentation der Systemkopplung*.

3.6 Fernzugang

Schnittstellen von Systemkopplungen sollen vom jeweiligen Betreiber aus der Ferne deaktivierbar bzw. aktivierbar sein.

Anhang:

- Mapping Netz- und Informationssystemsicherheitsverordnung
- Checkliste für Systemkopplungen

A. Anhang

A.1 Mapping Netz- und Informationssystemsicherheitsverordnung

In der folgenden Tabelle ist ein Mapping von den Sicherheitsmaßnahmen der 215. Verordnung: Netz- und Informationssystemsicherheitsverordnung – NISV vom 17. Juli 2019 zu den jeweiligen Abschnitten dieses Leitfadens dargestellt.

Tabelle 2: Mapping der .Sicherheitsmaßnahmen der Netz- und Informationssystemsicherheitsverordnung – NISV zu den relevanten Abschnitten dieses Dokuments.

Sicherheitsmaßnahmen der NISV	Abschnitte im Leitfaden
1. Governance und Risikomanagement	
1.1. Risikoanalyse	2.4
1.2. Sicherheitsrichtlinie	
1.3. Überprüfungsplan der Netz- und Informationssysteme	2.2, 2.3, 2.6
1.4. Ressourcenmanagement	2.5
1.5. Informationssicherheitsmanagementsystemprüfung	
1.6. Personalwesen	2.5
2. Umgang mit Dienstleistern, Lieferanten und Dritten	
2.1. Beziehungen mit Dienstleistern, Lieferanten und Dritten	2.1, 2.2, 2.3
2.2. Leistungsvereinbarungen mit Dienstleistern und Lieferanten	2.1, 2.2, 2.3
3. Sicherheitsarchitektur	
3.1. Systemkonfiguration	2.3, 3.2, 3.4
3.2. Vermögenswerte	
3.3. Netzwerksegmentierung	2.2, 2.3, 3.1
3.4. Netzwerksicherheit	3.1, 3.2
3.5. Kryptographie	3.3
4. Systemadministration	
4.1. Administrative Zugangsrechte	
4.2. Systeme und Anwendungen zur Systemadministration	3.2
5. Identitäts- und Zugriffsmanagement	
5.1. Identifikation und Authentifikation	
5.2. Autorisierung	
6. Systemwartung und Betrieb	
6.1. Systemwartung und Betrieb	
6.2. Fernzugriff	
7. Physische Sicherheit	
7.1. Physische Sicherheit	
8. Erkennung von Vorfällen	
8.1. Erkennung	3.5
8.2. Protokollierung und Monitoring	3.5
8.3. Korrelation und Analyse	3.5
9. Bewältigung von Vorfällen	
9.1. Vorfallsreaktion	2.4
9.2. Vorfallsmeldung	2.4
9.3. Vorfallsanalyse	2.4
10. Betriebskontinuität	
10.1. Betriebskontinuitätsmanagement	2.1, 2.4
10.2. Notfallmanagement	2.4, 2.5
11. Krisenmanagement	
11.1. Krisenmanagement	2.4

A.2 Checkliste für Systemkopplungen

Die folgende Checkliste listet Schwerpunkte der o.g. Anforderungen auf. Sie enthält nicht alle beschriebenen Maßnahmen, so dass sie **nicht zur Vollständigkeitsprüfung der Umsetzung der Anforderungen genutzt werden kann**. Sie bietet lediglich einen **Überblick über die wichtigsten Maßnahmen**.

Betreiber des Leit-/Fernwirkgeräts:	***<Partner1>***
Systemkopplung von:	***<Standort1>* zu: *<Partner2><Standort2>***
Fernwirk-Protokoll	***<z.B. IEC60870-5-101>***

2	**Organisatorische Maßnahmen**	
2.1	**Vereinbarung zur Systemkopplung**	
	Es liegt eine zwischen den Partnern abgestimmte Vereinbarung gemäß Abschnitt 2.1 vor.	□
	Alle in diesem Abschnitt genannten Informationen sind in der Vereinbarung enthalten.	□
2.2	**Realisierungskonzept der Systemkopplung**	
	Es liegt ein Realisierungskonzept gemäß Abschnitt 2.2 vor.	□
	Alle in diesem Abschnitt genannten Informationen sind in der Vereinbarung enthalten.	□
	Das Realisierungskonzept wird zyklisch – z.B. jährlich – auf Aktualität überprüft.	□
2.3	**Dokumentation der Systemkopplung**	
	Es liegt eine Dokumentation der Umsetzung gemäß Abschnitt 2.3 vor.	□
	Alle in diesem Abschnitt genannten Informationen sind in der Vereinbarung enthalten.	□
	Die für die Systemkopplung zuständigen Leit- und Fernwirktechniker haben Zugriff auf die Dokumentation.	□
	Die Dokumentation wird zyklisch – z.B. jährlich – auf Aktualität überprüft.	□
2.4	**Incident Management**	
	Basierend auf der Bewertung der Kritikalität der Kopplung ist der Ablauf, wie leit- und fernwirktechnische Störungen größeren Ausmaßes behandelt werden, im Notfall- bzw. Krisenmanagement-Prozess beschrieben.	□
	Notfallpläne sind für als kritisch eingestufte Kopplungen erstellt.	□
	Die benötigten technischen und personellen Ressourcen für die Notfallmaßnahmen sind vorhanden.	□
2.5	**Schulung**	
	Zuständige Personen werden regelmäßig gemäß Abschnitt 2.5 geschult.	□
2.6	**Abnahme und Inbetriebnahmeprüfung**.	
	Vor der Inbetriebnahme und nach signifikanten Änderungen findet eine Prüfung gemäß Abschnitt 2.6 statt.	□
3	**Technische Maßnahmen**	
	Die Einhaltung der Maßnahmen wird zyklisch, z.B. jährlich, überprüft.	□
3.1	**Netzwerksegmentierung**	
	Wo möglich ist die Kopplung in einer DMZ-Struktur realisiert.	□
	Wo technisch möglich beschränken filternde Komponenten den Zugang zum eigenen Netzwerk. Andernfalls werden zumindest Filterfunktionen der Kopplungskomponenten verwendet, wenn vorhanden.	□
	Maßnahmen gegen das uneingeschränkte Anfordern von Ressourcen sind implementiert.	□
3.2	**Zugelassener Datenverkehr und sichere Protokolle**	
	Es werden ausschließlich die vereinbarten Protokolle verwendet und die vereinbarten Typkennungen und Datenpunkte über die vereinbarten Ports ausgetauscht.	□
	Für IEC 60870-5-101/-104 werden die in Abschnitt 3.2 beschriebenen Anforderungen umgesetzt.	□
	Eine Fernparametrierung von Seiten des Partners auf die Schnittstelle der Kopplung ist nicht möglich.	□

	Schnittstellen zur Administration werden über das interne bzw. Management-Interface realisiert.	□
	Der Datenaustausch mit dem Partner geschieht ausschließlich über das externe Interface.	□
	Für die Administration werden ausschließlich sichere Protokolle gemäß Abschnitt 3.2 verwendet.	□
3.3	**Kryptographische Methoden**	
	Sicherheitserhöhende Einstellungen der Protokolle sind aktiviert und etwaige kryptographische Erweiterungen werden eingesetzt.	□
	Der Schutz vor Replay Angriffen gemäß Abschnitt 3.3 ist umgesetzt.	□
	Kryptographische Verfahren und Schlüsselmindestlängen entsprechen dem Stand der Technik.	□
	Falls digitale Zertifikate genutzt werden, sind PKIs etabliert.	□
	Die Anforderungen an die Schlüsselverwaltung gemäß Abschnitt 3.3 sind umgesetzt.	□
	Gegenseitige Authentifizierung, Integritätsprüfung und Verschlüsselung werden gemäß Tabelle 1 umgesetzt.	□
3.4	**Härtung**	
	Alle Komponenten sind gemäß Abschnitt 3.4 gehärtet und mit aktuellem Schadsoftwareschutz versehen.	□
	Nur die für die Kopplung benötigten Funktionen sind aktiviert.	□
	Die sichere Grundkonfiguration und die durchgeführten Härtungsmaßnahmen sind dokumentiert.	□
3.5	**Monitoring der Systemkomponenten und Perimeterüberwachung**	
	Die aktuellen Konfigurationen und Parametrierunten werden gemäß Abschnitt 3.5 überwacht.	□
	Die genutzten Komponenten sind in die Überwachungssysteme integriert und werden auf anormales Verhalten überwacht.	□
3.6	**Fernzugang**	
	Die Schnittstellen von Systemkopplungen können aus der Ferne deaktiviert und aktiviert werden.	□