A PHOENIX CONTACT COMPANY

Cybersicherheit

Konformitätserklärung BDEW-Whitepaper

Inhaltsverzeichnis

Einführung und Übersicht

Einführung

Die vorliegende Konformitätserklärung beschreibt die Konformität gegenüber dem Dokument „Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“ von Oesterreichs Energie und BDEW[1] (nachfolgend BDEW-Whitepaper genannt). Diese gilt für folgende Produkte:

- DIGICOM Version 7.0.0 oder höher
- KOMBISAVE ab Firmware-Version 3.00
- KOMBISAVE+ RN, RF, RQ und RL ab Firmware-Version 3.00
- POWERSAVE RN und RF ab Firmware-Version 2.00

Übersicht

Nachfolgende Kapitel sind gleich Aufgebaut wie Kapitel 4 des BDEW-Whitepapers. Als erstes sind jeweils die Kapitelnummer und der Originaltext aus dem BDEW-Whitepaper zitiert. Danach folgt die Konformitätserklärung der NSE AG.

[1] Oesterreichs Energie und BDEW (V2 vom 08.05.2018): *Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme.* Wien / Berlin: Oesterreichs E-Wirtschaft / BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Sicherheitsanforderungen

Sichere Systemarchitektur

BDEW 4.1.1 ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 13.1.3, 14.2.5, 14.2.7, 17.2.1

Die Einzelkomponenten und das Gesamtsystem müssen auf einen sicheren Betrieb hin entworfen und entwickelt werden. Zu den Prinzipen eines sicheren Systemdesigns gehören:

Security-By-Design: Das Gesamtsystem und seine Einzelkomponenten sind von Grund auf im Hinblick auf Sicherheit entwickelt. Vorsätzliche Angriffe und unberechtigte Handlungen werden explizit betrachtet, die Auswirkungen von Sicherheitsvorfällen werden durch das Systemdesign minimiert.

Minimal-Need-To-Know-Prinzip: Jede Komponente und jeder Benutzer erhält nur die Rechte, die für die Ausführung einer Aktion notwendig sind. So werden z.B. Anwendungen und Netzwerk-Dienste nicht mit Administratorprivilegien, sondern nur mit den minimal nötigen Systemrechten betrieben.

Defence-In-Depth Prinzip: Sicherheitsrisiken werden nicht durch einzelne Schutzmaßnahmen angegangen, sondern durch die Implementierung gestaffelter, auf mehreren Ebenen ansetzender und sich ergänzender Sicherheitsmaßnahmen begrenzt.

Redundanz-Prinzip: Das Gesamtsystem ist so ausgelegt, dass der Ausfall einzelner Komponenten die sicherheitsrelevanten Funktionen nicht beeinträchtigt. Das Systemdesign verringert die Wahrscheinlichkeit und die Auswirkungen von Problemen, die durch das uneingeschränkte Anfordern von Systemressourcen, wie z.B. Arbeitsspeicher oder Netzwerkbandbreite entstehen (sog. Resource-Consumption oder DoS-Angriffe).

NSE AG SAVE-Schutzgeräte und das Bedienprogramm DIGICOM ermöglichen die Realisierung von Systemen, die sicher betrieben werden können. Beachten Sie hierzu auch die Erläuterungen im Funktionshandbuch Kapitel 50 Cybersicherheit.

Patchfähigkeit und Patch-Management

BDEW 4.1.2 ISO/IEC 27002:2013 / 27019:2017:12.6.1

Alle Systemkomponenten müssen patchfähig sein. Der Auftragnehmer muss einen Patch-Managementprozess für die Einzelkomponenten und das Gesamtsystem unterstützen, anhand dessen das Testen, Installieren und Dokumentieren von Sicherheits-Patches und Updates gesteuert und verwaltet werden kann. Sicherheits-Patches und Updates müssen durch den Betreiber selbst bzw. durch vom ihm beauftragte Dienstleister installiert werden können. Das Installieren bzw. Deinstallieren von Patches muss vom Betreiber autorisiert werden und darf nicht automatisch geschehen. Die Installation bzw. Deinstallation ist im System nachvollziehbar und manipulationsgeschützt zu protokollieren. Die Integrität von Sicherheits-Patches und Updates muss durch einen kryptographischen Mechanismus prüfbar sein.

NSE AG Updates für alle Systemkomponenten können vom Betreiber installiert werden. Alle Installationsvorgänge werden in den Sicherheitsmeldungen protokolliert. Es können nur von NSE signierte Updatepakete installiert werden.

Bereitstellung von Sicherheits-Patches für alle Systemkomponenten

BDEW 4.1.3	ISO/IEC 27002:2013 / 27019:2017:12.5.1, 12.6.1 Der Auftragnehmer muss gewährleisten, dass Sicherheitsupdates für alle Systemkomponenten während des gesamten, vertraglich geregelten Betriebszeitraums zur Verfügung stehen. Updates von Basiskomponenten, die nicht vom Auftragnehmer entwickelt wurden, wie z.B. Betriebssystem, Bibliotheken oder Datenbank-Managementsystem, muss der Auftragnehmer von den jeweiligen Herstellern beziehen, diese testen und sie gegebenenfalls an den Auftraggeber weiterleiten. Test, Freigabe und Bereitstellung der Updates müssen innerhalb eines angemessenen, vertraglich geregelten Zeitrahmens erfolgen.
NSE AG	Sicherheitsupdates werden intern geprüft, freigegeben und auf der Webseite veröffentlicht. Die Installation liegt in der Verantwortung des Auftraggebers. Die Vertragsdauer beträgt standardmässig zwei Jahre, kann aber auch individuell mit dem Auftraggeber vereinbart werden. Auf den Geräten wird die Vertragsdauer mit der Wartungsdatei hinterlegt. Beachten Sie bezüglich Wartungsdatei auch das Funktionshandbuch Kapitel 50 Cybersicherheit hinterlegt.

Support für eingesetzte Systemkomponenten

BDEW 4.1.4	ISO/IEC 27002:2013 / 27019:2017:12.6.1, 14.2.7 Der Auftragnehmer muss sicherstellen, dass sowohl für von ihm eigenentwickelte als auch für fremdentwickelte Systemkomponenten (z.B. Betriebssystem, Datenbank-Managementsystem, etc.) innerhalb des geplanten und vertraglich festgeschriebenen Betriebszeitraums Herstellersupport und Sicherheitsupdates zur Verfügung stehen. Das Abkündigungsverfahren und alle relevanten Mindestlaufzeiten wie z.B. Last-Customer-Shipping und End-Of-Support müssen verbindlich festgeschrieben werden.
NSE AG	Sicherheitsupdates und entsprechende Informationen werden auf der Webseite veröffentlicht. Abkündigungsverfahren, Last-Customer-Shipping sowie End-Of-Support sind definiert und festgeschrieben.

Verschlüsselung vertraulicher Daten

BDEW 4.1.5	ISO/IEC 27002:2013 / 27019:2017:10.1.1, 12.4.2, 13.1.2, 18.1.3, 18.1.4 Vertrauliche Daten dürfen nur verschlüsselt gespeichert bzw. übertragen werden.
NSE AG	Vertrauliche Daten werden verschlüsselt gespeichert. Die Kommunikation über die Ethernet-Schnittstellen erfolgt verschlüsselt. Die Kommunikation über USB oder RS-485 erfolgt unverschlüsselt. Beachten Sie hierzu die Erläuterungen im Funktionshandbuch Kapitel 50 Cybersicherheit.

Kryptographische Verfahren

BDEW 4.1.6	ISO/IEC 27002:2013 / 27019:2017:10.1.1, 10.1.2, 13.1.4 ENR, 18.1.5 Bei der Auswahl von kryptographischen Verfahren sind nationale Gesetzgebungen zu berücksichtigen. Es dürfen nur 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.

NSE AG	Die Auswahl der verwendeten kryptographischen Verfahren und Schlüssel orientiert sich an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Sichere Standard-Konfiguration

BDEW 4.1.7	ISO/IEC 27002:2013 / 27019:2017:9.4.4, 12.5.1, 14.3.1 Das Gesamtsystem muss nach der Erstinstallation bzw. bei der (Wieder-) Inbetriebnahme in einem betriebssicheren Zustand konfiguriert sein, wobei diese definierte Grundkonfiguration dokumentiert sein muss. Dienste, Services und Funktionen sowie Daten, die nur zur Entwicklung oder zum Testbetrieb notwendig sind, müssen vor der Auslieferung bzw. vor dem Übergang in den Produktivbetrieb nachweisbar entfernt bzw. dauerhaft deaktiviert werden.

NSE AG	Die Grundkonfiguration erlaubt ausschliesslich Kommunikation über das Bedientableau oder mittels USB-Schnittstelle. Alle anderen Kommunikationsschnittstellen (Ethernet, RS-485) sind standardmässig deaktiviert.

Integritätsprüfung

BDEW 4.1.8	ISO/IEC 27002:2013 / 27019:2017:12.5.1, 14.2.1, 14.2.4 Systemdateien, Anwendungen, Konfigurationsdateien und Anwendungs-Parameter müssen auf Integrität überprüft werden können, beispielsweise durch kryptographische Prüfsummen.

NSE AG	Die Integrität der Systemdateien und Anwendungen wird durch kryptographische Verfahren sichergestellt. Die Integrität der Konfigurationsdateien und Anwendungs-Parameter wird durch Prüfsummen gewährleistet.

Nutzung von Cloud-Diensten

BDEW 4.1.9	ISO/IEC 27002:2013 / 27019:2017: 15.1.1, 15.1.2, 15.2.1 Bei der Nutzung von Cloud-Diensten sind die folgenden Anforderungen zu berücksichtigen: a) Mit dem Cloud-Dienstleister müssen Vereinbarungen getroffen werden, welche sicherheitsrelevante Prozesse für den Betrieb der Cloud-Infrastruktur regeln. b) Funktionen zur Steuerung kritischer Infrastrukturen, deren Manipulation/Veränderung die Energieversorgung gefährden kann, dürfen nicht in externen Cloud-Diensten realisiert werden. c) Der Ausfall eines Cloud-Dienstes bzw. des Zugriffs auf diesen Dienst darf zu keinen wesentlichen Einschränkungen der definierten Grundfunktion des Systems führen. Störungen und Ausfälle des Cloud-Dienstes müssen auch in der Notfallkonzeption und Wiederanlaufplanung berücksichtigt werden (siehe 4.8.2).
NSE AG	Diese Anforderung ist für die vorliegende Konformitätserklärung nicht relevant, da keine Cloud-Dienste verwendet werden.

Anforderungen an die Dokumentation

BDEW 4.1.10	ISO/IEC 27002:2013 / 27019:2017:7.2.2, 12.1.1, 14.1.1, 14.2.7 Dem Auftraggeber muss spätestens zur Abnahme eine projektspezifische Dokumentation übergeben werden. Für Einzelkomponenten und Gesamtsysteme muss eine Beschreibung aller sicherheitsrelevanten Systemeinstellungen und Parameter sowie ihrer Standardwerte enthalten sein. Außerdem werden sicherheitsspezifische Implementierungsdetails aufgelistet und kurz beschrieben (z.B. verwendete kryptographische Verfahren). Für ein Gesamtsystem sind zusätzlich Informationen über die Systemarchitektur zu dokumentieren. Dies umfasst den grundsätzlichen Aufbau des Systems und die Interaktionen aller beteiligten Komponenten. In dieser Dokumentation wird besonders auf die sicherheitsrelevanten oder schützenswerten Systemkomponenten sowie ihre gegenseitigen Abhängigkeiten und Interaktionen eingegangen.
NSE AG	Die Dokumentation erfolgt über Geräte- und Funktionenhandbücher.

Projektorganisation

Ansprechpartner

BDEW 4.2.1	ISO/IEC 27002:2013 / 27019:2017:6.1.1, 6.1.5, 15.1.2 Der Auftragnehmer muss einen Ansprechpartner definieren, der während der Angebotsphase, der System-Entwicklung und während des geplanten Betriebs-und Wartungszeitraumes für den Bereich der IT-Sicherheit verantwortlich ist.
NSE AG	Der Ansprechpartner für den Bereich der IT-Sicherheit und sein Stellvertreter sind in der Abteilung F&E der NSE AGpositioniert.

Sicherheits- und Abnahmetests

BDEW 4.2.2	ISO/IEC 27002:2013 / 27019:2017:14.2.7, 14.2.8, 14.2.9, 15.2.1 Die einzelnen Systemkomponenten und die wesentlichen Funktionen des Gesamtsystems müssen in einer repräsentativen Konfiguration vor der Auslieferung vom Auftragnehmer durch eine vom Entwicklungsteam unabhängige Organisationseinheit einem Sicherheits- und Stresstest unterzogen werden. Die Vorgehensweise ist mit dem Auftraggeber abzustimmen. Die Ergebnisse der Tests sowie die dazugehörige Dokumentation (Softwarestände, Prüfkonfiguration, etc.) werden dem Auftraggeber zur Verfügung gestellt. Zusätzlich hat der Auftraggeber das Recht, diese Tests auch selbst vorzunehmen oder durch einen externen Dienstleister durchführen zu lassen. Art und Umfang der Abnahmetests werden durch den Auftraggeber festgelegt. Dem Auftraggeber bzw. dem von ihm Beauftragten ist für die Prüfungen ein Systemzugriff mit den technisch maximal möglichen Zugriffsrechten einzuräumen.
NSE AG	Die einzelnen Systemkomponenten respektive die wesentlichen Funktionen des Gesamtsystems werden vor der Auslieferung nach definierten Vorgaben geprüft.

Sichere Datenspeicherung und Übertragung

BDEW 4.2.3	ISO/IEC 27002:2013 / 27019:2017:6.2.1, 8.3.3, 10.1.1, 13.2.2, 13.2.3, 13.2.4, 14.3.1 Vertrauliche Daten des Auftraggebers, die im Entwicklungs- und Wartungsprozess benötigt werden oder anfallen, dürfen über ungeschützte Verbindungen nur verschlüsselt übertragen werden. Bei einer Speicherung auf mobilen Datenträgern oder Systemen dürfen solche Daten nur verschlüsselt gespeichert werden. Die Menge und die Dauer der Aufbewahrung der gespeicherten Daten müssen auf ein vertraglich festzulegendes Minimum beschränkt sein.
NSE AG	Da kein direkter Auftraggeber vorhanden ist, der vertrauliche Daten übermittelt, ist diese Anforderung für die vorliegende Konformitätserklärung nicht relevant.

Übergabe projektspezifischer Anpassungen

BDEW 4.2.4	ISO/IEC 27002:2013 / 27019:2017:14.2.7 Bei Individualprojekten und bei projekt- bzw. kundenspezifischen Erweiterungen, Anpassungen und Engineering-Dienstleistungen müssen alle projektspezifischen Parametrierungen, Änderungen und Anpassungen dem Auftraggeber vollständig und umfassend dokumentiert ausgehändigt werden.
NSE AG	Diese Anforderung ist für die vorliegende Konformitätserklärung nicht relevant.

Basissystem

Grundsicherung und Systemhärtung

BDEW 4.3.1	ISO/IEC 27002:2013 / 27019:2017:9.4.4, 12.6.2, 13.1.2, 14.2.4, 14.2.10 ENR Alle Komponenten des Basissystems müssen anhand anerkannter Best-Practice-Guides dauerhaft gehärtet und mit aktuellen Service-Packs und Sicherheits-Patches versehen sein. Unnötige Benutzer, Default User, Programme, Netzwerkprotokolle, Dienste und Services müssen deinstalliert, oder – falls eine Deinstallation nicht möglich ist – dauerhaft deaktiviert und gegen versehentliches Reaktivieren geschützt werden. Die sichere Grundkonfiguration des Gesamtsystems muss überprüft und dokumentiert sein.
NSE AG	Alle Komponenten des Basissystems sind, gemäss Ausführungen zu den allgemeinen Anforderungen (Kapitel 4.1 BDEW) und wie im Funktionshandbuch Kapitel 50 Cybersicherheit beschrieben, gehärtet.

Schadsoftware-Schutz

BDEW 4.3.2	ISO/IEC 27002:2013 / 27019:2017:12.2.1 Alle vernetzten Systeme müssen an geeigneter Stelle mit einem Schadsoftware-Schutz versehen sein. Alternativ zum Einsatz eines Schadsoftware-Schutzes auf allen Systemkomponenten ist vom Auftragnehmer ein umfassendes Schadsoftware-Schutzkonzept vorzulegen, das einen gleichwertigen Schutz bietet. Sofern eine Pattern-basierte Lösung eingesetzt werden soll, muss eine automatische und zeitnahe Aktualisierung der Pattern-Dateien möglich sein. Dabei darf keine direkte Verbindung mit Updateservern in externen Netzen wie dem Internet benutzt werden. Der Zeitpunkt der Aktualisierung auf den Endsystemen muss konfigurierbar sein.
NSE AG	Der Einsatz von Antiviren-Software ist nicht erforderlich, da nur vollständige und signierte Updatepakete installiert werden können. Dadurch wird verhindert, dass Schadsoftware auf dem Gerät installiert und ausgeführt werden kann.

Autonome Benutzerauthentifizierung

BDEW 4.3.3	ISO/IEC 27002:2013 / 27019:2017:9.2.1, 9.2.2, 9.4.2 Die zur Nutzeridentifizierung und -authentifizierung notwendigen Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden.
NSE AG	Zurzeit werden die Daten zur Nutzeridentifizierung und -authentifizierung im Gerät hinterlegt. Meldet sich ein Benutzer an, werden keine Daten von ausserhalb des Prozessnetzes bezogen. Damit ist diese Anforderung erfüllt.

Virtualisierungstechnologien

BDEW 4.3.4 ISO/IEC 27002:2013 / 27019:2017: 12.1.3, 12.3.1, 12.6.1, 13.1.3, 17.2.1

Bei der Nutzung von Virtualisierungstechnologien sind die folgende Anforderungen zu berücksichtigen:

a) Virtualisierte Komponenten, die unterschiedlichen Sicherheits- oder Vertrauenszonen zugeordnet sind (z.B. interne Komponenten und DMZ-Komponenten), dürfen nicht auf denselben Virtualisierungsservern betrieben werden. Die Netzwerksegmentierung von separierten Sicherheitszonen darf nicht über die Virtualisierungsserver umgangen werden können.

b) Die für Verwaltungs- und Administrationsdienste sowie die für die Datenspeicherung der Virtualisierungsinfrastruktur genutzten Netzwerke müssen von weiteren Netzwerken durch Firewalls segmentiert werden, an denen nur die minimal benötigten Netzwerkdienste restriktiv freigeschaltet werden. Der Zugriff auf die Verwaltungs- und Administrationsdienste und die o.g. Netzwerke muss auf Administratoren beschränkt werden.

c) Die Virtualisierungsschicht, die Verwaltungs- und Administrationsschnittstellen und die zugehörige Infrastruktur müssen gemäß Hersteller-Empfehlungen einheitlich konfiguriert, gesichert und gehärtet so wie im Patch-Management und im Datensicherungskonzept berücksichtigt werden.

d) Die Virtualisierungsserver müssen über hinreichende Ressourcen für den Betrieb aller auf ihnen betriebenen virtualisierten Komponenten verfügen. Dies gilt insbesondere auch für Betriebssituationen unter erhöhter Last.

e) Der Ausfall von Virtualisierungsservern oder sonstigen Komponenten der Virtualisierungsinfrastruktur darf keine negativen Auswirkungen auf die definierten Verfügbarkeitsanforderungen haben. Störungen und Ausfälle der Virtualisierungsumgebung müssen auch in der Notfallkonzeption und Wiederanlaufplanung berücksichtigt werden (siehe 4.8.2)

NSE AG Diese Anforderung ist für die vorliegende Konformitätserklärung nicht relevant, da keine Virtualisierungstechnologien eingesetzt werden.

Netzwerk und Kommunikation

Eingesetzte Protokolle und Technologien

BDEW 4.4.1 ISO/IEC 27002:2013 / 27019:2017:9.4.1, 9.4.2, 10.1.1, 10.1.2, 12.9.1 ENR, 13.1.1, 13.1.2, 13.1.3, 13.1.4 ENR

a) Wo technisch möglich, dürfen generell nur sichere Kommunikationsstandards und Protokolle benutzt werden, die Integritätsüberprüfung, Authentifizierung und ggf. Verschlüsselung bieten. Für Protokolle zur Remote-Administration und Parametrierung ist dies zwingend umzusetzen. Bei nicht standardkonformen bzw. proprietären Protokollen sind die genannten Punkte ebenfalls zu berücksichtigen.

b) Das Gesamtsystem und jede dazugehörige Netzwerkkomponente müssen sich in die Netzwerk-Konzeption des Gesamtunternehmens einbinden lassen. Relevante Netzwerk-Konfigurationsparameter wie IP-Adressen müssen zentral verwaltet werden können. Zur Administration und zum Monitoring werden sichere Protokolle verwendet, die Integritätsschutz, Authentifizierung und Verschlüsselung gewährleisten. Die Netzwerkkomponenten sind gehärtet, unnötige Dienste und Protokolle sind deaktiviert, Management-Interfaces sind durch ACLs geschützt.

c) Netzwerkkomponenten, die vom Auftragnehmer bereitgestellt werden, müssen in ein zentrales Inventory- und Patch-Management eingebunden werden können.

d) Wo technisch möglich, wird auf WAN-Verbindungen das IP-Protokoll verwendet und unverschlüsselte Applikations-Protokolle durch Verschlüsselung auf den unteren Netzwerkebenen geschützt (z.B. durch TLS-Verschlüsselung oder durch verschlüsselte VPN-Technologie).

e) Beim Einsatz von gemeinsam genutzten Netzwerk-Infrastrukturkomponenten (z.B. bei VLAN-oder MPLS-Technologie) definiert das Netzwerk mit dem höchsten Schutzbedarf die Anforderungen an die Hardware und deren Parametrierung. Eine gleichzeitige Nutzung der Netzwerkkomponenten bei unterschiedlichem Schutzbedarf darf nur vorgenommen werden, wenn eine Herabsetzung des Schutzniveaus oder der Verfügbarkeit durch die Gleichzeitigkeit in keinem Fall möglich ist.

NSE AG Die Sicherheit der verfügbaren Kommunikationsstandards und Protokolle ist gemäss den Ausführungen zu den allgemeinen Anforderungen (Kapitel 4.1 BDEW) und wie im Funktionshandbuch Kapitel 50 Cybersicherheit beschrieben sichergestellt. Bei IEC 61850 sind zurzeit noch keine zusätzlichen Sicherheitsmassnahmen gemäss IEC 62351 umgesetzt.

Sichere Netzwerkstruktur

BDEW 4.4.2 ISO/IEC 27002:2013 / 27019:2017:9.4.1, 12.9.1 ENR,13.1.1, 13.1.2, 13.1.3, 13.1.4 ENR, 13.1.5 ENR

a) Vertikale Netzwerksegmentierung: Soweit anwendbar und technisch möglich, wird die dem System zugrundeliegende Netzwerkstruktur in Zonen mit verschiedenen Funktionen und unterschiedlichem Schutzbedarf aufgeteilt. Wo technisch möglich, werden diese Netzwerk-Zonen durch Firewalls, filternden Router oder Gateways getrennt. Die Kommunikation mit weiteren Netzwerken hat ausschließlich über vom Auftraggeber zugelassene Kommunikationsprotokolle unter Einhaltung der geltenden Sicherheitsregeln zu erfolgen.

b) Horizontale Netzwerksegmentierung: Soweit anwendbar und technisch möglich, wird die dem System zugrundeliegende Netzwerkstruktur auch horizontal in unabhängige Zonen (z.B. nach Standorten) aufgeteilt, wobei die Trennung der Zonen ebenfalls durch Firewalls, filternde Router oder Gateways erfolgen muss.

NSE AG Diese Anforderung liegt in der Verantwortung des Auftraggebers und ist somit nicht relevant für die vorliegende Konformitätserklärung.

Dokumentation der Netzwerkstruktur und -konfiguration

BDEW 4.4.3 ISO/IEC 27002:2013 / 27019:2017:8.1.1

Die Netzwerkkonzeption und -konfiguration, alle physischen, virtuellen und logischen Netzwerkverbindungen und die verwendeten Protokolle, IP-Adressen und Ports sowie die Netzwerk-Perimeter, die Bestandteil des Systems sind bzw. mit ihm interagieren, müssen dokumentiert sein. Änderungen, z.B. durch Updates, werden innerhalb des Change-Managements in die Dokumentation aufgenommen. Die Dokumentation muss Angaben über normale und maximal zu erwartende Datenübertragungsraten enthalten, damit gegebenenfalls auf den Netzwerkkomponenten eine Limitierung der Datenübertragungsraten zur Verkehrssteuerung und Verhinderung von DoS-Problemen implementiert werden kann.

NSE AG Diese Anforderung liegt in der Verantwortung des Auftraggebers und ist somit nicht relevant für die vorliegende Konformitätserklärung.

Sichere Fern-Zugänge

BDEW 4.4.4 ISO/IEC 27002:2013 / 27019:2017:9.1.2, 9.4.1, 9.4.2

a) Administration, Wartung und Konfiguration aller Komponenten muss auch über ein Out-of-Band-Netz, zum Beispiel über lokalen Zugriff, via serielle Schnittstelle, Netzwerk oder direkter Steuerung der Eingabegeräte (KVM), möglich sein.

b) Fern-Zugriff muss über zentral verwaltete Zugangsserver unter der Kontrolle des Systembetreibers durchgeführt werden. Die Zugangsserver müssen in einer DMZ betrieben werden und eine Isolation des Prozessnetzes sicherstellen. Es muss ein 2-Faktor-Authentifizierungsverfahren benutzt werden.

c) Direkte Einwahl-Zugänge in Endgeräte sind grundsätzlich nicht erlaubt.

d) Der Zugriff auf einen Fernzugang muss zentral geloggt werden, wiederholte Fehlversuche werden gemeldet.

e) Alle Fern-Zugangs-Möglichkeiten müssen dokumentiert werden.

NSE AG Diese Anforderung liegt in der Verantwortung des Auftraggebers und ist somit nicht relevant für die vorliegende Konformitätserklärung.

Funktechnologien

BDEW 4.4.5 ISO/IEC 27002:2013 / 27019:2017:10.1.1, 13.1.1, 13.1.2, 13.1.3

Der Einsatz von Nahbereichs-Funktechnologien (z.B. WLAN, Bluetooth, ZigBee, RFID etc.) ist nur nach Analyse der damit verbundenen Risiken und unter Beachtung der nachfolgend beschriebenen Mindestsicherungsmaßnahmen in Abstimmung mit dem Auftraggeber und nach Genehmigung zulässig:

- Drahtlose Übertragungstechnik muss nach dem Stand der Technik abgesichert werden.
- WLANs dürfen nur in dedizierten und durch Firewalls und Applikations-Proxies abgetrennten Netzwerksegmenten betrieben werden.
- WLANs sind so einzurichten, dass bestehende WLANs nicht gestört oder beeinträchtigt werden.

NSE AG Diese Anforderung ist für die vorliegende Konformitätserklärung nicht relevant, da keine Nahbereichs-Funktechnologien eingesetzt werden.

Anwendung

Rollenkonzepte

BDEW 4.5.1 ISO/IEC 27002:2013 / 27019:2017:6.1.2, 9.2.1, 9.2.3, 9.2.6, 9.4.1

Das Gesamtsystem muss eine granulare Zugriffskontrolle auf Daten und Ressourcen erlauben und muss hierzu über ein Benutzerkonzept verfügen, in dem mindestens folgende Benutzerrollen vorgesehen sind:

- Administrator: Benutzer, der das System installiert, wartet und betreut. Der Administrator hat deshalb u. a. die Berechtigung zur Änderung der Sicherheits- und Systemkonfiguration.
- Bediener: Benutzer, der das System im Rahmen der vorgesehenen Nutzung bedient. Dies beinhaltet auch das Recht zur Änderung von betriebsrelevanten Einstellungen.
- Read-Only-Nutzer: Benutzer, der den Status des Systems abrufen und definierte Betriebsdaten lesen darf, aber nicht berechtigt ist, Änderungen durchzuführen.

Die Standard-Zugriffsrechte müssen einer sicheren Systemkonfiguration entsprechen.

	Sicherheitsrelevante Systemeinstellungen und Konfigurationswerte dürfen nur von der Administrator-Rolle gelesen und geändert werden können. Zur normalen Systemnutzung sind nur Bediener- oder Read-Only-Nutzer-Rechte notwendig. Benutzer-Accounts müssen einzeln deaktiviert werden können, ohne sie vom System entfernen zu müssen.

NSE AG Das Rollenkonzept ist wie gefordert umgesetzt. Die Umsetzung ist im Funktionshandbuch Kapitel 50 Cybersicherheit beschrieben.

Benutzer-Authentifizierung und Anmeldung

BDEW 4.5.2	ISO/IEC 27002:2013 / 27019:2017:9.3.1, 9.4.2, 9.2.1, 9.2.2, 9.4.3, 12.4.1 Die Anwendung muss eine personenspezifische Identifizierung und Authentifizierung vornehmen, Gruppen-Accounts werden von Auftraggeber nur in genau spezifizierten Ausnahmefällen erlaubt. a) Ohne erfolgreiche Benutzer-Authentifizierung darf das System nur genau definierte Aktionen erlauben. b) Das System muss eine Passwort-Policy unterstützten, welche dem Stand der Technik entspricht. c) Wo technisch möglich, wird eine starke 2-Faktor-Authentifizierung verwendet, z.B. durch die Verwendung von Tokens oder SmartCards. d) Die zur Nutzeridentifizierung und Authentifizierung benötigten Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden (siehe auch 4.3.3). e) Erfolgreiche und fehlgeschlagene Anmeldeversuche müssen zentral geloggt werden, fehlgeschlagene Anmeldeversuche müssen zentral alarmiert werden können.

NSE AG Die Anforderungen an die Benutzeridentifizierung und die Authentifizierung wurden wie gefordert umgesetzt und sind im Funktionshandbuch Kapitel 50 Cybersicherheit beschrieben (insbesondere durch die Abschnitte „Sicherheitsmeldungen“ und „Fehlversuche beim Anmelden“).

Autorisierung von Aktionen auf Benutzer- und Systemebene

BDEW 4.5.3	ISO/IEC 27002:2013 / 27019:2017:9.4.1, 9.4.4 Vor bestimmten sicherheitsrelevanten/-kritischen Aktionen muss die Autorisierung des anfordernden Benutzers bzw. der anfordernden Systemkomponente überprüft werden. Zu den relevanten Aktionen können auch das Auslesen von Prozess-Datenpunkten oder Konfigurationsparametern gehören.
Ergänzungen und Anmerkungen	Die hier angeführten sicherheitsrelevanten/-kritischen Aktionen sind vom Auftraggeber/Betreiber der Systeme im Einzelnen zu spezifizieren. Diese Aktionen sind dann auch mit der Angabe der Benutzerkennung zentral zu loggen.
Sekundär-, Automatisierungs- und Fernwirk-technik	Für Schutz- und Stationsleittechnik in der Regel nicht notwendig, eine Anwendung sollte durch den Auftraggeber/Betreiber geprüft werden.

NSE AG Diese Anforderung ist für die vorliegende Konformitätserklärung nicht relevant.

Web-Applikationen und Web-Services

BDEW 4.5.4	ISO/IEC 27002:2013 / 27019:2017:14.2.5 Für Web-Applikationen, Web-Schnittstellen und Web-Services sind die Empfehlungen der OWASP TOP 10 und des OWASP Application Security Verification Standard Projekte sowie des BSI-Leitfadens zur Entwicklung sicherer Webanwendungen zu berücksichtigen. Abweichungen sind zu begründen und vom Auftraggeber vorab zu genehmigen.

NSE AG Diese Anforderung ist für die vorliegende Konformitätserklärung nicht relevant, da keine Web-Applikationen und Web-Services eingesetzt werden.

Integritätsprüfung

BDEW 4.5.5	ISO/IEC 27002:2013 / 27019:2017:14.2.5 Die Integrität von Daten, die in sicherheitsrelevanten Aktionen verarbeitet werden, muss vor der Verarbeitung überprüft werden (beispielsweise auf Plausibilität, korrekte Syntax und Wertebereich).

NSE AG Sowohl im Konfigurationstool als auch im Gerät werden die Plausibilität und der Wertebereich geprüft. Die Integrität bei der Übertragung der Daten zum Gerät ist gewährleistet. Zudem wird auf dem Gerät die Integrität der Daten zyklisch geprüft.

Logging

BDEW 4.5.6	ISO/IEC 27002:2013 / 27019:2017:12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3 a) Das Gesamtsystem muss über eine einheitliche Systemzeit verfügen und die Möglichkeit zur Synchronisation dieser Systemzeit mit einer externen, gesicherten Zeitquelle bieten. b) Das System muss Benutzeraktionen sowie sicherheitsrelevante Aktionen, Vorkommnisse und Fehler in einem zur nachträglichen und zentralen Auswertung geeignetem Format protokollieren. Es werden Datum und Uhrzeit, involvierte Benutzer und Systeme sowie das Ereignis und Ergebnis für einen konfigurierbaren Mindestzeitraum aufgezeichnet. c) Die zentrale Speicherung der Logdateien erfolgt an einem frei konfigurierbaren Ort. Ein Mechanismus zur automatisierten Übertragung des Logfiles auf zentrale Komponenten muss zur Verfügung stehen. d) Das Logfile muss gegen spätere Modifikation geschützt sein. e) Bei Überlauf des Logfiles werden die älteren Einträge überschrieben, das System muss bei knapp werdendem Logging-Speicherplatz warnen. f) Es muss möglich sein, sicherheitsrelevante Meldungen in ein vorhandenes Alarm-Management aufzunehmen.

NSE AG Die Zeitsynchronisation ist beispielsweise über NTP möglich. Sicherheitsrelevante Ereignisse werden in den Sicherheitsmeldungen geloggt. Für die Sicherheitsmeldungen ist kein Mindestzeitraum konfigurierbar. Stattdessen werden im Falle eines Überlaufs des Speicherplatzes für die

Sicherheitsmeldungen ältere Einträge überschrieben. Sobald allerdings mehr als 80 % des Speicherplatzes für die Sicherheitsmeldungen mit noch nicht ausgelesenen Einträgen gefüllt ist, kann mithilfe des binären Statussignals ASECBUF eine Warnung gesendet werden. Die Sicherheitsmeldungen auf dem Gerät können nicht manipuliert werden. Die mittels DIGICOM ausgelesene Liste von Sicherheitsmeldungen ist momentan nicht gegen spätere Modifikation geschützt.

Entwicklung

Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse

BDEW 4.6.1 ISO/IEC 27002:2013 / 27019:2017:9.4.5, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, 14.3.1

a) Das System muss beim Auftragnehmer von zuverlässigen und geschulten Mitarbeitern entwickelt werden. Falls die Entwicklung oder Teile davon an einen Subunternehmer ausgelagert werden sollen, bedarf dies der schriftlichen Zustimmung durch den Auftraggeber. An den Unterbeauftragten sind mindestens die gleichen Sicherheitsanforderungen zu stellen wie an den Auftragnehmer.

b) Der Auftragnehmer muss das System nach anerkannten Entwicklungsstandards und Qualitätsmanagement/-sicherungs-Prozessen entwickeln. Im Rahmen des Entwicklungsprozesses müssen insbesondere die folgenden sicherheitsrelevanten Entwicklungsschritte berücksichtigt werden:

- Definition der Sicherheitsanforderungen
- Bedrohungsmodellierung und Risikoanalyse
- Ableitung von Anforderungen an Systemdesign und Implementierung
- Sichere Programmierung
- Anforderungstests
- Sicherheitsprüfungen vor der Inbetriebnahme

c) Das Testen erfolgt nach dem 4-Augen-Prinzip: Entwicklung und Tests werden von verschiedenen Personen durchgeführt. Die Testpläne und -prozeduren sowie erwartete und tatsächliche Testergebnisse müssen dokumentiert und nachvollziehbar sein. Sie können bei Bedarf vom Auftraggeber eingesehen werden.

d) Der Auftragnehmer muss über einen dokumentierten Entwicklungs-Sicherheitsprozess verfügen, der die physische, organisatorische und personelle Sicherheit abdeckt und die Integrität und Vertraulichkeit des Systems schützt. Die Effektivität des o.g. Prozesses kann durch eine externe Auditierung überprüft werden.

e) Der Auftragnehmer muss über eine Programmierrichtlinie verfügen, in der auf sicherheitsrelevante Anforderungen explizit eingegangen wird: So sind z.B. unsichere Programmiertechniken und Funktionen zu vermeiden. Eingabedaten müssen verifiziert werden, um z.B. Pufferüberlauf-Fehler zu verhindern. Wo möglich, werden sicherheitserhöhende Compileroptionen und Bibliotheken benutzt.

f) Die Freigabe des Systems bzw. von Updates/Sicherheits-Patches muss anhand eines spezifizierten und dokumentierten Freigabe-Prozesses stattfinden.

NSE AG SAVE-Schutzgeräte und das Bedienprogramm DIGICOM werden von zuverlässigen, geschulten und hinsichtlich Sicherheit sensibilisierten Mitarbeiten entwickelt. Die Entwicklung erfolgt intern entlang einem Entwicklungsprozess sowie einer Programmierrichtlinie. Tests erfolgen nach dem 4-Augen Prinzip und werden von verschiedenen Personen durchgeführt.

Sichere Entwicklungs- und Test-Systeme, Integritäts-Prüfung

BDEW 4.6.2 ISO/IEC 27002:2013 / 27019:2017:9.4.5, 12.1.4, 14.2.7, 14.3.1

a) Die Entwicklung muss auf sicheren Systemen erfolgen, die Entwicklungsumgebung, Quellcode und Binärdateien müssen gegen fremde Zugriffe gesichert sein. Alle Entwicklungssysteme müssen anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet sein und über einen aktuellen Schadsoftwareschutz verfügen sowie mit allen aktuellen Sicherheits-Patches versehen sein.

b) Entwicklung und Test des Systems sowie von Updates, Erweiterungen und Sicherheits-Patches muss in einer vom Produktivsystem getrennten Test-Umgebung erfolgen.

c) Auf Produktiv-Systemen darf mit Ausnahme von interpretierten Skriptsprachen kein Quellcode gespeichert werden.

d) Es muss möglich sein, die Integrität von Quellcode und Binärdateien auf unerlaubte Veränderungen hin zu überprüfen, beispielsweise durch gesicherte Prüfsummen.

e) Es ist eine Versionshistorie für alle eingesetzte Software zu führen, die es ermöglicht, die durchgeführten Softwareänderungen nachzuvollziehen.

NSE AG Die aufgeführten Anforderungen an sichere Entwicklungs- und Test-Systeme sowie an die Integritätsprüfung werden vollständig erfüllt.

Die Entwicklung erfolgt auf sicheren Systemen. Entwicklungsumgebungen, Quellcodes und Binärdateien sind nach aktuellem Stand der Technik gegen fremde Zugriffe gesichert. Die Versionshistorie wird mittels einer Versionsverwaltungssoftware nachvollziehbar dokumentiert.

Wartung

Anforderung an Wartungsprozesse

BDEW 4.7.1 ISO/IEC 27002:2013 /27019:2017:9.1.2, 9.2.1, 9.2.2, 15.1.1, 15.1.2

a) Der Fern- und Vor-Ort-Zugriff darf nur durch einen definierten und geschulten Personenkreis und nur von abgesicherten Systemen aus erfolgen. Die für den Fern- und Vor-Ort-Zugriff genutzten Zugangs-Systeme und IT-Infrastrukturen müssen anhand anerkannter Best-Practice-Vorgaben und nach aktuellem Stand der Technik gehärtet sein und über einen aktuellen Schadsoftwareschutz verfügen sowie mit allen aktuellen Sicherheits-Patches versehen sein.

b) Durch einen definierten Wartungsprozess muss sichergestellt sein, dass das Wartungspersonal im Rahmen seiner Tätigkeiten nur Zugriff auf die benötigten Systeme, Dienste und Daten und Zutritt zu den entsprechenden Räumlichkeiten erhält.

c) Der interaktive Fern-Zugang muss über personalisierte Accounts und unter Nutzung von 2-Faktor-Authentifizierungerfolgen. Für automatisierte Abläufe sind spezielle Kennungen einzurichten, die nur bestimmte Funktionen ausführen können und die keinen interaktiven Zugang ermöglichen.

d) Es muss technisch sichergestellt sein, dass ein Fern-Zugriff nur erfolgen kann, wenn dieser vom verantwortlichen Betreiber freigegeben wird. Bei externen Dienstleistern müssen die Freigabe und die Trennung für jede Fernzugriffs-Sitzung einzeln erfolgen. Eine Sitzung ist nach Ablauf einer angemessenen Zeit automatisch zu trennen. Insbesondere sind die für den Fernzugriff genutzten Zugangs-Systeme während des Fern-Zugriffs von anderen Netzen logisch oder physisch zu entkoppeln. Eine physische Entkopplung ist der logischen vorzuziehen.

NSE AG Diese Anforderung liegt im Aufgabenbereich des Auftraggebers und ist somit nicht relevant für die vorliegende Konformitätserklärung.

Sichere Updateprozesse

BDEW 4.7.2	ISO/IEC 27002:2013 / 27019:2017:12.5.1, 14.2.2, 14.2.3, 14.2.7, 14.2.9 Die Bereitstellung und Installation von Updates, Erweiterungen und Patches muss nach einem definierten Prozess und nach Rücksprache mit dem Auftraggeber erfolgen.
NSE AG	Der Prozess für die Bereitstellung von Updatepaketen ist definiert.

Konfigurations- und Change-Management, Rollbackmöglichkeiten

BDEW 4.7.3	ISO/IEC 27002:2013 / 27019:2017:12.1.2, 12.5.1, 12.6.2, 12.9.1 ENR, 14.2.2, 14.2.9, a) Das System muss mit einem Konfigurations-und Change-Management entwickelt und betrieben werden. b) Das System muss ein Rollback auf eine festgelegte Anzahl von Konfigurationszuständen unterstützen.
NSE AG	Die Sicherung von Konfigurationen ist über das Bedienprogramm möglich. Ein Rollback auf vorhergehende Firmwareversionen und somit auf vorhergehende Konfigurationen ist möglich. Die Rollbackmöglichkeit besteht für alle Firmewareversionen seit Einführung der Massnahmen zur Umsetzung der Cybersicherheit (Firmwarestände siehe Abschnitt Einführung)**.** Die Archivierung von älteren Konfigurationsversionen hat durch den Auftraggeber/Betreiber zu erfolgen. Vorhergehende Firmware-Stände können über die Webseite oder auf Anfrage bezogen werden. Es wird sichergestellt, dass ältere Konfigurationsversionen auch mit neueren Versionen der Bediensoftware bearbeitet werden können.

Behandlung von Sicherheitslücken

BDEW 4.7.4	ISO/IEC 27002:2013 / 27019:2017:12.6.1, 16.1.2, 16.1.3 Der Auftragnehmer muss über einen dokumentierten Prozess verfügen, um Sicherheitslücken zu behandeln. Innerhalb dieses Prozesses muss es allen Beteiligten, aber auch Außenstehenden möglich sein, tatsächliche oder potentielle Sicherheitslücken zu melden. Außerdem muss sich der Auftragnehmer über aktuelle Sicherheitsprobleme, die das System oder Teilkomponenten betreffen könnten, zeitnah informieren. Der Prozess definiert, wie und in welchem Zeitrahmen eine bekanntgewordene Lücke überprüft, klassifiziert, behoben und an alle betroffenen Kunden mit entsprechenden Maßnahmenempfehlungen weitergemeldet wird. Wenn dem Auftragnehmer eine Sicherheitslücke bekannt wird, muss er den Auftraggeber unter der Maßgabe der Vertraulichkeit zeitnah informieren, auch wenn noch kein Patch zur Behebung des Problems zur Verfügung steht.
NSE AG	Die Überprüfung und Behandlung von Sicherheitslücken erfolgt gemäss einem dokumentierten Prozess und liegt in der Verantwortung des Ansprechpartners für den Bereich der IT-Sicherheit und dessen Stellvertreter (siehe Abschnitt Ansprechpartner). Aussenstehenden ist es möglich, Sicherheitslücken zu melden.

Datensicherung und Notfallplanung

Backup: Konzept, Verfahren, Dokumentation, Tests

BDEW 4.8.1	ISO/IEC 27002:2013 / 27019:2017:12.1.1, 12.3.1 Es müssen dokumentierte und getestete Verfahren zur Datensicherung und -Wiederherstellung der Einzelkomponenten bzw. des Gesamtsystems und der jeweiligen Konfigurationen existieren. Die Konfigurationsparameter von dezentralen Komponenten müssen zentral gesichert werden können. Die Dokumentation und die Verfahren müssen bei relevanten System-Updates angepasst und erneut getestet werden.
NSE AG	Backups der Konfigurationsstände können durch den Auftraggeber mithilfe des Bedienprogrammes DIGICOM erstellt werden. Ausserdem steht auf der NSE-Website ein Archiv mit verschiedenen Firmware-Ständen zur Verfügung.

Notfallkonzeption und Wiederanlaufplanung

BDEW 4.8.2	ISO/IEC 27002:2013 / 27019:2017:17.1.1, 17.2.1 Für relevante Notfall-und Krisenszenarien müssen vom Auftragnehmer dokumentierte und getestete Vorgehensweisen und Wiederanlaufpläne inklusive Angabe der Wiederherstellungszeiten zur Verfügung gestellt werden. Die Dokumentation und Verfahren müssen bei relevanten System-Updates angepasst und im Rahmen des Abnahmeverfahrens für Release-Wechsel erneut getestet werden.
NSE AG	Diese Anforderung liegt im Aufgabenbereich des Auftraggebers und ist somit nicht relevant für die vorliegende Konformitätserklärung.