SIEMENS

SICAM RTUs
SICAM TOOLBOX II

BDEW
Konformitätserklärung

DC0-112-2.04

Document Label:
SICRTUs-HBBDEWCONFORMANCE-GER_V2.04
Ausgabedatum:
02.03.2015

Vorwort

Inhalt des Handbuchs

Diese Konformitätserklärung beschreibt die Konformität der

Produkte

- SICAM RTUs Hard- und Firmware die im Oktober 2011 oder später eine Lieferfreigabe haben (Details siehe *Gültigkeitsbereich*)
- SICAM TOOLBOX II V5.0 oder höher.

mit dem

- *BDEW Whitepaper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme V1.0* vom 10.Juni 2008

Gültigkeitsbereich

Dieses Dokument ist für die Produkte der SICAM RTUs Produktlinie mit Hard- und Firmwareständen ab Oktober 2011 und das SICAM TOOLBOX II Engineering System zu Parametrierung, Diagnose, Simulation, …V5.0 oder höher gültig.

Das sind im Detail:

- SICAM AK
- SICAM TM
- SICAM CMIC
- SICAM EMIC
- SICAM BC
- SICAM TOOLBOX II
  (als Applikation, umfasst weder Hardware noch Betriebssystem oder andere Standardprogramme wie z.B.: Microsoft Office oder Adobe Acrobat Reader)

Hinweis

Das Dokument beschreibt ausschließlich Produkteigenschaften der SICAM RTUs und SICAM TOOLBOX II und keine Systemeigenschaften, wie sie durch anlagenspezifische Vernetzung und Parametrierung der Produkte zu einem Gesamtsystem entstehen.

Die im Dokument beschriebenen Kommentare beziehen sich auf die Bereiche:

- Produktentwicklung
- Produktservice

Nicht abgedeckt werden die Bereiche:

- Systemintegration (Gesamtsystem, bestehend aus einzelnen SICAM RTUs Komponenten und anderen Komponenten wie Netzwerkkomponenten, Schutzgeräte, …)
- Projektplanung / -umsetzung
- Systemservice
- Leitstellenbetrieb / Systembetrieb

Zielgruppe

Dieses Dokument richtet sich vorrangig an Personen in den Bereichen:

- System- und Gerätevertrieb

- Projektplanung- /-Umsetzung
- Systemservice
- Systembetrieb

Verwendete Konventionen

Handbücher, auf die verwiesen wird, sind in Kursivschrift dargestellt, wie z.B. *Gemeinsame Funktionen, System und Basissystemelemente*, Abschnitt *Informationsobjekte*.

Hinweis

Ist eine wichtige Information über das Produkt, die Handhabung des Produktes oder den jeweiligen Teil der Dokumentation, auf den besonders aufmerksam gemacht werden soll.

Inhaltsverzeichnis

1 Einleitung

Inhalt

1.1 Allgemein

Dieses Dokument beschreibt die Konformität der SICAM RTUs und SICAM TOOLBOX II zu den im *BDEW Whitepaper – „Anforderungen an sichere Steuerungs- und Telekommunikationssysteme“* gestellten Sicherheitsanforderungen.

1.2 Zielsetzung

- Leitsysteme inkl. der Subsysteme gegen Sicherheitsbedrohungen im täglichen Betrieb angemessen zu schützen, die Auswirkungen von Bedrohungen auf den Betrieb zu minimieren und die Aufrechterhaltung des Geschäftsbetriebs auch bei Sicherheitsvorfällen sicherzustellen bzw. ein definiertes Mindestmaß an Diensten bzw. Dienstequalität schnellstmöglich wieder herzustellen.
- Diese Systeme auch den sich ändernden Sicherheitsbedrohungen laufend anzupassen, damit sie ausreichend geschützt und das Restrisiko minimiert wird.
- Grundlagen für die Angebotslegung zur Verfügung stellen.

1.3 Anwendungshinweise

Im *Kapitel 2* dieses Dokuments (*BDEW Sicherheitsanforderungen*) ist die Umsetzung der Anforderungen aus dem BDEW Whitepaper beschrieben. Damit der Zusammenhang zwischen den Anforderung aus dem BDEW Whitepaper und deren Umsetzung für die SICAM RTUs einfach zuzuordnen sind, wurden die Kapitelnummern und Namen aus dem BDEW Whitepaper übernommen.

Das heißt zum Beispiel, dass die Umsetzung der BDEW Anforderung 2.4.3 - Anwendungsprotokolle, in diesem Dokument im *Kapitel 2.4.3 Anwendungsprotokolle* beschrieben ist.

Folgende Tabelle gibt eine Übersicht welche Bereiche (Produkt- /Systementwicklung, Projektplanung/ -umsetzung, Produkt- /Systemservice, Leitstellenbetrieb/ Systembetrieb) laut *Oesterreichs Energie und DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE* von den Sicherheitsanforderungen betroffen sind

Nr.	BDEW Sicherheitsanforderung	Produkt- /Systementwicklung	Projektplanung/ -umsetzung	Produkt- /Systemservice	Leitstellenbetrieb/ Systembetrieb
2.1	Allgemeines/Organisation				
2.1.1	Allgemeines				
2.1.1.1	Sichere Systemarchitektur	✓	✓	✓	✓
2.1.1.2	Ansprechpartner	-	✓	✓	✓
2.1.1.3	Patchfähigkeit, Patchmanagement	✓	✓	-	-
2.1.1.4	Bereitstellung von Sicherheitspatches für alle Systemkomponenten	✓	✓	✓	✓
2.1.1.5	Support für eingesetzte Systemkomponenten	✓	✓	✓	✓

Nr.	BDEW Sicherheitsanforderung	Produkt-/Systementwicklung	Projektplanung/-umsetzung	Produkt-/Systemservice	Leitstellenbetrieb/Systembetrieb
2.1.1.6	Verschlüsselung sensibler Daten bei Speicherung und Übertragung	✓	✓	✓	-
2.1.1.7	Verschlüsselungsstandards	✓	✓	-	-
2.1.1.8	Interne/externe Sicherheits- und Anforderungstests und zugehörige Dokumentation	✓	✓	-	-
2.1.1.9	Sichere Standard-Konfiguration und Erstinstallation bzw. (Wieder-) Inbetriebnahme	✓	✓	-	-
2.1.1.10	Integritäts-Prüfung	✓	✓	-	-
2.1.2	Dokumentation				
2.1.2.1	Design-Dokumentation, Beschreibung sicherheitsrelevanter Systemkomponenten und Implementations-Spezifikationen	✓	✓	-	-
2.1.2.2	Administrator- und Benutzer- Dokumentation	✓	✓	-	-
2.1.2.3	Dokumentation sicherheitsrelevanter Einstellungen und Systemmeldungen	✓	✓	-	-
2.1.2.4	Dokumentation der Voraussetzungen und Umgebungs-Anforderungen für den sicheren System-Betrieb	-	✓	-	-
2.2	Bereich Basissystem				
2.2.1	Grundsicherung und Systemhärtung	✓	✓	✓	-
2.2.2	Antiviren-Software	✓	✓	✓	-
2.2.3	Autonome Benutzerauthentifizierung	-	✓	✓	-
2.3	Bereich Netze / Kommunikation				
2.3.1	Sichere Netzwerkkonzeption und Kommunikationsverfahren				
2.3.1.1	Eingesetzte Protokolle und Technologien	✓	✓	-	✓
2.3.1.2	Sichere Netzwerkstruktur	-	✓	✓	✓
2.3.1.3	Dokumentation der Netzwerkstruktur und –konfiguration	-	✓	✓	✓
2.3.2	Sichere Wartungsprozesse und RAS-Zugänge				
2.3.2.1	Sichere Fern-Zugänge	-	-	✓	✓
2.3.2.2	Anforderungen an die Wartungsprozesse	-	-	✓	✓
2.3.3	Funktechnologie: Bedarf und Sicherheitsanforderungen	-	✓	✓	✓
2.4	Bereich Anwendung				
2.4.1	Benutzerverwaltung				
2.4.1.1	Rollenkonzepte	✓	✓	✓	✓
2.4.1.2	Benutzer-Authentifizierung und Anmeldung	✓	✓	✓	✓
2.4.2	Autorisierung von Aktionen auf Benutzer- und Systemebene	-	-	-	✓
2.4.3	Anwendungsprotokolle	✓	✓	✓	✓
2.4.4	Web-Applikationen	✓	-	✓	✓
2.4.5	Integritätsprüfung relevanter Daten	✓	-	✓	✓
2.4.6	Protokollierung, Audit-Trails, Timestamps, Alarmkonzepte	✓	-	✓	✓
2.4.7	Self-Test und System-Verhalten	✓	-	✓	✓

Nr.	BDEW Sicherheitsanforderung	Produkt- /Systementwicklung	Projektplanung/ -umsetzung	Produkt- /Systemservice	Leitstellenbetrieb/ Systembetrieb
2.5	Entwicklung, Test und Rollout				
2.5.1	Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse	✓	-	✓	✓
2.5.2	Sichere Datenhaltung und Übertragung	-	-	✓	-
2.5.3	Sichere Entwicklungs-, Test- und Staging-Systeme, Integritäts- Prüfung	✓	✓	✓	-
2.5.4	Sichere Update- und Wartungsprozesse	✓	✓	✓	-
2.5.5	Konfigurations- und Change- Management, Rollbackmöglichkeiten	✓	✓	✓	-
2.5.6	Behandlung von Sicherheitslücken	-	✓	✓	-
2.5.7	Sourcecode-Hinterlegung	-	✓	-	-
2.6	Datensicherung/-wiederherstellung und Notfallplanung				
2.6.1	Backup: Konzept, Verfahren, Dokumentation, Tests	-	✓	✓	-
2.6.2	Notfallkonzeption und Wiederanlaufplanung	-	✓	✓	-

2 BDEW Sicherheitsanforderungen

Inhalt

2.1 Allgemeines/Organisation

2.1.1 Allgemeines

2.1.1.1 Sichere Systemarchitektur

BDEW 2.1.1.1	*Das Gesamtsystem muss auf einen sicheren Betrieb hin entworfen und entwickelt werden. Zu den Prinzipen eines sicheren Systemdesigns gehören:* ***Minimal-Need-To-Know-Prinzip****: Jede Komponente und jeder Benutzer erhält nur die Rechte, die für die Ausführung einer Aktion nötig 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 System 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).*

SICAM RTUs und SICAM TOOLBOX II unterstützen Techniken zur Realisierung von Systemdesigns die einen sicheren Betrieb des Gesamtsystems gewährleisten.

Hinweis

Info für Projektplanung/-umsetzung:

Als Grundlage für ein sicheres Systemdesign und einen sicheren Systembetrieb sind im Dokument *SICAM RTUs / SICAM TOOLBOX II Administrator Security-Handbuch* unter anderem folgende Informationen enthalten:

- typische Anlagenkonfigurationen
- sichere Grundkonfiguration
- sicherheitsrelevante Systemeinstellungen, Parameter und deren Defaults
- Maßnahmen zur Systemhärtung
- Traffic-Matrix (Kommunikationsschnittstellen)
- Anwendungshinweise für sicherheitsverantwortliches Handeln (Patchmanagement, Virenschutz, Backup / Restore)
- Patchmanagement
- Virenschutz
- Backup / Restore
- Erläuterung von sicherheitsspezifischen Log und Audit-Meldungen; mögliche Ursachen; passende Gegenmaßnahmen

Diese Informationen können als Ausgangsbasis für das sichere Design und den sicheren Betrieb eines Gesamtsystems verwendet werden.

2.1.1.2 Ansprechpartner

BDEW 2.1.1.2	*Der Auftragnehmer muss einen Ansprechpartner definieren, der während der Angebotsphase, der System-Entwicklung und während des geplanten Betriebszeitraumes für den Bereich der IT-Sicherheit verantwortlich ist.*

Hinweis

Diese Anforderung hat keine Relevanz für Produktentwicklung oder Produktservice.

Info für Projektplanung/-umsetzung, Systemservice:

Ist im Rahmen der Projektplanung/-umsetzung und beim Systemservice zu berücksichtigen.

2.1.1.3 Patchfähigkeit, Patchmanagement

BDEW 2.1.1.3	*Alle Komponenten des Gesamtsystems müssen patchfähig sein. Das Einspielen eines Patches sollte möglichst ohne Unterbrechung des normalen Betriebs und mit geringen Auswirkungen auf die Verfügbarkeit des Gesamtsystems erfolgen. Beispielsweise ist eine primärtechnische Außerbetriebnahme der kompletten Anlage zum Patchen der sekundärtechnischen Komponenten zu vermeiden. Bevorzugt werden die Patches zuerst auf den passiven Redundanz-Komponenten eingespielt und nach einem Switch-Over-Prozess (Wechsel der aktiven Komponente im Redundanzsystem) und einem darauffolgendem Test auf den restlichen Komponenten installiert.* *Der Hersteller muss einen Patchmanagementprozess für das gesamte System unterstützen, anhand dessen das Testen, Installieren und Dokumentieren von Sicherheitspatches und Updates gesteuert und verwaltet werden kann. Die Updates sollen vom Betriebspersonal, das diese Systeme administriert, eingespielt werden. Das Installieren bzw. Deinstallieren von Patches muss vom Anlagenbetreiber autorisiert werden und darf nicht automatisch geschehen.*

SICAM RTUs

Bei SICAM RTUs können alle Firmwares einzeln nachgeladen und upgedatet werden, wodurch sich eine Patchfähigkeit des Systems ergibt.

Während eines Firmwareupdates ist zumindest das betroffene Modul nicht einsatzfähig. Ist eine Unterbrechung des normalen Betriebes nicht akzeptabel, kann durch den Einsatz von redundanten Systemen ein unterbrechungsfreier Betrieb gewährleistet werden.

Firmwares für SICAM RTUs werden von der SICAM TOOLBOX II zentral verwaltet. Neue Firmwares werden zuerst in der SICAM TOOLBOX II gespeichert und dann auf SICAM RTUs verteilt.

Im Bereich der Produktentwicklung für SICAM RTUs existiert bei der Siemens AG ein Patchmanagementprozess, nach dem alle Firmwareausgaben, die darin enthaltenen Erweiterungen und Fehlerbehebungen nachvollziehbar dokumentiert sind.

Patchmanagementprozess:

- Überwachung
  Regelmäßige Scans von externen Informationsquellen
  z.B.: OEM (Microsoft, Sybase), CERT community, Vulnerability Datenbanken
- Prüfen Sie Relevanz und Klassifizierung
  Vorinformation von Verkaufs-, Wartungs- und Service Abteilungen
- Implementierung und Test
  von Sicherheits-Patches oder Workarounds

- Freigabe
  von Sicherheits-Patches oder Workarounds;
  Information von Verkaufs-, Wartungs- und Service Abteilungen

Mittels der Funktion "Live Update" der SICAM TOOLBOX II können sämtliche Firmwareupdates für SICAM RTUs automatisiert in der SICAM TOOLBOX II eingelagert werden, wodurch sich die Updatemöglichkeit wesentlich vereinfacht.

SICAM TOOLBOX II

Die SICAM TOOLBOX II wird mittels Maintenance Releases und Hotfixes gepatcht.

Im Bereich der Entwicklung für die SICAM TOOLBOX II existiert bei der Siemens AG ein Patchmanagementprozess, nach dem alle Ausgaben, die darin enthaltenen Erweiterungen und Fehlerbehebungen nachvollziehbar dokumentiert sind.

Hinweis

Info für Projektplanung/-umsetzung, Systemservice:

Es ist darauf zu achten dass durch entsprechende Maßnahmen wie z.B.: Redundanz, Notsteuerebene, Handbetrieb, … die Auswirkungen einer Patchung/Update einzelner Systemkomponenten auf die Verfügbarkeit des Gesamtsystems möglichst gering sind.

Es ist ein Patchmanagementprozess mit dem Kunden zu vereinbaren, der die zur Verfügungstellung, Test, Installation und Dokumentation von Sicherheitspatches und Updates bezüglich Abläufen und Verantwortungen definiert.

2.1.1.4 Bereitstellung von Sicherheitspatches für alle Systemkomponenten

BDEW 2.1.1.4	*Der Auftragnehmer muss Sicherheitsupdates für alle Systemkomponenten während des gesamten Betriebszeitraums, der vertraglich geregelt wird, zur Verfügung stellen. Updates von Basiskomponenten, die nicht vom Auftragnehmer entwickelt wurden, wie z. B. Betriebssystem, Bibliothek oder Datenbank-Managementsystem, muss der Auftragnehmer von den jeweiligen Herstellern beziehen, diese testen und sie gegebenenfalls an den Auftraggeber weiterleiten. Die Bereitstellung der Updates muss innerhalb eines angemessenen Zeitrahmens, dessen Frist vertraglich festzulegen ist, erfolgen.*

Je nach vertraglicher Vereinbarung stellt die Siemens AG Sicherheitsupdates für SICAM RTUs und die SICAM TOOLBOX II während der gesamten Produktlebensdauer zur Verfügung.

- Die Bereitstellung der Updates erfolgt innerhalb eines angemessenen Zeitrahmens, der vertraglich festzulegen ist.
- Patches werden erst nach ausführlichen Test zur Verfügung gestellt.
- Updates sollen vom Betriebspersonal, das diese Systeme administriert, eingespielt werden.
- Das Installieren von Patches muss vom Anlagenbetreiber autorisiert werden und darf nicht automatisch geschehen.

SICAM RTUs

Updates von Basiskomponenten, die nicht von der Siemens AG entwickelt wurden, wie z. B. von Betriebssystemen oder Bibliotheken, werden von den jeweiligen Herstellern bezogen, getestet und im Rahmen neuer Firmwarereleases zur Verfügung gestellt.

SICAM TOOLBOX II

Updates von Basiskomponenten, die nicht von der Siemens AG entwickelt wurden, wie z. B. Datenbank-Managementsystem, Bibliotheken, werden von den jeweiligen Herstellern bezogen, getestet und im Rahmen neuer Releases (Maintenance Releases, Hotfixes) zur Verfügung gestellt.

2.1.1.5 Support für eingesetzte Systemkomponenten

BDEW 2.1.1.5	*Der Auftragnehmer muss sicherstellen, dass für die nicht von ihm entwickelten Systemkomponenten (z. B. Betriebssystem, Datenbank-Managementsystem,…) innerhalb des geplanten Betriebszeitraums, der vertraglich geregelt wird, Herstellersupport und Sicherheitsupdates zur Verfügung stehen. Das Abkündigungsverfahren und alle relevanten Fristen wie z. B. Last-Customer-Shipping und End-Of-Support müssen vertraglich festgeschrieben werden.*

Es wird sichergestellt, dass Support für die nicht von der Siemens AG entwickelten Systemkomponenten, die Produktbestandteil von SICAM RTUs und SICAM TOOLBOX II sind (z. B. Betriebssysteme, Datenbank-Managementsysteme,…), innerhalb der geplanten Produktlebensdauer zur Verfügung steht.

Die Abkündigungsverfahren für SICAM RTUs und SICAM TOOLBOX II definieren alle relevanten Fristen wie z. B. Last-Customer-Shipping und End-Of-Support.

2.1.1.6 Verschlüsselung sensibler Daten bei Speicherung und Übertragung

BDEW 2.1.1.6	*Sensible Daten dürfen im System nur verschlüsselt gespeichert bzw. übertragen werden. Zu den zu schützenden Daten können beispielsweise Protokolldateien, Passwörter oder vertrauliche Daten nach behördlichen Vorgaben oder den relevanten Gesetzen, wie z.B. dem Bundesdatenschutzgesetz gehören. Gegebenfalls soll das System auch die sichere, selektive Löschung bestimmter Daten ermöglichen, beispielsweise durch Überschreiben mit Zufallsdaten.*

SICAM RTUs

In SICAM RTUs werden bei Parametrierung mittels SICAM TOOLBOX II keine Passwörter im Klartext, sondern verschlüsselt (https) übertragen. Die Benutzerauthentisierung und Rechtevergabe findet in der SICAM TOOLBOX II statt.

Um eine Benutzerauthentisierung der SICAM TOOLBOX II im abgesetzten Betrieb mit SICAM RTUs zu ermöglichen, kann in den SICAM RTUs ein "Connection Password" eingestellt werden. Dieses wird in der SICAM RTUs und nicht in der SICAM TOOLBOX II gespeichert. Es wird das HASH-Challenge-Response-Verfahren eingesetzt.

SICAM RTUs übertragen bei WEB-Parametrierung keine Passwörter im Klartext, sondern verschlüsselt (https).

In SICAM RTUs werden Preshared Keys (für IPSec, SNMP) sowie Passwörter (für SICAM WEB), welche zur Authentifizierung verwendet werden, gesichert abgelegt.

SICAM TOOLBOX II

Die Übertragung von Passwörtern zwischen Client und Server erfolgt verschlüsselt.

Die Speicherung der Passwörter am Client und Server erfolgt verschlüsselt.

2.1.1.7 Verschlüsselungsstandards

BDEW 2.1.1.7	*Bei der Auswahl von Verschlüsselungsstandards sind nationale Gesetzgebungen zu berücksichtigen. Es dürfen nur anerkannte Verschlüsselungs-Verfahren und Schlüsselmindestlängen benutzt werden, die nach aktuellem Stand der Technik auch in Zukunft als sicher gelten. Selbstentwickelte Verschlüsselungs-Algorithmen sind nicht erlaubt. Bei der Implementierung der Verschlüsselungs-Verfahren sollte, wo möglich, auf anerkannte Verschlüsselungs-Bibliotheken zurückgegriffen werden, um Implementierungsfehler zu vermeiden.*

In SICAM RTUs und SICAM TOOLBOX II werden nur anerkannte Verschlüsselungsverfahren mit nach aktuellem Stand der Technik als sicher geltenden Schlüssellängen verwendet.

2.1.1.8 Interne/externe Sicherheits- und Anforderungstests und zugehörige Dokumentation

BDEW 2.1.1.8	*Die einzelnen Systemkomponenten und die wesentlichen Funktionen des Gesamtsystems (in einer repräsentativen Konfiguration) müssen vor der Auslieferung vom Auftragnehmer durch eine vom Entwicklungsteam unabhängige Abteilung 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.*

In SICAM RTUs und SICAM TOOLBOX II werden die einzelnen Systemkomponenten und die wesentlichen Funktionen eines SICAM RTUs / SICAM TOOLBOX II Gesamtsystems in einer repräsentativen Testkonfiguration im Rahmen von Typtests durch eine vom Entwicklungsteam unabhängige Abteilung einem ausführlichen Funktions-, Sicherheits- und Stresstest unterzogen.

Die Ergebnisse der Tests sowie die dazugehörige Dokumentation (Softwarestände, Prüfkonfiguration, etc.) wird verwaltet.

2.1.1.9 Sichere Standard-Konfiguration und Erstinstallation bzw. (Wieder-) Inbetriebnahme

BDEW 2.1.1.9	*Das System 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.*

In SICAM RTUs und SICAM TOOLBOX II sind alle securityrelevanten Dienste per Default ausgeschalten (z.B. Fernwartung, Fernreset etc.). Benötigte Dienste sind bei Bedarf freizuschalten, in diesem Fall muss das Default-Passwort geändert werden.

Die Dokumentation der Grundkonfiguration und der freigeschaltenen Dienste ist im Dokument *SICAM RTUs / SICAM TOOLBOX II Administrator Security-Handbuch* beschrieben.

Hinweis

Info für Projektplanung/-umsetzung

Die SICAM TOOLBOX II hat nach der Installation 3 Standardbenutzer mit Defaultpasswörtern. Diese müssen nach der Installation geändert werden

Die SICAM TOOLBOX II umfasst weder Hardware noch Betriebssystem oder andere Standardprogramme wie z.B.: Microsoft Office oder Adobe Acrobat Reader.

Die „Sichere Standard-Konfiguration und Erstinstallation bzw. (Wieder-) Inbetriebnahme“ von Betriebssystem und anderen Standardprogrammen eines SICAM TOOLBOX II Systems muss im Rahmen der Projektplanung/-umsetzung erfolgen.

Bei WEB-Parametrierung müssen die Default-Passwörter geändert werden.

2.1.1.10 Integritäts-Prüfung

BDEW 2.1.1.1	*Systemdateien, Anwendungen, Konfigurationsdateien und Anwendungs-Parameter müssen auf Integrität überprüft werden können, beispielsweise durch Prüfsummen.*

SICAM RTUs

Die Firmwares und Parameterblöcke der SICAM RTUs sind mittels Prüfsummen gesichert und werden im Betrieb laufend auf Integrität überprüft.

Mit der SICAM TOOLBOX II kann ein Vergleich der Firmwarerevisonen und Parameterstände im Zielsystem und in der SICAM TOOLBOX II Datenbank durchgeführt werden, um etwaige Veränderungen zu erkennen.

SICAM TOOLBOX II

Die SICAM TOOLBOX II wird mittels Windows-Installer installiert, somit stehen die dort verwendeten Sicherheitsmechanismen zur Wahrung der Applikationsintegrität zur Verfügung.

Die Integrität der Anwendungsdaten ist durch die Mechanismen auf Betriebssystem- und Datenbankebene sichergestellt.

2.1.2 Dokumentation

2.1.2.1 Design-Dokumentation, Beschreibung sicherheitsrelevanter Systemkomponenten und Implementations-Spezifikationen

BDEW 2.1.2.1	*Dem Auftraggeber muss spätestens zur Abnahme eine Gesamtdokumentation über das High-Level-Design des Gesamtsystems zur Verfügung gestellt werden. Darin beschrieben sind der grundsätzliche 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. Außerdem werden sicherheitsspezifische Implementierungsdetails aufgelistet und kurz beschrieben (z. B. verwendete Verschlüsselungsstandards)..*

Für SICAM RTUs und SICAM TOOLBOX II ist das High-Level-Design und der grundsätzliche Systemaufbau samt der Interaktionen der beteiligten Komponenten anhand typischer Anlagenkonfigurationen im Adminstratorhandbuch für SICAM RTUs beschrieben.

Hinweis

Info für Projektplanung/-umsetzung

Diese typischen Anlagenkonfigurationen sind als Beispiele gedacht und decken nicht alle möglichen Systemkonfigurationen ab.

Sie können nur als Ausgangsbasis für das Design und die Dokumentation eines Gesamtsystems verwendet werden.

2.1.2.2 Administrator- und Benutzer- Dokumentation

BDEW 2.1.2.2	*Es müssen getrennte Dokumentationen für den Administrator und die System-Benutzer existieren. Beide Dokumentationen sollten für die jeweiligen Gruppen unter anderem eine Auflistung der sicherheitsrelevanten Einstellungen und Funktionen enthalten und Regeln für sicherheitsverantwortliches Handeln nennen.*

Da im Bereich der Sekundär-/Automatisierungstechnik für SICAM RTUs und SICAM TOOLBOX II eine Benutzerdokumentation im Sinn des BDEW-Whitepapers nicht relevant ist, wird für SICAM RTUs und SICAM TOOLBOX II nur eine Administrator-Dokumentation (Administrator: nimmt Änderungen an der Anlagenparametrierung / Systemkonfiguration der Anlage vor) erstellt.

Inhalt der Administrator-Dokumentation für SICAM RTUs und SICAM TOOLBOX II:

- Sicherheitsrelevante Systemeinstellungen, Parameter und deren Defaults
- Typische Anlagenkonfigurationen
- Anwendungshinweise für sicherheitsverantwortliches Handeln (Backup, Patchmanagement, Virenschutz)
- Erläuterung sicherheitsspezifischen Log und Audit-Meldungen; mögliche Ursachen; passende Gegenmaßnahmen
- Traffic-Matrix (Kommunikationsschnittstellen)
- Maßnahmen zur Systemhärtung

  Zu den anzuwendenden Härtungsmaßnahmen zählen bei SICAM RTUs:
  - Deaktivierung unnötiger System- und Kommunikationsdienste (abgesetzter Betrieb, Fernwartung, NTP, WEB, ….)
  - Deaktivierung unnötiger Standard-Nutzer (WEB)

  - Aktivierung sicherheitserhöhender Konfigurationsoptionen

  Zu den anzuwenden Härtungsmaßnahmen zählen bei SICAM TOOLBOX II:

  - Deinstallation oder Deaktivierung unnötiger Softwarekomponenten (ST-Emulation, Telegrammsimulation, Datenflusstest, …)
  - Deaktivierung unnötiger System- und Kommunikationsdienste (abgesetzter Betrieb, Fernwartung)
  - Deaktivierung unnötiger Standard-Nutzer
  - Aktivierung sicherheitserhöhender Konfigurationsoptionen
  - Einschränkung der Rechte von Nutzern und Programmen
- Backup- / Restore
- Sichere Grundkonfiguration
- …

2.1.2.3 Dokumentation sicherheitsrelevanter Einstellungen und Systemmeldungen

BDEW 2.1.2.3	*In der Administratordokumentation existiert eine Beschreibung aller sicherheitsrelevanten Systemeinstellungen und Parameter sowie ihrer Defaultwerte. Die Dokumentation weist auf Konsequenzen von grob unsicheren Konfigurationseinstellungen hin. Außerdem sind in einer Dokumentation alle sicherheitsspezifischen Log und Audit-Meldungen erläutert und mögliche Ursachen sowie gegebenenfalls passende Gegenmaßnahmen genannt.*

Die Administratordokumentation für SICAM RTUs und SICAM TOOLBOX II enthält eine Beschreibung aller sicherheitsrelevanten Systemeinstellungen und Parameter sowie ihrer Defaultwerte.

Die Dokumentation weist auf Konsequenzen von grob unsicheren Konfigurationseinstellungen hin. Außerdem sind alle sicherheitsspezifischen Log und Audit-Meldungen erläutert und mögliche Ursachen sowie gegebenenfalls passende Gegenmaßnahmen genannt.

2.1.2.4 Dokumentation der Voraussetzungen und Umgebungs-Anforderungen für den sicheren System-Betrieb

BDEW 2.1.2.4	*In der Administratordokumentation existiert eine Darstellung in der die Voraussetzungen für einen sicheren Systembetrieb beschrieben werden. Dazu zählen unter anderem Anforderungen an den Benutzerkreis, Netzwerkumgebung sowie Interaktion und Kommunikation mit anderen Systemen und Netzwerken.*

Hinweis

Diese Anforderung hat keine Relevanz für Produktentwicklung oder Produktservice.

Information für Projektplanung / -umsetzung:

Die Administratordokumentation für SICAM RTUs und SICAM TOOLBOX II enthält typische Anlagenkonfigurationen und somit eine Darstellung der Voraussetzungen für einen sicheren Systembetrieb . Dazu zählen unter anderem Anforderungen an den Benutzerkreis, Netzwerkumgebung sowie Interaktion und Kommunikation mit anderen Systemen und Netzwerken.

2.2 Bereich Basissystem

2.2.1 Grundsicherung und Systemhärtung

BDEW 2.2.1	*Alle Komponenten des Basissystems müssen anhand anerkannter Best-Practice-Guides dauerhaft gehärtet und mit aktuellen Service-Packs und Sicherheits-Patches versehen sein. Ist dieses technisch nicht durchführbar, ist für die Übergangsphase (bis zur vollständigen Erfüllung der Forderung aus 0) eine dokumentierte entsprechende Sicherheitsmaßnahme zu ergreifen. Unnötige Benutzer, Defaultuser, Programme, Netzwerkprotokolle, Dienste und Services sind deinstalliert, oder – falls eine Deinstallation nicht möglich ist – dauerhaft deaktiviert und gegen versehentliches Reaktivieren geschützt. Die sichere Grundkonfiguration der Systeme muss überprüft und dokumentiert sein. Insbesondere müssen die in diesem Dokument geforderten Maßnahmen, die zur Härtung der Systeme beitragen, durchgeführt sein.*

Alle Komponenten der SICAM RTUs und SICAM TOOLBOX II sind anhand anerkannter Best-Practice-Guides dauerhaft gehärtet, wodurch sich eine sichere Grundkonfiguration der SICAM RTUs und SICAM TOOLBOX II ergibt.

Die sichere Grundkonfiguration und die Maßnahmen zur Systemhärtung sind im Dokument *SICAM RTUs / SICAM TOOLBOX II Administrator Security-Handbuch* beschrieben.

Maintenance Releases, Hotfixes und Firmwares die Sicherheits-Patches beinhalten werden für SICAM RTUs und SICAM TOOLBOX II zeitnah zur Verfügung gestellt.

Hinweis

Info für Projektplanung/-umsetzung und Systemservice:

Die SICAM TOOLBOX II umfasst weder Hardware noch Betriebssystem oder andere Standardprogramme wie z.B.: Microsoft Office oder Adobe Acrobat Reader.
Die Grundsicherung und Systemhärtung des Betriebssystems und anderer Standardprogramme muss im Rahmen der Systementwicklung, Projektplanung/-umsetzung und Systemservice konzipiert, realisiert und gewartet werden.

2.2.2 Antiviren-Software

BDEW 2.2.2	*Alle vernetzten, Ix-Basierenden Systeme müssen an geeigneter Stelle mit Antiviren-Software und Malware-Schutz versehen sein. Alternativ zum Einsatz von Antiviren-Scannern auf allen Systemen ist vom Lieferanten ein umfassendes Antiviren-Konzept vorzulegen, das einen gleichwertigen Schutz bietet. Für eine automatische und zeitnahe Aktualisierung der Antiviren-Pattern-Dateien muss gesorgt sein, wobei keine direkte Verbindung mit Updateservern in externen Netzen, wie dem Internet benutzt werden darf. Eine Realisierungsmöglichkeit wäre zum Beispiel die Verwendung eines internen Updateservers. Der Zeitpunkt der Aktualisierung auf den Endsystemen ist konfigurierbar. Als Alternative zur automatischen Aktualisierung ist ein sicherer Prozess zu definieren und zu dokumentieren, bei dem die Updates regelmäßig und zeitnah manuell in das System eingespielt werden.*

Bei den SICAM RTUs Komponenten handelt es sich um selbstentwickelte Embedded-Systeme, für die es keine bekannten Viren gibt. Es ist daher auch keine Schutzsoftware für diese Systeme verfügbar.
Zusätzlich werden die Komponenten vor Inbetriebnahme gehärtet, um erhöhten Schutz gegen mögliche Schadsoftware zu erreichen.

Hinweis

Info für Projektplanung/-umsetzung und Systemservice:

Die SICAM TOOLBOX II umfasst weder Hardware noch Betriebssystem oder andere Standardprogramme wie z.B.: Microsoft Office oder Adobe Acrobat Reader.
Der Virenschutz muss im Rahmen der Projektplanung/-umsetzung konzipiert und realisiert werden.

2.2.3 Autonome Benutzerauthentifizierung

BDEW 2.2.3	*Die zur Nutzeridentifizierung und –authentifizierung auf Betriebssystemebene nötigen Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden. Die Anbindung an einen zentralen, prozessnetz-internen Directory Service sollte in Betracht gezogen werden.*

SICAM RTUs benötigen keine Benutzerverwaltung, da die gesamte Parametrierung über die SICAM TOOLBOX II erfolgt.

Bei der Verwendung der WEB-Parametrierung kann die Benutzerauthentifizierung je Gerät erfolgen.

Die SICAM TOOLBOX II verwaltet die Zugriffsrechte mit einem Benutzer/Rollen-Konzept. Die Benutzer und Rollen können frei angelegt und zugeordnet werden.
Die Authentisierung der Benutzer kann über das Betriebssystem oder innerhalb der SICAM TOOLBOX II erfolgen.
Beim Zugriff auf SICAM RTUs mittels SICAM TOOLBOX II über den abgesetzen Betrieb ist in den SICAM RTUs eine Benutzer-Authentisierung mittels „Connection Passwort“ möglich.

2.3 Bereich Netze / Kommunikation

2.3.1 Sichere Netzwerkkonzeption und Kommunikationsverfahren

2.3.1.1 Eingesetzte Protokolle und Technologien

BDEW 2.3.1.1	*a) Wo technisch möglich, dürfen nur sichere Kommunikationsstandards- und Protokolle benutzt werden, die Integritätsüberprüfung, Authentifizierung und ggf. Verschlüsselung bieten. Das betrifft besonders die Protokolle zur Remote-Administration oder durch welche Benutzer-Anmeldeinformationen übertragen werden. Passwort-Übertragungen im Klartext sind nicht erlaubt (z. B. kein Telnet, keine Unix r-Dienste). Eine aktuelle Liste der sicheren Protokolle kann nach den jeweils internen Regularien des Auftraggebers bereit gestellt werden.* *b) Netzwerkkomponente müssen sich in die Netzwerk-Konzeption des Gesamtunternehmens einbinden lassen. Relevante Netzwerk-Konfigurationsparameter wie IP-Adressen müssen zentral administriert werden können.* *Zur Administration und zum Monitoring werden sichere Protokolle verwendet (SSHv2, SNMPv3). Die Netzwerkkomponenten sind gehärtet, unnötige Dienste und Protokolle sind deaktiviert, Management-Interfaces sind durch ACL geschützt.* *c) Netzwerkkomponenten, die vom Auftragnehmer bereitgestellt werden, müssen in ein zentrales Inventory- und Patchmanagement 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 SSL/TLS-Verschlüsselung oder durch VPN-Technologie).* *e) Wo technisch möglich, werden Firewall-freundliche Protokolle benutzt: z. B. TCP anstatt UDP, OPC über Netzgrenzen hinweg vermeiden.* *f) 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.*

SICAM RTUs

a) Für die Übertragung von Prozessdaten werden Standardprotokolle wie IEC-61850, IEC-60870-5-101, IEC 60870-5-104 verwendet.
Da diese Protokolle derzeit keine Authentifizierung und Verschlüsselung bieten, kann man bei Bedarf mittels VPN-Technologie diese Anforderungen abdecken. Die Integritätsprüfung erfolgt mittels CRC oder Prüfsummen.

b) Netzwerk-Konfigurationsparameter für alle SICAM RTUs Komponenten werden zentral mittels SICAM TOOLBOX II verwaltet.

   Administration und Monitoring von SICAM RTUs Netzwerkkomponenten erfolgt mittels SICAM TOOLBOX II

   Die Netzwerkkomponenten von SICAM RTUs sind gehärtet, unnötige Dienste und Protokolle sind deaktiviert, Managementinterfaces stehen ausschließlich der SICAM TOOLBOX II zur Verfügung.

c) Inventory und Patchmanagement von SICAM RTUs Netzwerkkomponenten erfolgt mittels SICAM TOOLBOX II

d) Der Einsatz von IP ist über die Standardprotokolle IEC-61850 und IEC-60870-5-104 möglich, Verschlüsselung mittels VPN-Technologie

e) Die Standardprotokolle IEC-61850 und IEC-60870-5-104 verwenden TCP, UDP wird ausschließlich zur Zeitsynchronisation mittels NTP eingesetzt

f) **Hinweis**

Info für Projektplanung/-umsetzung:

Ist beim Systemdesign zu berücksichtigen.

SICAM TOOLBOX II

a) Remote Administration der SICAM TOOLBOX II erfolgt verschlüsselt mittels Remote Desktop Protocol (RDP) und Remote Desktop Connection Client (RDC).

Remote Administration von SICAM RTUs: unverschlüsselt via TCP/IP und ohne Passwort.

b) Die SICAM TOOLBOX II ist gehärtet, unnötige Dienste und Protokolle sind deaktiviert, Managementinterfaces stehen ausschließlich über die Betriebssystemebene zur Verfügung.

Hinweis

Info für Projektplanung/-umsetzung und Systemservice:

Die SICAM TOOLBOX II setzt auf Microsoft Windows als Betriebssystem auf. Administration, Monitoring und Härtung des Betriebssystems sind nicht Bestandteil der SICAM TOOLBOX II.

c) Patches der SICAM TOOLBOX II können händisch installiert oder in zentrale Patchmanagementsysteme eingebunden werden.

Hinweis

Info für Projektplanung/-umsetzung und Systemservice:

Die SICAM TOOLBOX II setzt auf Microsoft Windows als Betriebssystem auf. Inventory und Patchmanagement des Betriebssystems sind nicht Bestandteil der SICAM TOOLBOX II.

d) SICAM TOOLBOX II verwendet für die Kommunikation über WAN-Verbindungen ausschließlich das IP-Protokoll, Verschlüsselung mittels VPN-Technologie oder auf Windows Betriebssystemebene.

e) SICAM TOOLBOX II verwendet ausschließlich TCP

f) **Hinweis**

Info für Projektplanung/-umsetzung:

Ist beim Systemdesign zu berücksichtigen.

2.3.1.2 Sichere Netzwerkstruktur

BDEW 2.3.1.2	*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
	c) Firewalls und VPNs werden über einen vom Auftraggeber definierten Prozess zentral bereitgestellt und administriert.

Hinweis

Info für Projektplanung/-umsetzung:

Diese Anforderung ist nicht produktrelevant, und ist während des Systemdesigns und der Projektplanung/Umsetzung zu berücksichtigen.

2.3.1.3 Dokumentation der Netzwerkstruktur und –konfiguration

BDEW 2.3.1.3	*Die Netzwerkkonzeption und -konfiguration, alle physikalischen, virtuellen und logischen Netzwerkverbindungen und die verwendeten Protokolle sowie die Netzwerk-Perimeter, die Bestandteil des Systems sind bzw. mit ihm interagieren, müssen dokumentiert sein. Änderungen, z. B. durch Updates werden innerhalb des Changemanagements 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.*

Hinweis

Info für Systementwicklung und Projektplanung/-umsetzung:

Diese Anforderung ist nicht produktrelevant, und ist während des Systemdesigns und der Projektplanung/Umsetzung zu berücksichtigen.

2.3.2 Sichere Wartungsprozesse und RAS-Zugänge

2.3.2.1 Sichere Fern-Zugänge

BDEW 2.3.2.1	*Hinweis: Der Ausdruck „Wartung“ bezieht sich in diesem Dokument allgemein auf alle vom Auftraggeber/Betreiber zu beauftragenden Service- Maßnahmen wie Instandhaltungsarbeiten, Störungsanalysen, Fehler- und Störungsbehebung, Verbesserungen, Anpassungen, usw.* *a) Administration, Wartung und Konfiguration aller Komponenten muss auch über ein Out-of-Band-Netz, zum Beispiel Zugriff lokal, via serielle Schnittstelle, Netzwerk oder direkter Steuerung der Eingabegeräte (KVM), möglich sein.* *b) Fern-Zugriff muss über zentral verwaltete Zugangserver durchgeführt werden. Die Zugangserver müssen in einer DMZ betrieben werden und eine Isolation des Prozessnetzes sicherstellen. Es muss ein starkes 2-Faktor-Authentifizierungsverfahren benutzt werden.* *c) Direkte Einwahl Zugänge in Endgeräte sind grundsätzlich nicht erlaubt.* *d) Der Zugriff auf einen Fern-Zugang muss (zentral) geloggt werden, wiederholte Fehlversuche werden gemeldet.* *e) Alle Fern-Zugangs-Möglichkeiten müssen dokumentiert werden.*

Hinweis

Info für Systemdesign, Produkt/-Systemservice und Leitstellen-/Systembetrieb:

Diese Anforderung ist nicht produktrelevant, und ist während Systemdesign, Produkt-/Systemservice und Leitstellen-/Systembetrieb zu berücksichtigen.

2.3.2.2 Anforderungen an die Wartungsprozesse

BDEW 2.3.2.2	*a) Der interaktive Fern-Zugang muss über personalisierte Accounts erfolgen. Für automatisierte Abläufe sind spezielle Kennungen einzurichten, die nur bestimmte Funktionen ausführen können und die keinen interaktiven Zugang ermöglichen.* *b) Es muss technisch sichergestellt sein, dass ein Fern-Zugriff nur erfolgen kann, wenn dieser vom Betriebspersonal, das diese Systeme administriert, freigegeben wird. Bei externen Dienstleister muss die Freigabe für jeden Verbindungsaufbau einzeln erfolgen. Eine Sitzung ist nach Ablauf einer angemessenen Zeit automatisch zu trennen.* *c) Am Standort des Auftragnehmers muss der Fern-Zugriff durch einen definierten und geschulten Personenkreis und nur von speziell gesicherten Systemen aus erfolgen. Insbesondere sind diese Zugangs-Systeme während des Fern-Zugriffs von anderen Netzen logisch oder physikalisch zu entkoppeln. Eine physikalische Entkopplung ist der logischen vorzuziehen.* *d) Durch einen definierten Wartungsprozess (siehe oben) muss sichergestellt sein, dass das Wartungspersonal im Rahmen des Remote-Zugangs nur Zugriff auf die benötigten Systeme, Dienste und Daten erhält.* *e) Das Wartungspersonal muss den aktuell gültigen Anforderungen gemäß der SÜFV genügen, sofern es für Unternehmen mit überregionaler Elektrizitätsversorgung tätig ist.* *f) Die Vorortwartung durch Servicetechniker stellt ein ernst zu nehmendes Sicherheitsrisiko dar. Es ist zu vermeiden, dass der Auftragnehmer eigene Hardware an das Prozessnetz anschließt (z. B. Wartungs- Notebooks, aber auch Speichergeräte wie USB-Sticks). Falls dies doch nötig sein sollte, muss diese Hardware speziell abgesichert und vom Auftraggeber genehmigt sein sowie zeitnah auf Malware untersucht werden. Der Auftragnehmer ist verpflichtet, die Durchsetzung einer angemessenen internen Sicherheitsrichtlinie für diese Dienstleistung nachzuweisen.*

Hinweis

Info für Produkt/-Systemservice und Leitstellen-/Systembetrieb:

Diese Anforderung ist nicht produktrelevant, und ist während Produkt-/Systemservice und Leitstellenbetrieb/Systembetrieb zu berücksichtigen.

2.3.3 Funktechnologie: Bedarf und Sicherheitsanforderungen

BDEW 2.3.3	*Der Einsatz von WLAN, Bluetooth und anderen drahtlosen Übertragungstechniken ist bei Systemen mit hohem oder sehr hohem Schutzbedarf generell verboten. Ein Einsatz ist nur nach Analyse der damit verbundenen Risiken und unter Beachtung der nachfolgend beschriebenen Mindestsicherungsmaßnahmen in Abstimmung mit dem Auftraggeber und nach Genehmigung zulässig:* • *WLANs dürfen nur in dedizierten und durch Firewalls und Applikations-Proxies abgetrennten Netzwerk-Segmenten betrieben werden.* • *Drahtlose Übertragungstechnik muss nach dem Stand der Technik abgesichert werden.* • *Neue WLANs sind so einzurichten, dass bestehende WLANs nicht gestört oder beeinträchtigt werden.*

In SICAM RTUs sind keine Funktechnologien vorhanden. Daher ist diese Anforderung für SICAM RTUs nicht relevant.

Hinweis

Info für Projektplanung/-umsetzung:

Werden in einer Systemlösung Funktechnologien verwendet sind entsprechende Maßnahmen auf Geräteebene der Übertragungseinrichtungen (z.B.: Funkmodem, …) zu setzen.

In SICAM TOOLBOX II sind keine Funktechnologien vorhanden. Daher ist diese Anforderung für SICAM TOOLBOX II nicht relevant.

Hinweis

Info für Projektplanung/-umsetzung:

Werden auf einem SICAM TOOLBOX II – PC Funktechnologien verwendet sind entsprechende Maßnahmen auf Geräte-Hardware und/oder Betriebssystemebene zu setzen.

2.4 Bereich Anwendung

2.4.1 Benutzerverwaltung

2.4.1.1 Rollenkonzepte

BDEW 2.4.1.1	*Das System muss 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.* • ***Auditor**: Benutzerrolle, die ausschließlich die Berechtigung zum Einsehen und Archivieren der Audit-Logs besitzt.* • ***Operator**: Benutzer, der das System im Rahmen der vorgesehenen Nutzung bedient. Dies beinhaltet auch das Recht zur Änderung von betriebsrelevanten Einstellungen.* • ***Data-Display**: Benutzer, der den Status des Systems abrufen und definierte Betriebsdaten lesen darf, aber nicht berechtigt ist, Änderungen durchzuführen.* *Gegebenenfalls wird eine Benutzerrolle „Backup-Operator“ definiert, die Datensicherungen aller relevanten System- und Anwendungsdaten durchführen kann.* *Das System muss eine granulare Zugriffskontrolle auf Daten und Ressourcen erlauben. Die Zugriffsrechte entsprechen einer sicheren Systemkonfiguration. Sicherheitsrelevante Systemeinstellungen und Konfigurationswerte können nur von der Administrator-Rolle gelesen und geändert werden. Zur normalen Systemnutzung sind nur Operator oder Data-Display Rechte notwendig. Benutzer-Accounts können einzeln deaktiviert werden, ohne sie vom System entfernen zu müssen.*

SICAM RTUs

Es gibt in SICAM RTUs bei Verwendung der SICAM TOOLBOX II keine Benutzer- und Rollenverwaltung, da die Benutzer- und Rollenverwaltung in der SICAM TOOLBOX II erfolgt

Bei der Verwendung der WEB-Parametrierung von SICAM RTUs erfolgt die Benutzerauthentifizierung je Gerät.

Im SICAM CMIC und SICAM EMIC gibt es die Rollen „Admin“ und „Gast“ (entspricht „Administrator“ und „Data-Display“).
Bei den NIP's (in SICAM RTUs) gibt es kein Rollen. Daten können ausschließlich angesehen werden.

SICAM TOOLBOX II

Es existiert in der SICAM TOOLBOX II eine Benutzer/Rollenfunktion.
Zugriffe und Berechtigungen können rollenspezifisch frei definiert werden, den Benutzern können Rollen zugeordnet werden.

Die Standardrollen der SICAM TOOLBOX II (Administrator, Profi, Standard) können von einem SICAM TOOLBOX II Administrator um zusätzliche Rollen erweitert werden.

2.4.1.2 Benutzer-Authentifizierung und Anmeldung

BDEW 2.4.1.2	• *Die Anwendung muss eine personenspezifische Identifizierung und Authentifizierung vornehmen, Gruppenaccounts werden von Auftraggeber nur in genau spezifizierten Ausnahmefällen erlaubt.* • *Ohne erfolgreiche Benutzer-Authentifizierung darf das System keinerlei Aktionen erlauben.* • *Das System muss Passwörter mit vom Auftraggeber definierbarer Stärke und Gültigkeitsdauer erzwingen.* • *Wo technisch möglich, wird eine starke 2-Faktor-Authentifizierung verwendet, z. B. durch die Verwendung von Tokens oder SmartCards.* • *Die zur Nutzeridentifizierung und Authentifizierung benötigten Daten dürfen nicht ausschließlich von außerhalb des Prozessnetzes bezogen werden. Die Anbindung an einen zentralen, prozessnetzinternen Directory Service sollte in Betracht gezogen werden.* • *Erfolgreiche und fehlgeschlagene Anmeldeversuche müssen zentral geloggt werden.* *Die folgenden Punkte sind gegebenenfalls unter vorrangiger Beachtung der Anforderungen an einen sicheren Anlagenbetrieb und von Verfügbarkeitsaspekten umzusetzen:* *Das System soll Mechanismen implementieren, die eine sichere und nachvollziehbare Übergabe von Benutzer-Sessions im laufenden Betrieb ermöglichen.* *Wo möglich und sinnvoll sollen Benutzer-Sessions nach einer definierbaren Inaktivitäts-Zeit gesperrt werden.* *Bei einer Überschreitung einer konfigurierbaren Anzahl von fehlgeschlagenen Anmeldeversuchen soll eine Alarmmeldung ausgelöst und wenn möglich das Konto gesperrt werden.*

SICAM RTUs

In SICAM RTUs wird bei Verwendung der SICAM TOOLBOX II die Benutzer-Authentifizierung und Anmeldung der SICAM TOOLBOX II verwendet.

Zusätzlich kann im abgesetzten Betrieb mit der SICAM TOOLBOX II für die Benutzer-Authentisierung ein "Connection Password" eingestellt werden. Dieses wird in den SICAM RTUs und nicht in der SICAM TOOLBOX II gespeichert.

Bei der Verwendung der WEB-Parametrierung von SICAM RTUs erfolgt die Benutzerauthentifizierung und Anmeldung je Gerät über die Gruppenaccounts „Administrator“ und „Gast“.

In SICAM RTUs steht ein Security Logbuch zur Verfügung in welchem erfolgreiche und fehlgeschlagene Anmeldeversuche geloggt werden.

SICAM TOOLBOX II

- Die Benutzer-Authentifizierung und Anmeldung erfolgt ein- oder mehrstufig:
  - Anmeldung am Betriebssystem des Gerätes (einstufige Authentifizierung/Anmeldung)
  - Anmeldung an die SICAM TOOLBOX II Applikation (entweder über die Benutzerverwaltung in der SICAM TOOLBOX II oder single SignOn an die SICAM TOOLBOX II mit dem Betriebssystem Benutzer.)
  - Anmeldung der SICAM TOOLBOX II Benutzer an SICAM RTUs mit „Connection Password“ im abgesetzten Betrieb (optional)
- Zum Loggen erfolgreicher und fehlgeschlagener Anmeldeversuche steht ein Security Logbuch zur Verfügung. Die Daten können automatisch mittels integriertem Syslog-Client an das Windows Event Log und/oder einen externen Syslog-Server weitergeleitet werden..

Hinweis

Info für Systementwicklung und Projektplanung/-umsetzung:

Mit Microsoft Windows als Basisbetriebssystem der SICAM TOOLBOX II sind alle geforderten Punkte

während der Systementwicklung bzw. Projektplanung/Umsetzung realisierbar.

Die Nutzeridentifizierung und Authentifizierung über einen zentralen, prozessnetzinternen Directory Service ist aus Verfügbarkeitsgründen problematisch, da im Fehlerfall (z.B.: Kommunikationsausfall) dieser nicht zur Verfügung steht und somit keine Systemanmeldung und Fehlersuche möglich wäre.

2.4.2 Autorisierung von Aktionen auf Benutzer- und Systemebene

BDEW 2.4.2	*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.*

Nach Anmeldung an der SICAM TOOLBOX II können die Benutzer die in ihrer Rolle definierten Rechte wahrnehmen. Zusätzlich kann der Zugang zu SICAM RTUs mittels „Connection Passwort“ auf Benutzerebene geschützt werden.

SICAM RTUs

Im Bay Controller SICAM BC ist die Vorortbedienung mittels Schlüsselschalter gesichert.

In SICAM CMIC und SICAM EMIC werden derzeit nur Prozesszustände angezeigt. Eine Steuerung ist nicht möglich.

Hinweis

Info für Projektplanung/-umsetzung:

Sicherheitsrelevante/-kritische Aktionen, z.B. eine gesicherte Befehlsgabe, können bei SICAM RTUs z.B. mittels Schlüsselschalter realisiert werden.
Die Konzipierung und Realisierung ist nicht produktrelevant und erfolgt beim Systemdesign bzw. bei Projektplanung/-umsetzung.

SICAM TOOLBOX II

Mit der in der SICAM TOOLBOX II verfügbaren Benutzer- und Rollenverwaltung kann definiert werden, wer sicherheitsrelevante/-kritische Aktionen (z.B.: ST-Emulation, LogView, Telegrammsimulation, ...) durchführen darf.

Hinweis

Info für Projektplanung/-umsetzung:

Die Konzipierung und Realisierung der Benutzer- und Rollenverwaltung für SICAM TOOLBOX II ist projekt- oder kundenspezifisch und erfolgt beim Systemdesign bzw. bei Projektplanung/-umsetzung.

2.4.3 Anwendungsprotokolle

BDEW 2.4.3	*Es werden nur vom Auftraggeber freigegebene standardisierte Protokolle für Dienst- und Anwendungskommunikation benutzt. Ausnahmefälle bedürfen einer expliziten Genehmigung durch den Auftraggeber und sind zu dokumentieren. Es sind Protokolle vorzuziehen, welche die Integrität der Kommunikation sowie die korrekte Authentifizierung und Autorisierung der Kommunikationspartner sicherstellen und die durch Timestamps oder sichere Sequenznummern ein Wiedereinspielen bereits gesendeter Nachrichten verhindern. Bei Bedarf sollte auch eine Verschlüsselung der Protokolldaten implementiert werden. Bei nicht standard-konformen bzw. selbst entwickelten oder proprietären Protokollen sind die genannten Punkte ebenfalls zu berücksichtigen.*

Für die Übertragung von Prozessdaten werden Standardprotokolle wie IEC-61850, IEC-60870-5-101, IEC 60870-5-104 verwendet.

Bei einigen Protokollelementen in SICAM RTUs kann unter Anwendung des WEB-Browser ein PING abgesetzt werden.

Hinweis

Info für Projektplanung/-umsetzung:

Da die Standardprotokolle IEC-61850, IEC-60870-5-101 und IEC 60870-5-104 derzeit keine Authentifizierung, Authorisierung und Verschlüsselung bieten, müssen diese Anforderungen bei Bedarf mittels VPN-Technologie abgedeckt werden.

2.4.4 Web-Applikationen

BDEW 2.4.4	*Neben allgemeinen Aspekten der sicheren Anwendungsprogrammierung sind bei Web-Applikationen besonders die folgenden Punkte zu berücksichtigen:* • *Die Applikation ist in verschiedene Module (z. B. Präsentations-, Anwendungs- und Datenschicht) zu trennen. Gegebenenfalls sind diese Module auf verschiedene Server zu verteilen.* • *Die verschiedenen Komponenten und Prozesse sind mit den minimal möglichen Rechten zu betreiben, sowohl auf Anwendungs- als auch auf Systemebene.* • *Sämtliche Parameter, die vom Anwender (bzw. seinem Web-Browser) an die Web-Anwendung gesendet werden sind genau auf Gültigkeit, maximale Länge sowie auf korrekten Typ und Wertebereich hin zu überprüfen. Dies gilt auch für Parameter, die von der Web-Anwendung selbst in einem vorhergehenden Schritt zum Anwender geschickt wurden. Dabei ist insbesondere auf sog. XSS- und Injection-Sicherheitslücken zu achten, über die ein Angreifer eigene Kommandos ausführen kann.* • *Es ist besonders auf sicheres Session-Management zu achten, z. B. durch verschlüsselte oder signierte Session-IDs und zeitbeschränkte Sessions. Die Übertragung von Session-IDs ist durch SSL-Verschlüsselung zu schützen.* • *Der Anwender soll zwar bei Fehlverhalten mit Fehlermeldungen informiert werden, dabei dürfen aber keine für einen Angreifer verwertbaren Informationen mitgeliefert werden. Solche Informationen dürfen ausschließlich in einem nur intern zugänglichen Logfile gespeichert werden.* • *Web-Anwendungen mit hohem Schutzbedarf sollten vor Inbetriebnahme einem Sicherheits-Audit unterzogen werden.*

SICAM RTUs

In SICAM RTUs werden bei Verwendung der SICAM TOOLBOX II alle WEB-Applikationen (WEB-Parametrierung) deaktiviert.

Aktuelle SICAM RTUs unterstützen einen https-Webserver für den abgesetzten Betrieb mit SICAM TOOLBOX II oder WEB-Parametrierung.

Hinweis

Info für Projektplanung/-umsetzung:

Bei hohen Security-Anforderungen sollte auf die Verwendung der WEB-Parametrierung von SICAM RTUs verzichtet werden.

SICAM TOOLBOX II

Die SICAM TOOLBOX II verfügt über keine WEB-Applikationen oder WEB-Services.

Das WEB-Engineering der SICAM TOOLBOX II ist mittels Remote Desktop Services (RDS), Remote Desktop Protocol (RDP) und Remote Desktop Connection Client (RDC) realisiert und verwendet keine WEB-Technologien.

2.4.5 Integritätsprüfung relevanter Daten

BDEW 2.4.5	*Die Integrität von Daten, die in sicherheitsrelevanten Aktionen verarbeitet werden, muss vor der Verarbeitung überprüft werden (beispielsweise auf Plausibilität, korrekte Syntax und Wertebereich).*

SICAM RTUs

Sicherheitsrelevante Aktionen wie z.B. Befehlsgabe werden in SICAM RTUs vor der Verarbeitung überprüft (Plausibilität, korrekte Syntax, Wertebereich).

SICAM TOOLBOX II

Die SICAM TOOLBOX II wird mittels Windows-Installer installiert, somit stehen die dort verwendeten Sicherheitsmechanismen zur Wahrung der Applikationsintegrität zur Verfügung.

Die Integrität der Anwendungsdaten ist durch die Mechanismen auf Betriebssystem- und Datenbankebene sichergestellt.

2.4.6 Protokollierung, Audit-Trails, Timestamps, Alarmkonzepte

BDEW 2.4.6	*a) Jedes System muss über eine einheitliche Systemzeit verfügen und die Möglichkeit zur Synchronisation dieser Systemzeit mit einer externen 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) Das Logging von Events soll einfach konfigurierbar und modifizierbar sein.* *d) Sicherheitsrelevante Events sollen in den Systemlogs als solche markiert werden, um eine automatische Auswertung zu erleichtern.* *e) Die zentrale Speicherung der Logdateien erfolgt an einem frei konfigurierbarem Ort.* *f) Ein Mechanismus zur automatisierten Übertragung des Logfiles auf zentrale Komponenten muss zur Verfügung stehen.* *g) Das Logfile muss gegen spätere Modifikation geschützt sein.* *h) Das Logfile darf nur von der Benutzerrolle Auditor archiviert werden können.* *i) Bei Überlauf des Logfiles werden die älteren Einträge überschrieben, das System muss bei knapp werdendem Logging-Speicherplatz warnen.* *j) Es muss möglich sein, sicherheitsrelevante Meldungen in ein vorhandenes Alarmmanagement aufzunehmen.*

SICAM RTUs

a) SICAM RTUs stellen mehrere Möglichkeiten der Zeitsynchronisation zur Verfügung, z.B. NTP, GPS, DCF77, …

b) In SICAM RTUs steht die Historydiagnose zur Verfügung, in welche alle auftretenden Fehler (z.B.: abgewiesener Befehl wegen Zeitdifferenz/Befehlsalter) chronologisch mit Zeit und Datum resetsicher eingetragen werden. Diese Historydiagnose kann mittels SICAM TOOLBOX II lokal oder über die Ferne ausgelesen werden.
Des weiteren steht in SICAM RTUs ein Security Logbuch zur Verfügung, wobei die Ereignisse mittels Syslog-Client an einen Syslog-Server übertragen werden.

c) Die Historydiagnose ist in SICAM RTUs fix konfiguriert, das Security Logbuch in SICAM RTUs incl. Syslog-Client kann bei Bedarf aktiviert werden.

d) Die Historydiagnose in SICAM RTUs behandelt alle Events gleich, das Security Logbuch in SICAM RTUs unterscheidet mehrere Facility-Types und Severities.

e) Die Historydiagnose in SICAM RTUs wird lokal gespeichert und kann mittels SICAM TOOLBOX II über die Ferne ausgelesen und abgespeichert werden.
Die Security Logbuch Einträge in SICAM RTUs werden mittels Syslog-Client an einen Syslog-Server übertragen.

f) Die Historydiagnose in SICAM RTUs wird lokal gespeichert und kann mittels SICAM TOOLBOX II über die Ferne ausgelesen und abgespeichert werden.
Die Security Logbuch Einträge in SICAM RTUs werden mittels Syslog-Client an einen Syslog-Server übertragen.

g) Die Historydiagnose in SICAM RTUs wird lokal gespeichert, Einträge können nicht modifiziert oder gelöscht werden.
Die Security Logbuch Einträge in SICAM RTUs werden mittels Syslog-Client an einen Syslog-Server übertragen, in welchem diese gegen Manipulation geschützt werden können.

h) Die Historydiagnose in SICAM RTUs wird lokal gespeichert, Einträge können nicht modifiziert oder gelöscht werden. (Archiviert = an einen anderen Ort kopieren und im Original löschen).
Die Security Logbuch Einträge in SICAM RTUs werden mittels Syslog-Client an einen Syslog-Server übertragen, in welchem die Benutzerrolle „Auditor“ angewendet werden kann.

i) Die Historydiagnose in SICAM RTUs überschreibt ältere Einträge bei Überlauf, eine Warnmöglichkeit bei Überlauf ist nicht vorhanden.
Die Security Logbuch Einträge in SICAM RTUs werden mittels Syslog-Client an einen Syslog-Server übertragen. Die Übertragung erfolgt unquittiert mittels UDP.

j) SICAM RTUs beinhalten ein umfassendes Alarmmanagement, in dem auftretende Fehler im gesamten System in einer komprimierten Form zur Verfügung stehen (Summenfehler, Summenstörung). Eine eventuell notwendige Detaildiagnose erfolgt zentral mittels SICAM TOOLBOX II .
Die Security Logbuch Einträge in SICAM RTUs werden mittels Syslog-Client an einen Syslog-Server übertragen.

SICAM TOOLBOX II

a) Die Zeitsynchronisation ist kein Bestandteil der SICAM TOOLBOX II, sondern Aufgabe des Betriebssystems

b) Die SICAM TOOLBOX II verfügt über ein Logbuch, in dem auswählbare Benutzeraktionen wie z.B.: Parameteränderung, Parameterdownload, Firmwareladen ins Zielsystem, … protokolliert werden können.
Des weiteren verfügt die SICAM TOOLBOX II über ein Security Logbuch, wobei die Ereignisse in das Windows-Eventlog und/oder mittels Syslog-Client an einen Syslog-Server übertragen werden.

c) Die SICAM TOOLBOX II verfügt über ein Logbuch, in dem auswählbare Benutzeraktionen wie z.B.: Parameteränderung, Parameterdownload, Firmwareladen ins Zielsystem, … protokolliert werden können.
Des weiteren verfügt die SICAM TOOLBOX II über ein Security Logbuch incl. Syslog-Client, welches bei Bedarf aktiviert werden kann. Hierfür ist das Benutzerrecht „Security Administrator“ erforderlich.

d) Die Einträge des SICAM TOOLBOX II – Logbuchs können beliebig gefiltert werden.
Die Einträge des SICAM TOOLBOX II – Security Logbuchs unterscheiden mehrere Facility-Types und Severities.

e) Das SICAM TOOLBOX II – Logbuch wird zentral in der SICAM TOOLBOX II Datenbank gespeichert.
Die Security Logbuch Einträge in SICAM TOOLBOX II werden mittels Syslog-Client an einen Syslog-Server übertragen.

f) Das SICAM TOOLBOX II – Logbuch wird zentral in der SICAM TOOLBOX II Datenbank gespeichert, das gilt auch für den Betrieb mehrerer SICAM TOOLBOX II Clients mit einer Netzdatenbank.
Die Security Logbuch Einträge in SICAM TOOLBOX II werden mittels Syslog-Client an einen Syslog-Server übertragen.

g) Das SICAM TOOLBOX II – Logbuch ist durch die Rollenverwaltung der SICAM TOOLBOX II geregelt, die Zugriffsrechte, somit auch das Recht Datensätze zu löschen, können vom SICAM TOOLBOX II Administrator vergeben werden.
Die Security Logbuch Einträge in SICAM TOOLBOX II werden mittels Syslog-Client an einen Syslog-Server übertragen, in welchem diese gegen Manipulation geschützt werden können.

Hinweis

Info für Projektplanung/-umsetzung:

Bei hohen Security-Anforderungen sollten das Löschrecht auf Datensätze des SICAM TOOLBOX II Logbuchs (=Logbuch konfigurieren) allen Rollen entzogen werden.

h) Das SICAM TOOLBOX II – Logbuch ist durch die Rollenverwaltung der SICAM TOOLBOX II geregelt, die Zugriffsrechte, somit auch das Recht Datensätze zu archivieren (=exportieren + löschen), können vom SICAM TOOLBOX II Administrator vergeben werden.
Die Security Logbuch Einträge in SICAM TOOLBOX II werden mittels Syslog-Client an einen Syslog-Server übertragen, in welchem die Benutzerrolle Auditor angewendet werden kann.

i) Das SICAM TOOLBOX II – Logbuch überschreibt ältere Einträge nicht, es kann eine „Warnschwelle“ bei einer definierten Anzahl von Einträgen definiert werden.
Die Security Logbuch Einträge in SICAM TOOLBOX II werden mittels Syslog-Client an einen Syslog-Server übertragen. Die Übertragung erfolgt unquittiert mittels UDP.

j) Das SICAM TOOLBOX II – Logbuch kann nicht in ein zentrales Alarmmanagement aufgenommen werden.
Die Security Logbuch Einträge in SICAM TOOLBOX II werden mittels Syslog-Client an einen Syslog-Server übertragen.

Hinweis

Info für Projektplanung/-umsetzung:

Bei Bedarf kann durch eine Systemlösung das SICAM TOOLBOX II Logbuch mittels Oracle-Zugriff ausgelesen und in ein zentrales Alarmmanagement eingebunden werden.

2.4.7 Self-Test und System-Verhalten

BDEW 2.4.7	*Das System bzw. die sicherheitsspezifischen Module sollen beim Start und in regelmäßigen Abständen interne Konsistenz-Prüfungen von sicherheitsrelevanten Einstellungen und Daten durchführen. Beim Versagen dieser Konsistenzprüfungen oder sicherheitsrelevanter Komponenten muss das System in einen Betriebszustand übergehen, der die primären Systemfunktionen aufrecht erhält, solange Gefährdungen oder Schäden für Anlagen und Personen ausgeschlossen sind.*

SICAM RTUs

SICAM RTUs führen beim Start und in regelmäßigen Abständen interne Konsistenz-Prüfungen von sicherheitsrelevanten Einstellungen und Daten durch. Beim Versagen dieser Konsistenzprüfungen oder sicherheitsrelevanter Komponenten wird das entsprechende Modul deaktiviert um Gefährdungen oder Schäden für Anlagen oder Personen auszuschließen.

Durch das modulare Design von SICAM RTUs werden nur direkt betroffene Teile deaktiviert, während alle anderen Funktionen weiterlaufen (z.B.: Regelbaugruppe läuft bei Defekt der Kommunikationsbaugruppe weiter).

SICAM TOOLBOX II

Die SICAM TOOLBOX II verwendet zur Konsistenzprüfung Funktionen der Betriebssystem- und Datenbankebene.

Da es sich bei der SICAM TOOLBOX II um ein Parametrier- und Diagnosewerkzeug und kein Betriebsführungssystem handelt, hat die SICAM TOOLBOX II keine Auswirkung auf Systemfunktionen.

2.5 Entwicklung, Test und Rollout

2.5.1 Sichere Entwicklungsstandards, Qualitätsmanagement und Freigabeprozesse

BDEW 2.5.1	*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. Das Testen des Systems erfolgt nach dem 4-Augenprinzip: Entwicklung und Tests werden von verschiedenen Personen durchgeführt. Die Testpläne und –prozeduren, sowie erwartete und tatsächliche Testergebnisse müssen dokumentiert und nachvollziehbar sein, sie können vom Auftraggeber eingesehen werden.* *c) Der Auftragnehmer muss über einen dokumentierten Entwicklungs-Sicherheitsprozess verfügen, der die physikalische, organisatorische und personelle Sicherheit abdeckt und die Integrität und Vertraulichkeit des Systems schützt. Die Effektivität des o.g. Prozesses kann durch ein externes Audit überprüft werden.* *d) 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.* *e) Die Freigabe des Systems bzw. von Updates/Sicherheitspatches muss anhand eines spezifizierten und dokumentierten Freigabe-Prozesses stattfinden.*

a) Die SICAM RTUs und SICAM TOOLBOX II werden von zuverlässigen und geschulten Mitarbeitern entwickelt.
Beispielsweise wurde die gesamte Entwicklungsmannschaft zum Thema "Secure Coding" ausführlich geschult.

b) Die Siemens AG entwickelt die SICAM RTUs und SICAM TOOLBOX II nach dem anerkannten CMMI Entwicklungs- und Qualitätssicherungsprozess.

Entwicklung und Tests werden von verschiedenen Personen durchgeführt. Die Testpläne und –prozeduren, sowie erwartete und tatsächliche Testergebnisse werden dokumentiert und sind nachvollziehbar.

c) Die Siemens AG verfügt über einen dokumentierten Entwicklungs-Sicherheitsprozess für die SICAM RTUs und SICAM TOOLBOX II, der die physikalische, organisatorische und personelle Sicherheit abdeckt und die Integrität und Vertraulichkeit des Systems schützt. Die Effektivität des o.g. Prozesses kann durch ein externes Audit überprüft werden.

d) Die Siemens AG verfügt über eine Programmierrichtlinie für die SICAM RTUs und SICAM TOOLBOX II, in der auf sicherheitsrelevante Anforderungen explizit eingegangen wird: So werden z. B. unsichere Programmiertechniken und Funktionen vermieden. Eingabedaten werde verifiziert, um z.B. Pufferüberlauf-Fehler zu verhindern. Wo möglich, werden sicherheitserhöhende Compileroptionen und Bibliotheken benutzt.

e) Die Freigabe neuer Firmwarereleases für SICAM RTUs sowie neuer Releases des Produkts SICAM TOOLBOX II findet anhand eines spezifizierten und dokumentierten Freigabe-Prozesses statt.
Das gilt analog für Sicherheitspatches der beiden Produkte.

2.5.2 Sichere Datenhaltung und Übertragung

BDEW 2.5.2	*Sensible Daten des Auftraggebers, die im Entwicklungs- und Wartungsprozess benötigt werden oder anfallen, dürfen über ungeschützte Verbindungen nur verschlüsselt übertragen werden. Gegebenenfalls, z. B. bei der Nutzung auf mobilen Systemen, dürfen solche Daten auch nur verschlüsselt gespeichert werden. Das betrifft z. B. interne Informationen und Dokumente des Auftraggebers, aber auch Protokolldateien, Fehleranalysen und relevante Systemdokumentation. Die Menge und die Dauer der Aufbewahrung der gespeicherten Daten muss auf das notwendige Minimum beschränkt sein.*

Hinweis

Info für Projektplanung/-umsetzung und Produkt-/Systemservice:

Diese Anforderung ist nicht produktrelevant, und ist während Projektplanung/-umsetzung und Produkt-/Systemservice zu berücksichtigen

2.5.3 Sichere Entwicklungs-, Test- und Staging-Systeme, Integritäts-Prüfung

BDEW 2.5.3	*a) Die Entwicklung muss auf sicheren Systemen erfolgen, die Entwicklungsumgebung, Quellcode und Binärdateien sind gegen fremde Zugriffe zu sichern.* *b) Entwicklung und Test des Systems sowie von Updates, Erweiterungen und Sicherheitspatches muss in einer vom Produktivsystem getrennten Staging- Umgebung erfolgen.* *c) Auf Produktiv-Systemen darf 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.*

SICAM RTUs

a) Die Produktentwicklung von SICAM RTUs erfolgt auf sicheren Systemen. Die Entwicklungsumgebung, Quellcode und Binärdateien sind gegen fremde Zugriffe gesichert.
Die Entwicklungsrechner werden durch den Einsatz von ständig aktualisierten Virenscannern und zentralen Updatemechanismen für Betriebssystem- und Applikationspatches auf Letztstand gehalten.

b) Die Produktentwicklung und der Test von SICAM RTUs sowie von Updates, Erweiterungen und Sicherheitspatches erfolgt in einer vom Produktivsystem getrennten Testumgebung.

c) Der Source-Code der SICAM RTUs ist nur bei der Siemens AG verfügbar. Auf Produktiv-Systemen wird kein Source-Code gespeichert.

d) Die Integrität der SICAM RTUs Firmware- und Parameter-Binaries wird auf dem Zielsystem auf unerlaubte Veränderungen hin überprüft. Hierzu sind alle Binaries mittels Prüfsummen gesichert.

e) Bei SICAM RTUs wird eine Versionshistorie für die gesamte Software geführt, die es ermöglicht die durchgeführten Softwareänderungen nachzuvollziehen.

SICAM TOOLBOX II

a) Die Produktentwicklung der SICAM TOOLBOX II erfolgt auf sicheren Systemen. Die Entwicklungsumgebung, Quellcode und Binärdateien sind gegen fremde Zugriffe gesichert.
Die Entwicklungsrechner werden durch den Einsatz von ständig aktualisierten Virenscannern und zentralen Updatemechanismen für Betriebssystem- und Applikationspatches auf Letztstand gehalten.

b) Die Produktentwicklung und der Test der SICAM TOOLBOX II sowie von Updates, Erweiterungen und Sicherheitspatches erfolgt in einer vom Produktivsystem getrennten Testumgebung.

c) Der Source-Code des Produkts SICAM TOOLBOX II ist nur bei der Siemens AG verfügbar. Auf Produktiv-Systemen wird kein Source-Code gespeichert.

d) Die SICAM TOOLBOX II wird mittels Windows-Installer installiert, somit stehen die dort verwendeten Sicherheitsmechanismen zur Wahrung der Applikationsintegrität zur Verfügung.

e) Beim Produkt SICAM TOOLBOX II wird eine Versionshistorie für die gesamte Software geführt, die es ermöglicht die durchgeführten Softwareänderungen nachzuvollziehen.

2.5.4 Sichere Update- und Wartungsprozesse

BDEW 2.5.4	*a) Bereitstellung und Installation von Updates, Erweiterungen und Patches muss nach einem definierten Prozess und nach Rücksprache mit dem Auftraggeber erfolgen.* *b) Von Seiten des Auftragnehmers muss die Wartung durch einen definierten, geschulten Personenkreis und von speziell gesicherten Systemen aus erfolgen.*

Hinweis

Info für Projektplanung/-Umsetzung und Systemservice:

Produktseitige Updates für SICAM RTUs und SICAM TOOLBOX II werden von der Siemens EA PRO zur Verfügung gestellt.

Das Update von Anlagen ist jedoch anlagenspezifisch zu definieren und vertraglich zu regeln.

2.5.5 Konfigurations- und Change- Management, Rollbackmöglichkeiten

BDEW 2.5.5	*a) Das System muss mit einem Konfigurations- und Changemanagement entwickelt und betrieben werden.* *b) Das System muss ein Rollback auf eine festgelegte Anzahl von Konfigurationszuständen unterstützen.*

a) SICAM RTUs und SICAM TOOLBOX II werden unter Anwendung eines Konfigurations- und Changemanagement entwickelt.

b) **Hinweis**

Info für Projektplanung/-Umsetzung und Systemservice:

Ein Rollback auf ältere Firmwareversionen einer Anlagenkonfiguration kann bei SICAM RTUs firmwarespezifisch erfolgen, da ältere Firmwarerevisionen in der SICAM

TOOLBOX II Datenbank vorhanden sind.

Ein Rollback auf ältere Parameterstände einer Anlagenkonfiguration ist durch regelmäßiges Erstellen von Backups im Rahmen der Projektplanung/-umsetzung und Produkt-/Systemservice einfach möglich

Diese Anforderung ist nicht produktrelevant, und ist bei Projektplanung/-umsetzung und Systemservice zu berücksichtigen.

2.5.6 Behandlung von Sicherheitslücken

BDEW 2.5.6	*Der Auftragnehmer muss über einen dokumentierten Prozess verfügen, um Sicherheitslücken zu behandeln. Innerhalb dieses Prozesses soll 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, gefixt und an alle System-Besitzer 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.*

Die Siemens AG verfügt für SICAM RTUs und SICAM TOOLBOX II über einen dokumentierten Prozess um Sicherheitslücken zu behandeln.

Innerhalb dieses Prozesses ist es allen Beteiligten, aber auch Außenstehenden möglich, tatsächliche oder potentielle Sicherheitslücken für SICAM RTUs und SICAM TOOLBOX II zu melden.

Für SICAM RTUs und SICAM TOOLBOX II stehen Informationen zu Sicherheitsproblemen zeitnah zur Verfügung, auch wenn noch kein Patch zur Behebung des Problems zur Verfügung steht.

Hinweis

Info für Projektplanung/-umsetzung und Systemservice:

Die SICAM TOOLBOX II setzt auf Microsoft Windows als Betriebssystem auf.
Die Betrachtung der Sicherheitslücken der SICAM TOOLBOX II umfasst weder Betriebssystem noch Standardapplikationen des Computers, auf dem die SICAM TOOLBOX II als Applikation installiert ist.

2.5.7 Sourcecode-Hinterlegung

BDEW 2.5.7	*Bei Bedarf ist die Hinterlegung des Quellcodes und der entsprechenden Dokumentation bei einem Treuhänder zu vereinbaren, um beispielsweise im Falle einer Insolvenz des Auftragnehmers sicherheitskritische Updates zu ermöglichen.*

Hinweis

Siemens schließt eine Hinterlegung des Sourcecode aus. Ein hinterlegter Sourcecode wird im Normalfall nicht gewartet und ist im tatsächlichen Bedarfsfall einer Insolvenz kaum anwendbar.

2.6 Datensicherung/-wiederherstellung und Notfallplanung

2.6.1 Backup: Konzept, Verfahren, Dokumentation, Tests

BDEW 2.6.1	*Es müssen dokumentierte Verfahren zur Datensicherung und –wiederherstellung der einzelnen Anwendungen bzw. des Gesamtsystems und der jeweiligen Konfigurationen existieren. Die Konfigurationsparameter von dezentralen Komponenten müssen zentral gesichert werden können. Die Verfahren werden vom Auftraggeber regelmäßig einem Test unterzogen. Die Dokumentation und die Verfahren müssen bei relevanten System-Updates angepasst und erneut getestet werden. Das Datensicherungs-Verfahren soll eine Prüf-Operation gegen den aktuellen Datenstand ermöglichen und auch den Schutzbedarf der zu sichernden Daten berücksichtigen (z. B. durch Verwendung von Verschlüsselung).*

Für SICAM RTUs und SICAM TOOLBOX II existieren Verfahren zur Datensicherung und –wiederherstellung der einzelnen Anwendungen bzw. des Gesamtsystems und der jeweiligen Konfigurationen. Diese sind im Dokument *SICAM RTUs / SICAM TOOLBOX II Administrator Security-Handbuch* dokumentiert.

Die Konfigurationsparameter von dezentralen SICAM RTUs Komponenten werden zentral in der SICAM TOOLBOX II gespeichert.

Hinweis

Info für Projektplanung/-umsetzung und Systembetrieb:

Im Rahmen der Systementwicklung sind Konzepte und Verfahren zu Backup und Restore der Gesamtanlage zu erstellen, wie z.B.: die Automatisierung des Backupprozesses.

Im Rahmen der Projektplanung/-umsetzung muss definiert werden wer welche Verantwortungen beim Systembetrieb hat, und wann Verantwortungsübergänge sind (z.B.: Site Acceptance Test, Ende Probebetrieb, Ende Garantie, …).

Im Rahmen des Systembetriebes müssen die Verfahren zu Backup und Restore zyklisch getestet werden, weiters muss der Status der Backuperstellung laufend überwacht werden.

2.6.2 Notfallkonzeption und Wiederanlaufplanung

BDEW 2.6.2	*Für relevante Notfall- und Krisenszenarien müssen vom Auftragnehmer dokumentierte Betriebskonzepte und getestete Wiederanlaufpläne (inklusive Angabe der Wiederherstellungszeiten) zur Verfügung gestellt werden. Die Dokumentation und Verfahren werden bei relevanten System- Updates angepasst und im Rahmen des Abnahmeverfahrens für Release-Wechsel erneut getestet.*

Hinweis

Info für Projektplanung/-umsetzung und Systembetrieb:

Diese Anforderung ist nicht produktrelevant, und ist während Projektplanung/-umsetzung und Systemservice zu berücksichtigen

Literaturverzeichnis

BDEW Whitepaper – Anforderungen an sichere Steuerungs- und Telekommunikationssysteme	Version 1.0
Oesterreichs Energie und DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE Gemeinsame Ausführungshinweise zur Anwendung des BDEW Whitepaper	Arbeitsversion 2.01

Glossar

A

AAA-Server

Ein AAA-Server (Authentification, Authorization, and Accounting) ist ein System, das fundamentale Systemzugangsfunktionen verwaltet: Die Authentifizierung, Autorisierung und Benutzung sowie deren Abrechnung.

Authentifizierung

Vorgang zur Überprüfung der Identität einer Person.

B

BDEW

Bundesverband **d**er **E**nergie- und **W**asserwirtschaft

BDEW Whitepaper

"BDEW Whitepaper – Anforderungen an sichere Steuerungs- und Telekommunikationssysteme",

Dieses Dokument definiert grundlegende Sicherheitsmaßnahmen und Anforderungen für IT-basierte Steuerungs-, Automatisierungs-und Telekommunikations-Systeme, unter Berücksichtigung der allgemeinen technischen und betrieblichen Voraussetzungen.

C

CIP

Critical **I**nfrastructure **P**rotection

CRC

Cyclic **R**edundancy **C**heck

Zyklische Redundanzprüfung

D

DoS

Denial **o**f **S**ervice (Dienstverweigerung oder -ablehnung)

So wird in der digitalen Datenverarbeitung die Folge einer Überlastung von Infrastruktursystemen bezeichnet. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Host (Server), einen Rechner oder sonstige Komponenten in einem Datennetz.

M

Malware

oder Malicious code = bösartige Software, Schadprogramme

N

NERC

North American **E**lectric **R**eliability **C**ouncil (Corporation?)

NIP

Netzwerk Schnittstellen-Prozessor (**N**etwork **I**nterface **P**rocessor)

Der NIP dient der Ankopplung von SICAM Systemen an ein Ethernet LAN gemäß IEEE 802.3

P

Patch

Ein Patch (englische Bezeichnung für "Flicken", auch "Bug fix" genannt) ist ein kleines Programm, das z.B. Bugs (Fehler) von in der Regel großen Anwendungsprogrammen repariert.

S

SSL

Secure **S**ockets **L**ayer -> TLS

T

TLS

Transport **L**ayer **S**ecurity

TLS, weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert, wobei Version 1.0 von TLS der Version 3.1 von SSL entspricht.