SIEMENS

SICAM RTUs
SICAM TOOLBOX II

BDEW Conformance

DC0-113-2.04

Document Label:
SICRTUs-HBBDEWCONFORMANCE-ENG_V2.04
Issuing date
2015.03.02

Preface

Contents of the Manual

This Declaration of Conformance describes the conformance of the

products

- SICAM RTU hardware and firmware, having a delivery release in October 2011 or later (for details see *Scope of Validity*)
- SICAM TOOLBOX II V5.0 or higher.

with the

- *BDEW White Paper - "Requirements for Secure Control and Telecommunication Systems" V1.0* dated 10 June 2008

Scope of Validity

This document is valid for the products of the SICAM RTU product line with hardware and firmware versions dated October 2011 or later and for the SICAM TOOLBOX II Engineering System for Parameterization, Diagnostics, Simulation, …V5.0 or higher.

More specifically, this includes:

- SICAM AK
- SICAM TM
- SICAM CMIC
- SICAM EMIC
- SICAM BC
- SICAM TOOLBOX II
  (as application, includes neither hardware, nor an operating system or other standard software such as Microsoft Office or Adobe Acrobat Reader)

Note

This document only describes product characteristics of SICAM RTUs and of SICAM TOOLBOX II. It does not describe any system characteristics that result from system-specific networking and parameterizing of the products into an system.

The comments described in this document relate to the fields of:

- product development
- product service

The following fields are not covered:

- system integration (system, consisting of individual SICAM RTU components and other components such as network components, protective devices, …)
- project planning/implementation
- system service
- control center operation / system operation

Target Group

This document is destined primarily for persons active in the following areas:

- sales of systems and equipment

- project planning/implementation
- system service
- system operation

Conventions Used

Manuals referred to are represented in italics such as e.g. *Common Functions, System and Basic System Elements*, Section *Information Objects*.

Note

is important information about the product, the handling of the product or the respective part of the documentation, to which special attention is to be given.

Table of Contens

1 Introduction

Contents

1.1 General Information

This document describes the conformance of the SICAM RTUs product line and of SICAM TOOLBOX II with the security requirements specified in the *BDEW White Paper – "Requirements for Secure Control and Telecommunication Systems"*.

1.2 Objectives

- To protect control systems including subsystems appropriately against security threats in everyday operations, to minimize the consequences of threats on operations, to maintain business operations even in the event of security related incidents and/or to restore a defined minimum of services and service quality as fast as possible.
- To continue to adapt these systems to the changing security threats on an ongoing basis so that they are adequately protected and the residual risk is minimized.
- To provide the basis for the submission of bids.

1.3 Instructions for Use

Chapter 2 of this document (*BDEW Security Requirements*) describes the implementation of the requirements contained in the BDEW White Paper. To make it easy to establish a relationship between requirements from the BDEW White Paper and their implementation for SICAM RTUs, chapter numbers and names from the BDEW White Paper were also used herein.

This means, for example, that the implementation of the BDEW Requirement 2.4.3 - Application Protocols is described herein in *Chapter 2.4.3 Application Protocols*.

The following table provides an overview showing which areas (product/system development, project planning/implementation, product/system service, control center operation/system operation) the security requirements relate to, according to *Oesterreichs Energie* and *DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE*.

No.	BDEW Security Requirement	Product /System Development	Project Planning/ Implementation	Product/System Service	Control Center Operation/ System Operation
2.1	General Requirements and Housekeeping				
2.1.1	General				
2.1.1.1	Secure System Architecture	✓	✓	✓	✓
2.1.1.2	Contact Person	-	✓	✓	✓
2.1.1.3	Patching and Patch Management	✓	✓	-	-
2.1.1.4	Provision of Security Patches for all System Components	✓	✓	✓	✓
2.1.1.5	Third Party Support	✓	✓	✓	✓
2.1.1.6	Encryption of Sensitive Data during Storage and Transmission	✓	✓	✓	-
2.1.1.7	Cryptographic Standards	✓	✓	-	-

No.	BDEW Security Requirement	Product /System Development	Project Planning/ Implementation	Product/System Service	Control Center Operation/ System Operation
2.1.1.8	Internal and External Software and Security Tests and Related Documentation	✓	✓	-	-
2.1.1.9	Secure Standard Configuration, Installation and Start-Up	✓	✓	-	-
2.1.1.10	Integrity Checks	✓	✓	-	-
2.1.2	Documentation				
2.1.2.1	Design Documentation, Specification of Security Relevant System Components and Implementation Characteristics	✓	✓	-	-
2.1.2.2	Administrator- and User Documentation	✓	✓	-	-
2.1.2.3	Documentation of Security Parameters and Security Log Events or Warnings	✓	✓	-	-
2.1.2.4	Documentation of Requirements and Assumptions needed for Secure System Operation	-	✓	-	-
2.2	Base System				
2.2.1	System Hardening	✓	✓	✓	-
2.2.2	Anti Virus Software	✓	✓	✓	-
2.2.3	Autonomous User Authentication	-	✓	✓	-
2.3	Networks / Communication				
2.3.1	Secure Network Design and Communication Standards				
2.3.1.1	Deployed Communication Technologies and Network Protocols	✓	✓	-	✓
2.3.1.2	Secure Network Design	-	✓	✓	✓
2.3.1.3	Documentation of Netzwork Design and Configuration	-	✓	✓	✓
2.3.2	Secure Maintenance Processes and Remote Access				
2.3.2.1	Secure Remote Access	-	-	✓	✓
2.3.2.2	Maintenance Processes	-	-	✓	✓
2.3.3	Wireless Technologies: Assessment and Security Requirements	-	✓	✓	✓
2.4	Application				
2.4.1	User Account Management				
2.4.1.1	Role-Based Access Model	✓	✓	✓	✓
2.4.1.2	User Authentication and Log-On Process	✓	✓	✓	✓
2.4.2	Authorisation of Activities on User and System Level	-	-	-	✓
2.4.3	Application Protocols	✓	✓	✓	✓
2.4.4	Web Applications	✓	-	✓	✓
2.4.5	Integrity Checks of Relevant Data	✓	-	✓	✓
2.4.6	Logging, Audit Trails, Timestamps, Alarm Concepts	✓	-	✓	✓
2.4.7	Self-Test and System Behaviour	✓	-	✓	✓
2.5	Development, Test und Rollout				
2.5.1	Secure Development Standards, Quality Management and Release Processes	✓	-	✓	✓

No.	BDEW Security Requirement	Product /System Development	Project Planning/ Implementation	Product/System Service	Control Center Operat-ion/ System Operation
2.5.2	Secure Data Storage and Transmission	-	-	✓	-
2.5.3	Secure Development, Test and Staging Systems, Integrity Checks	✓	✓	✓	-
2.5.4	Secure Update and Maintenance Processes	✓	✓	✓	-
2.5.5	Configuration and Change Management, Rollback	✓	✓	✓	-
2.5.6	Fixing Security Vulnerabilities	-	✓	✓	-
2.5.7	Source Code Escrow	-	✓	-	-
2.6	Backup, Recovery and Disaster Recovery				
2.6.1	Backup: Concept, Method, Documentation, Test	-	✓	✓	-
2.6.2	Disaster Recovery	-	✓	✓	-

2 BDEW Security Requirements

Contents

2.1 General Requirements and Housekeeping

2.1.1 General

2.1.1.1 Secure System Architecture

BDEW 2.1.1.1	*The system shall be designed and built for secure operations. Examples of secure design principles are:* ***Minimal-privileges/Need-to-know principle:*** *User and system components only possess the minimal privileges and access rights they need to fulfill a certain function. Applications and network services, for example, should not be run with administrator privileges.* ***Defence-in-depth principle:*** *Security threats are not mitigated by a single countermeasure only, but by implementing several complementary security techniques at multiple system levels.* ***Redundancy principle:*** *Due to a redundant system design the failure of a single component will not interfere with the system security functions. The system design shall reduce the likelihood and impact of problems which occur due to excessive consumption of system resources (e. g. RAM, network bandwidth) or denial-of-service attacks.*

SICAM RTUs and SICAM TOOLBOX II support techniques for the implementation of system designs that ensure the secure operation of the system.

Note

Information for project planning/implementation:

As a basis for secure system design and secure system operation, the administrator manuals for SICAM RTUs and SICAM TOOLBOX II include the following information:

- typical system configurations
- secure base configuration
- security relevant system settings, parameters, and their defaults
- measures for system hardening
- traffic matrix (communication interfaces)
- instructions for security conscious behavior (patch management, anti virus protection, backup / restore)
- patch management
- anti virus protection
- backup / restore
- explanation of security specific log and audit messages; possible causes; suitable countermeasures

These pieces of information can be used as the basis for the secure design and operation of an system.

2.1.1.2 Contact Person

BDEW 2.1.1.2	*The contractor provides a contact person, who will be the single point of contact for IT security related topics during the bidding process, the system design phase and throughout the projected period of system operations.*

Note

This requirement is not relevant to product development or product service.

Information for project planning/implementation, system service:

it must be taken into consideration within the scope of project planning/implementation and in system service.

2.1.1.3 Patching and Patch Management

BDEW 2.1.1.3	*The system shall allow the patching of all system components during normal system operation. Installation of a patch should be possible without interruption of normal system operations and with little impact on the system's availability. For example, a complete shut down of the primary generation, transmission or distribution systems should not be necessary to install updates on secondary systems. Preferentially, the patches will be installed on passive redundant components first. After a switch-over process (change of the active component in the redundant system) and a subsequent test the patch will be installed on the remaining components.* *The contractor shall support a patch management process for the entire system, this process shall manage the testing, installation and documentation of security patches and system updates. In general, it should be possible that the operating staff who administrates the systems installs the patches and updates. Installation and de-installation of patches and updates shall be authorized by the system owner and must not be performed automatically.*

SICAM RTUs

For SICAM RTUs, any firmware can be reloaded and updated separately, which ensures the patchability of the system.

During a firmware updating process, at least the module concerned will not be operational. Where an interruption of normal operations is inacceptable, the use of redundant systems can ensure operations without interruptions.

Firmware for SICAM RTUs is managed centrally by SICAM TOOLBOX II. New firmware is first stored in SICAM TOOLBOX II and then distributed to SICAM RTUs.

In the area of product development for SICAM RTUs, Siemens AG has a patch management process in place according to which all firmware releases and the enhancements and bug fixes contained in them are traceably documented.

Patch management process:

- Monitoring
  Regular scans of external information sources
  e.g.: OEM (Microsoft, Sybase), CERT community, Vulnerability Databases
- Check for relevance and classification
  Preinformation of sales-, operation- and service departments
- Implementation & Test
  of security patches or workarounds

- Release
  of security patches or workarounds;
  information of sales-, operation- and service departments

By means of the "Live Update" function of SICAM TOOLBOX II, all firmware updates for SICAM RTUs can be stored in SICAM TOOLBOX II in an automated manner, which substantially simplifies the updating process.

SICAM TOOLBOX II

SICAM TOOLBOX II is patched by means of maintenance releases and hotfixes.

In the area of development for SICAM TOOLBOX II, Siemens AG has a patch management process in place according to which all releases and the enhancements and bug fixes contained in them are traceably documented.

Note

Information for project planning/implementation, system service:

It is important to ensure by appropriate measures such as redundancy, emergency control level, manual operation, … that the impact of patching/an update of individual system components on the availability of the whole system is as low as possible.

A patch management process must be agreed with the customer, which defines workflows and responsibilities in connection with the provision, testing, installation, and documentation of security patches and updates.

2.1.1.4 Provision of Security Patches for all System Components

BDEW 2.1.1.4	*The contractor shall provide security updates for all system components throughout the entire, contractually agreed lifecycle of the system. The contractor shall obtain updates for basic system components which are not developed by the contractor but by third parties (e. g. operating system, library, database management system) from the component vendor, test them and provide them, if applicable, directly to the customer. The contractor shall provide security updates in an appropriate time frame, which will be defined in the contract specifications.*

Depending on the contractual arrangements, Siemens AG provides security updates for SICAM RTUs and SICAM TOOLBOX II throughout the entire life cycle of the product.

- The provision of updates takes place within an appropriate time frame to be agreed by contract.
- Patches will be made available only after having been subjected to thorough testing.
- Updates are to be installed by the operating personnel who administrates these systems.
- The installation of patches must be authorized by the system operator and must not be performed automatically.

SICAM RTUs

Updates of basic components not developed by Siemens AG, e.g., of operating systems or libraries, are obtained from the respective manufacturers, tested, and provided within the scope of new firmware releases.

SICAM TOOLBOX II

Updates of basic components not developed by Siemens AG, e.g., database management systems, libraries, are obtained from the respective manufacturers, tested, and provided within the scope of new firmware releases (maintenance releases, hotfixes).

2.1.1.5 Third Party Support

BDEW 2.1.1.5	*The contractor shall ensure that during the scheduled life cycle of the system security support for third-party system components (e. g. operating systems, libraries, database management systems) is available. The end-of-life terms (e. g. Last Customer Ship Date, End of Support date) shall be defined in the contract specifications.*

It is ensured that support for the system components not developed by Siemens AG and forming part of SICAM RTUs and SICAM TOOLBOX II (e.g. operating systems, database management systems,…) is available during the scheduled product life cycle.

The end-of-life terms for SICAM RTUs and SICAM TOOLBOX II define all relevant deadlines such as "last customer shipping" und "end of support".

2.1.1.6 Encryption of Sensitive Data during Storage and Transmission

BDEW 2.1.1.6	*Sensitive data shall be stored or transmitted in encrypted form only. Sensitive data may include, but is not limited to: log files, passwords, or sensitive data as defined by regulatory or legal requirements (e. g. data protection laws). If applicable, the system shall allow for the secure deletion of selected data, for example by overwriting with random data.*

SICAM RTUs

In SICAM RTUs, no passwords are stored or transmitted during parameterization by means of SICAM TOOLBOX II. User authentication and the assignment of rights are carried out in SICAM TOOLBOX II.

To enable a user-authentication of SICAM TOOLBOX II in remote operation with SICAM RTUs, it is possible to set a "Connection Password" in the SICAM RTUs which is not stored in SICAM TOOLBOX II. The HASH-Challenge-Response-method is used.

In the cause of WEB-parameterization SICAM RTUs transmit passwords encrypted (https) and not as plain text.

In SICAM RTUs preshared keys (for IPSec, SNMP) and passwords (for SICAM WEB), which are used for authentification, are stored secured.

SICAM TOOLBOX II

The transmission of passwords between client and server is encrypted.

The storage of the passwords on client and server is encrypted.

2.1.1.7 Cryptographic Standards

BDEW 2.1.1.7	*When selecting cryptographic standards, regulations and national restrictions shall be considered. Only state-of-the-art cryptographic standards and key lengths shall be used. From the current state of scientific and technical knowledge these standards and key lengths shall also be considered secure for the foreseeable future. Cryptographic algorithms developed in-house shall not be used. Whenever possible, well-known cryptographic libraries should be used when implementing cryptographic functions to avoid implementation bugs.*

SICAM RTUs and SICAM TOOLBOX II use only recognized encryption methods with key lengths that, according to the current state of the art, are considered secure.

2.1.1.8 Internal and External Software and Security Tests and Related Documentation

BDEW 2.1.1.8	*The contractor shall perform a detailed security and stress test on the individual system components as well as on the entire system and its essential functions using a representative system configuration. The team undertaking these tests shall be independent from the development team. The test procedure shall be coordinated with the customer. The results of these tests and the according documentation (software versions, test configuration, etc.) shall be provided to the customer. Additionally, the customer is allowed to carry out the tests or let them be conducted by an external third party.*

In SICAM RTUs and SICAM TOOLBOX II, the individual system components and the key functions of an integral SICAM RTUs / SICAM TOOLBOX II system are, using a representative test configuration and within the scope of type testing conducted by a department independent from the development team, subjected to extensive function, security and stress testing.

The results of the tests and the pertinent documentation (software versions, test configurations, etc.) are managed.

2.1.1.9 Secure Standard Configuration, Installation and Start-Up

BDEW 2.1.1.9	*After initial installation and start-up the system shall be configured in a fail-safe manner. This defined base configuration shall be documented. System services and daemons, data and functions, which are used during development or for system testing only shall be verifiably removed or deactivated before the systems goes productive.*

In SICAM RTUs and SICAM TOOLBOX II, all security relevant services are deactivated by default (e.g. remote maintenance, remote reset, etc.). Required services have to be activated, as necessary. In that case it is necessary to change the default password.

The documentation of the base configuration and the activated services is described in the administrator manuals for SICAM RTUs and SICAM TOOLBOX II.

Note

Information for project planning/implementation

Upon its installation, SICAM TOOLBOX II has 3 default users with default passwords. They have to be changed following the installation.

TOOLBOX II includes neither hardware, nor an operating system or other standard software such as Microsoft Office or Adobe Acrobat Reader.

The "secure default configuration and initial installation or (re)launch" of the operating system and other standard programs of a SICAM TOOLBOX II system must be carried out within the scope of project planning/implementation.

In the course of WEB parameterization it is necessary to change the default password.

2.1.1.10 Integrity Checks

BDEW 2.1.1.1	*It shall be possible to verify the integrity of system and application files and executables, configuration and application parameter files, for example through the use of check sums.*

SICAM RTUs

Firmware and parameter blocks of the SICAM RTUs are protected by check sums and are, during operation, continuously checked for their integrity.

TOOLBOX II can be used to compare firmware revisions and parameter versions in the target system and the SICAM TOOLBOX II database in order to detect possible changes.

SICAM TOOLBOX II

SICAM TOOLBOX II is installed using the Windows Installer. Therefore, the security mechanisms Windows Installer contains are available to protect the integrity of the application.

The integrity of the application data is ensured by mechanisms at the operating system and database levels.

2.1.2 Documentation

2.1.2.1 Design Documentation, Specification of Security Relevant System Components and Implementation Characteristics

BDEW 2.1.2.1	*The contractor shall provide the customer with documentation covering the high level design of the entire system. The documentation shall be available not later than the time of the acceptance test and shall include the description of the system concept and of the interaction of all system components. The documentation shall characterise especially the details, interactions and dependencies of the system components which are security relevant or which deserve special protection. Furthermore the documentation shall list and describe in brief implementation details of security related functions (e. g. used cryptographic standards).*

For SICAM RTUs and SICAM TOOLBOX II, the high level design and the fundamental system structure including the interactions of the components involved are described by typical system configurations in the administrator manual for SICAM RTUs.

Note

Information for project planning/implementation

These typical system configurations are intended to serve as examples only and do not cover all possible system configurations.

They can be used only as a starting basis for the design and the documentation of an system.

2.1.2.2 Administrator and User Documentation

BDEW 2.1.2.2	*The contractor shall provide separate user and administrator documentation. Both documentations should include a list of security functions and parameters as well as instructions and responsibilities for secure operation of the system.*

Since a user documentation as specified in the BDEW White Paper is of no relevance to the area of secondary equipment/automation engineering for SICAM RTUs and SICAM TOOLBOX II, only an administrator documentation (administrator: makes changes to the parameterization / configuration of the system) is prepared for SICAM RTUs and SICAM TOOLBOX II.

Contents of the administrator documentation for SICAM RTUs and SICAM TOOLBOX II:

- Security relevant system settings, parameters, and their defaults
- Typical system configurations
- Instructions for security conscious behavior (backup, patch management, anti virus protection)
- Explanation of security specific log and audit messages; possible causes; suitable countermeasures
- Traffic matrix (communication interfaces)
- System hardening measures

  For SICAM RTUs, the hardening measures to be used include:

  - Deactivation of unnecessary system and communication services (remote operation, remote maintenance, NTP, WEB, ….)
  - Deactivation of unnecessary default users (WEB)
  - Activation of security enhancing configuration options

For SICAM TOOLBOX II, the hardening measures to be used include:

- Deinstallation or deactivation of unnecessary software components (ST emulation, message simulation, data flow test, …)
- Deactivation of unnecessary system and communication services (remote operation, remote maintenance)
- Deactivation of unnecessary default users
- Activation of security enhancing configuration options
- Limitation of the rights of users and programs

- Backup / restore
- Secure base configuration
- …

2.1.2.3 Documentation of Security Parameters and Security Log Events or Warnings

BDEW 2.1.2.3	*The administrator documentation shall include a description of all security parameters and their default values. The documentation shall alert of the consequences of grossly insecure parameter settings. Furthermore documentation shall be provided that includes all security events, warnings and log messages the system generates, possible causes and the related administrative action that should be taken.*

The administrator documentation for SICAM RTUs and SICAM TOOLBOX II includes a description of all security relevant system settings and parameters and their default values.

The documentation alerts of the consequences of grossly insecure configuration settings. Furthermore, it explains all security specific log and audit messages and specifies possible causes and, where applicable, suitable countermeasures.

2.1.2.4 Documentation of Requirements and Assumptions needed for Secure System Operation

BDEW 2.1.2.4	*The administrator documentation shall provide a description of requirements relevant for secure systems operation. The description may contain, for example, assumptions about user behaviour and network environment or requirements for interaction and communication with other systems or networks*

Note

This requirement is not relevant to product development or product service.

Information for project planning/implementation:

The administrator documentation for SICAM RTUs and SICAM TOOLBOX II contains typical system configurations and thus a description of the requirements for a secure system operation. This includes, for example, requirements for the group of users, the network environment, and the interaction and communication with other systems and networks.

2.2 Base System

2.2.1 System Hardening

BDEW 2.2.1	*All components of the base system shall be permanently hardened according to well-known best-practise guides. Furthermore the latest security patches and service packs shall be installed. If this is technically not feasible, a documented equivalent security measure shall be implemented for a transitional period (until the requirements of 2.1.1.3 are completely fulfilled). Unnecessary user accounts, default users, system daemons, programs, network protocols and services shall be removed, or - if removal is technically not possible – shall be permanently disabled and secured against accidental re-activation. The secure base system configuration shall be reviewed and documented. Especially, the security measures required in this document which contribute to system hardening shall be carried out.*

All components of the products SICAM RTUs and SICAM TOOLBOX II are permanently hardened according to recognized best practice guides. This results in a secure base configuration of SICAM RTUs and SICAM TOOLBOX II.

The secure base configuration and the measures for system hardening are described in the administrator manuals of SICAM RTUs and SICAM TOOLBOX II.

Maintenance releases, hotfixes, and firmware that include security patches will be provided in a timely manner for SICAM RTUs and SICAM TOOLBOX II.

Note

Information or project planning/implementation and system service:

SICAM TOOLBOX II includes neither hardware, nor an operating system or other default software such as Microsoft Office or Adobe Acrobat Reader.
Basic security and system hardening of the operating system and of other default software must be designed, implemented and maintained within the scope of system development, project planning/implementation and system service.

2.2.2 Anti Virus Software

BDEW 2.2.2	*The base systems of all IP-based networked system components shall be secured with virus and malware protection software. As an alternative to installing antivirus software on each system component, the contractor may implement a comprehensive antivirus and malware protection concept, which provides an equivalent protection. The patterns of the antivirus and malware protection software shall be automatically and timely updated without using a direct connection to update-servers located in external networks like the internet. A possible implementation would be to use an internal update server. The time when the patterns are updated shall be configurable. An alternative to automatic updates is a well-defined and documented secure manual process, through which the pattern updates are installed in the system, for example on an isolated central update server.*

SICAM RTU components are embedded systems from in-house development for which no virus is known. Thus there are is anti virus software available.
In addition, the components are hardened prior to startup in order to achieve enhanced protection against possible malware.

Note

Information for project planning/implementation and system service:

SICAM TOOLBOX II includes neither hardware nor an operating system or other default software such as Microsoft Office or Adobe Acrobat Reader.
Anti virus protection must be designed and implemented within the scope of project planning/implementation.

2.2.3 Autonomous User Authentication

BDEW 2.2.3	*Data used for user identification and authentication shall not solely be obtained from sources located outside of the secure process network. Integration of user identification and authentication into a central isolated directory service within the process network should be considered.*

SICAM RTUs require no user management, as the entire parameterization takes place via SICAM TOOLBOX II.

When using WEB parameterization, user authentication is carried out separately for each device.

SICAM TOOLBOX II manages the access rights with a user/role concept. The users and roles can be created and assigned freely. The authentication of the users can be done via the operating system or within the SICAM TOOLBOX II.
When accessing SICAM RTUs with SICAM TOOLBOX II via remote operation, there is an additional user authentication provided in the SICAM RTUs by means of the "Connection Password".

2.3 Networks / Communication

2.3.1 Secure Network Design and Communication Standards

2.3.1.1 Deployed Communication Technologies and Network Protocols

BDEW 2.3.1.1	*a) If technically feasible, the systems should use only secure communication standards and protocols which provide integrity checks, authentication and, if applicable, encryption. In particular, secure communication shall be used for remote administration or transmission of user log on information. The transmission of password information in clear text is not allowed (e.g. no telnet protocol, no Unix rsh services). An up-to-date list of secure protocols can be provided by the client according to its internal formalities.* *b) The system and its network components shall be easily integrable into the network conception of the whole company. Relevant network configuration parameters like IP addresses can be managed centrally. For administration and monitoring secure protocols shall be used (SSHv2, SNMPv3). The network components shall be hardened, unnecessary services and protocols shall be deactivated, management interfaces shall be protected with ACLs.* *c) It shall be possible to integrate network components which are provided by the contractor into a central asset and patch management process.* *d) If technically feasible, the IP protocol is used on WAN lines. Unencrypted application layer protocols should be secured by encryption on lower network layers (e. g.. with SSL/TLS encryption or by using VPN technologies).* *e) If applicable, firewall friendly protocols should be used: e. g. TCP instead of UDP, OPC over network boundaries should be avoided.* *f) If shared network infrastructure components (e. g.. VLAN or MPLS technology) will be used the network with the highest protection level requirement determines the security requirements of the used hardware components and their configuration. Concurrent use of the network hardware for networks with different protection levels is permitted only if this concurrent use does not decrease the security level or the availability.*

SICAM RTUs

a) For the transmission of process data, standard protocols such as IEC-61850, IEC-60870-5-101, and IEC 60870-5-104 are used.
Since these protocols do not provide for any authentication and encryption, as yet, these requirements can be covered by means of VPN technology, where necessary. Integrity checking is performed based on CRC or check sums.

b) The network configuration parameters for all SICAM RTUs components are managed centrally by means of SICAM TOOLBOX II.

Administration and monitoring of SICAM RTUs network components are carried out by means of SICAM TOOLBOX II

The network components of SICAM RTUs are hardened, unnecessary services and protocols are deactivated, management interfaces are available to SICAM TOOLBOX II only.

c) Inventory and patch management of SICAM RTUs network components is carried out by means of SICAM TOOLBOX II.

d) The use of IP is possible via the standard protocols IEC-61850 and IEC-60870-5-104. Encryption can be implemented via VPN technology.

e) The standard protocols IEC-61850 and IEC-60870-5-104 use TCP. UDP is used only for time synchronization by means of NTP.

f) **Note**

Information for project planning/implementation:

Must be taken into consideration in system design.

SICAM TOOLBOX II

a) The remote administration of SICAM TOOLBOX II is carried out in an encrypted manner by means of Remote Desktop Protocol (RDP) and Remote Desktop Connection Client (RDC).

Remote administration of SICAM RTUs: unencrypted via TCP/IP and without password.

b) SICAM TOOLBOX II is hardened, unnecessary services and protocols are deactivated, management interfaces are available only via the operating system level.

Note

Information for project planning/implementation and system service:

SICAM TOOLBOX II builds on Microsoft Windows as operating system. Administration, monitoring, and hardening of the operating system are not part of SICAM TOOLBOX II.

c) Patches of SICAM TOOLBOX II can be installed manually or incorporated into central patch management systems.

Note

Information for project planning/implementation and system service:

SICAM TOOLBOX II builds on Microsoft Windows as operating system. Inventory and patch management of the operating system are not part of SICAM TOOLBOX II.

d) For communication via WAN connections, SICAM TOOLBOX II uses exclusively the IP protocol. Encryption is implemented via VPN technology or at the Windows operating system level.

e) SICAM TOOLBOX II uses only TCP

f) **Note**

Information for project planning/implementation:

Must be taken into consideration in system design.

2.3.1.2 Secure Network Design

BDEW 2.3.1.2	*a) Vertical network segmentation: If applicable and technically feasible the network infrastructure of the system shall be divided into multiple vertical zones with different functions and protection requirements. Where technically feasible the network zones shall be separated by firewalls, filtering routers or gateways. Network connections to external networks shall be deployed only using communication protocols approved by the customer and in compliance with the security policies in effect.* *b) Horizontal network segmentation: If applicable and technically feasible the network infrastructure of the system shall be divided into independent horizontal segments (e. g.. according to different locations), the segments shall be separated by firewalls, filtering routers or gateways.* *c) Firewalls and VPN components shall be provided and managed centrally through a defined process by the customer.*

Note

Information for project planning/implementation:

This requirement is not of relevance to the products and must be taken into consideration during system design and project planning/implementation.

2.3.1.3 Documentation of Network Design and Configuration

BDEW 2.3.1.3	*The contractor shall provide documentation which shall describe the network design and configuration, all physical, virtual and logical network connections, the network protocols used, and all network perimeter components which are part of or which interact with the system. All changes (e. g.. by updates) shall be included in the documentation using a document management process. To support the implementation of rate limiting functions for QoS and to mitigate DoS problems, the documentation provides values of normal and maximal expected data rate for all network connections.*

Note

Information for system development and project planning/implementation:

This requirement is not of relevance to the products and must be taken into consideration during system design and project planning/implementation

2.3.2 Secure Maintenance Processes and Remote Access

2.3.2.1 Secure Remote Access

BDEW 2.3.2.1	Please note: the term “maintenance” used in this document denotes all service processes commissioned by the client or system operator, e. g.. repairs, fault analyses, failure and fault corrections, system enhancements and adjustments etc. *a) It shall be possible to perform administration, maintenance and configuration of all network components via out-of-band channels, like local access, serial interfaces, network or direct control of input devices (KVM).* *b) Remote access shall be performed through dedicated central administered terminal servers which ensure isolation of the process network and which are located in a DMZ. Strong 2- factor authentication shall be used.* *c) Direct dial-in access to devices is not allowed.* *d) Remote access shall be (centrally) logged, multiple failed login-in attempts shall result in a security event audit message.* *e) All remote access possibilities and ports shall be documented.*

Note

Information for system design, product/system service, and control center/system operations:

This requirement is not of relevance to the products and must be taken into consideration during system design, product/system service, and control center/system operations.

2.3.2.2 Maintenance Processes

BDEW 2.3.2.2	*f) Interactive remote access users shall use personal accounts. For non-interactive, automated processes restricted accounts shall be used, for which interactive access is disabled.* *g) Technical measures shall ensure that remote access sessions are explicitly activated by the administrative personnel. For external service personnel the activation must be performed for each individual session. Each session shall be disconnected after a reasonable time period.* *h) Maintenance shall be performed by defined and trained contractor personnel only, using secure systems only. The systems used for remote access are physically or logically disconnected from other systems and networks during a remote access session. A physical separation should be preferred.* *i) A defined maintenance process (compare above) shall ensure that maintenance personnel can only access systems, services and data they need for maintenance tasks.* *j) The maintenance personnel shall comply with the requirements of SÜFV if it will be deployed at supra-regional utilities.* *k) Local maintenance by service personnel poses a significant security threat. Attachment of contractor’s hardware (e. g. laptops, USB devices) to the process network should be avoided. If this is not feasible, the hardware must be approved by the client, specifically secured and shall be scanned for malware before attaching it. The contractor shall provide evidence that an adequate internal security policy is implemented.*

Note

Information for product/system service and control center/system operations:

This requirement is not of relevance to the products and must be taken into consideration during product/system service and control center/system operations

2.3.3 Wireless Technologies: Assessment and Security Requirements

BDEW 2.3.3	Wireless technology like WLAN and Bluetooth shall not be used for systems with high or very high protection level requirements. In consultation with the customer WLAN technology may be deployed after a risk analysis has been performed and if the following essential security requirements are complied with: • Wireless LANs shall only be deployed in separate networks zones, which are segregated from other networks by firewalls and application level proxies. • Wireless technology shall be secured according to state-of-the-art practice. • Novel WLANs shall not interfere with existing wireless networks.

SICAM RTUs does not include any wireless technologies. Hence, this requirement is not of relevance to SICAM RTUs.

Note

Information for project planning/implementation:

If wireless technologies are being used in a system solution, then appropriate measures at the device level of the transmission facilities (e.g. wireless modem, ...) must be taken.

SICAM TOOLBOX II does not include any wireless technologies. Hence, this requirement is not of relevance to SICAM TOOLBOX II.

Note

Information for project planning/implementation:

If wireless technologies are being used on a SICAM TOOLBOX II PC, then appropriate measures at the device hardware and/or operating system levels must be taken.

2.4 Application

2.4.1 User Account Management

2.4.1.1 Role-Based Access Model

BDEW 2.4.1.1	*The system shall utilise a role-based user model, in which at least the following user roles are defined:* • ***Administrator**: A user, who installs, maintains and administrates the system. Therefore the administrator role has the authorisation and the according privileges to change the system and security configuration and settings.* • ***Auditor**: User role which solely has the permission to inspect and archive the audit logs.* • ***Operator**: User who performs regular system operations. This might include the privilege to change operational system settings.* • ***Data-Display**: User, who is allowed to view the status of the system and to read defined datasets but is not allowed to make any changes to the system.* *If applicable, a "Backup Operator" role is defined, which is allowed to backup relevant system and application data.* *The system shall allow for a granular access control on data and resources. The default access permissions shall conform to a secure system configuration. Security relevant system configuration data can only be read or changed by the administrator role. For normal system use the operator or datadisplay role permissions shall be sufficient. Individual user accounts can be disabled without removing them from the system.*

SICAM RTUs

When using SICAM TOOLBOX II, there is no user and role management in SICAM RTUs, as the user and role management is carried out in SICAM TOOLBOX II.

When using the WEB parameterization of SICAM RTUs, user authentication is carried out separately for each device.

SICAM RTUs emic provides the roles "Admin" and "Guest" (corresponds to "Administrator" and "Data Display"). There are no roles for the NIP's (in SICAM RTUs), and data can be viewed only.

SICAM TOOLBOX II

There exists a user/role function in SICAM TOOLBOX II.
Access and authorizations can be defined freely in a role specific manner, and users can be assigned roles.

A SICAM TOOLBOX II administrator can add roles to the default roles of SICAM TOOLBOX II (Administrator, Professional, Standard).

2.4.1.2 User Authentication and Log-On Process

BDEW 2.4.1.2	*l) Users shall be identified and authenticated with personal accounts, group accounts shall only be used in precise defined exceptional cases.* *m) Before allowing any actions the system shall require each user to be successfully authenticated.* *n) The system shall force passwords with configurable strength and expiration periods. The password strength and expiration period shall be configurable by the customer.* *o) If technically feasible, 2-factor authentication shall be used, for example SmartCards or security tokens.* *p) Data used for user identification and authentication shall not solely be provided from sources external to the process network. Integration with a central, process net internal directory service should be considered.* *q) Successful and failed log on attempts shall be logged centrally.* If applicable, the following items shall be implemented after paramount consideration of safe system operation and availability issues: The system should implement mechanisms which allow for a secure and reproducible switching of user session during system operations. If applicable and technically feasible user sessions should be locked after a configurable time of inactivity. After a configurable number of failed log-on attempts a security event message should be logged and, if applicable, the account should be locked out

SICAM RTUs

In SICAM RTUs, when using SICAM TOOLBOX II, the user authentication and logon feature of SICAM TOOLBOX II is used.

Additionally it is possible in remote operation to set a "Connection Password" on the SICAM RTUs for user-authentication. This password is stored in the SICAM RTUs and not in the SICAM TOOLBOX II.

When using the WEB parameterization of SICAM RTUs, user authentication and logon are carried out separately for each device via the group accounts "Administrator" and "Guest".

In SICAM RTUs you can use a security logbook which logs all successful and failed login attempts.

SICAM TOOLBOX II

- User authentication and logon takes place in one or more stages:
  - Registration on the operation system of the device (single-stage authentication/registration)
  - Registration at the SICAM TOOLBOX II application (either via the user management in SICAM TOOLBOX II or single SignOn to the SICAM TOOLBOX II with the domain user account)
  - Registration of the SICAM TOOLBOX II user to SICAM RTUs with the „Connection Password“ in remote operation (optional)
- A security logbook is provided to log successful and failed login attempts. The logged data can be transmitted automatically, by means of an integrated syslog client, to the windows event log and/or an external syslog server.

Note

Information for system development and project planning/implementation:

Using Microsoft Windows as base operating system of SICAM TOOLBOX II, all required items are

implementable during system development and/or project planning/implementation.

User identification and authentication via a central directory service within the process network is a problem for reasons of availability, as it would not be available in the event of a fault or failure (e.g. communication failure). Consequently, no system logon and trouble-shooting would be possible.

2.4.2 Authorisation of Activities on User and System Level

BDEW 2.4.2	*Before certain security relevant or security critical activities are performed the system shall check the authorisation of the requesting user or system. Relevant activities may already be read access to process data or configuration parameters.*

After the registration to SICAM TOOLBOX II, the user can exercise the rights, set out in its role. Additionally it is possible to protect the access to the SICAM RTUs with the „Connection Password“.

SICAM RTUs

In the Bay Controller BC 1703 ACP, access to local operation is controlled by means of a key switch.

SICAM CMIC and SICAM EMIC only display process states. Controlling is not possible.

Note

Information for project planning/implementation:

Security relevant/critical actions, e.g., protected command initiation, can be implemented for SICAM RTUs, e.g., by means of a key switch.
Design and implementation are of no relevance to the products and are carried out during system design and/or project planning/implementation.

SICAM TOOLBOX II

The user and role management provided in SICAM TOOLBOX II can be used to define who is allowed to carry out security-relevant/security-critical actions (e.g., ST-Emulation, LogView, Message simulation, …).

Note

Information for project planning/implementation:

The design and implementation of user and role management for SICAM TOOLBOX II is project specific or customer specific and carried out within the scope of system design and/or project planning/implementation.

2.4.3 Application Protocols

BDEW 2.4.3	*Only standard application level protocols approved by the client shall be used. Exceptions shall be approved by the customer and documented. Protocols which protect the integrity of the transferred data and ensure correct authentication and authorisation of the communication partners should be preferred. Furthermore the used protocols should provide timestamps or secure sequence numbers to prevent re-injection of prior sent messages. If applicable, encryption of the protocol data should be implemented. The previous requirements also apply to non-standard, proprietary or in-house developed protocols.*

For the transmission of process data, standard protocols such as IEC-61850, IEC-60870-5-101, IEC 60870-5-104 are used.

Some SICAM RTUs protocol elements can transmit a PING by using the WEB-Browser.

Note

Information for project planning/implementation:

Since the standard protocols IEC-61850, IEC-60870-5-101, and IEC 60870-5-104 do not provide for any authentication, authorization, and encryption, as yet, these requirements must be covered, where necessary, by using VPN technology.

2.4.4 Web Applications

BDEW 2.4.4	*Additional to common secure application programming practise, the following topics shall be regarded when web applications are being developed:* *a) The application shall be separated into different modules (e. g.. presentation, application and data layers). If applicable, the modules shall be deployed on different servers.* *b) The web application components shall be configured with the minimal possible privileges, both on the application and the system level.* *c) All parameters which are passed to the web application from the user or his web browser shall extensively be tested for validity, maximum length, correct type and range. This applies also to data which has been sent from the application to the user beforehand. Special attention shall be paid to so called XSS and data injection vulnerabilities, through which an attacker can execute commands.* *d) Especially, secure session management has to be taken into account, for example by using singed or encrypted session IDs and session timeouts. The transmission of session IDs shall be secured by encryption.* *e) In the case of application errors the user should be informed by error messages. These error messages shall not provide detailed information which can be used by an attacker to plan further attacks. Such detailed error information shall only be logged to a log file, which is accessible by internal users only.* *f) Web applications with a high protection requirement shall be tested by a security audit before going productive.*

SICAM RTUs

When using SICAM TOOLBOX II, in SICAM RTUs all WEB applications (WEB parameterization) are disabled.

Current SICAM RTUs support a https-webserver for remote operation with SICAM TOOLBOX II or WEB-parameterization.

Note

Information for project planning/implementation:

In the event of high security requirements, use of the WEB parameterization feature of SICAM RTUs should be omitted.

SICAM TOOLBOX II

SICAM TOOLBOX II does not include any WEB applications or WEB services.

The WEB engineering of SICAM TOOLBOX II is implemented by means of Remote Desktop Services (RDS), Remote Desktop Protocol (RDP), and Remote Desktop Connection Client (RDC) and does not use any WEB technologies.

2.4.5 Integrity Checks of Relevant Data

BDEW 2.4.5	The system shall check the integrity of data before this data is processed in security relevant activities, (e. g. check for plausibility, correct syntax and value ranges).

SICAM RTUs

Security relevant actions such as command initiation are checked in SICAM RTUs prior to processing (plausibility, correct syntax, value range).

SICAM TOOLBOX II

SICAM TOOLBOX II is installed by means of Windows Installer. Therefore, the security mechanisms Windows Installer contains are available to protect the integrity of the application.

The integrity of the application data is ensured by mechanisms at the operating system and database levels.

2.4.6 Logging, Audit Trails, Timestamps, Alarm Concepts

BDEW 2.4.6	*a) All systems shall use a uniform system time which can be synchronised with an external time source.* *b) The system shall log user actions and security relevant actions, events and errors to an audit trail using a format which is appropriate for later and central analysis. The system shall record date, time, involved users and systems, as well as the event and its result for a configurable time period.* *c) The logging function shall be easy to configure and customise.* *d) Security events shall be highlighted in the system logs to allow for an easy automatic analysis.* *e) The central storage location of the log files shall be configurable.* *f) A mechanism for automatic transfer of the log files to central component shall be available.* *g) The log files shall be protected against later modification.* *h) The audit log shall only be archivable by the auditor role.* *i) The system shall overwrite the oldest stored audit records if the audit trail is full. The system shall issue a warning if the storage capacity decreases below a reasonable threshold.* *j) Security relevant events shall be integrable into an existing alarm management.*

SICAM RTUs

a) SICAM RTUs provides several time synchronization options, e.g., NTP, GPS, DCF77, …

b) SICAM RTUs offers the history diagnostic in which all occurring errors (e.g. command rejected due to time difference/command age) are entered chronologically and reset-proof, together with their times and dates. This history diagnostic can be read out via SICAM TOOLBOX II, locally or from remote locations.
Further SICAM RTUs offers a security logbook, which can transfer the logged events by means of a syslog client to a syslog server.

c) The history diagnostic is permanently configured in SICAM RTUs, the security logbook including the syslog server can be activated on demand.

d) The history diagnostic in SICAM RTUs handles all events the same way.
The security logbook in SICAM RTUs differentiates between several facility types and severities.

e) The history diagnostic in SICAM RTUs is stored locally and can be read out and stored from remote locations via SICAM TOOLBOX II.
The security logbook entries in SICAM RTUs are transmitted by means of the syslog client to a syslog server.

f) The history diagnostic in SICAM RTUs is stored locally and can be read out and stored from remote locations via SICAM TOOLBOX II.
The security logbook entries in SICAM RTUs are transmitted by means of the syslog client to a syslog server.

g) The history diagnostic in SICAM RTUs is stored locally. Entries cannot be modified or deleted.
The security logbook entries in SICAM RTUs are transmitted by means of the syslog client to a syslog server which protects these data against manipulation.

h) The history diagnostic in SICAM RTUs is stored locally. Entries cannot be modified or deleted. (archived = copy to another location and delete in the original)
The security logbook entries in SICAM RTUs are transmitted by means of the syslog client to a syslog server. The user role “Auditor” can be applied on the syslog server.

i) The history diagnostic in SICAM RTUs overwrites older entries in cases of overflow. There exists no warning option for cases of overflow.
The security logbook entries in SICAM RTUs are transmitted by means of the syslog client to a syslog server. The transmission takes place without acknowledgement via UDP.

j) SICAM RTUs includes a comprehensive alarm management where occurring errors are available in a compressed form (sum error, sum fault) throughout the entire system. Any detailed diagnostic that might become necessary is carried out centrally by means of SICAM TOOLBOX II.
The security logbook entries in SICAM RTUs are transmitted by means of the syslog client to a syslog server.

SICAM TOOLBOX II

a) Time synchronization is not part of SICAM TOOLBOX II, but a task of the operating system.

b) SICAM TOOLBOX II provides a log in which selectable user actions such as Change parameters, Download parameters, Load firmware into target system … can be logged.
Further SICAM TOOLBOX II offers a security logbook, which can transfer the logged events by means of a syslog client to the windows event log and/or to a syslog server.

c) Die SICAM TOOLBOX II provides a log in which selectable user actions such as Change parameters, Download parameters, Load firmware into target system … can be logged. Further SICAM TOOLBOX II offers a security logbook including a syslog client, which can be activated on demand. The user role “Security administrator” is required for activation.

d) The entries of the SICAM TOOLBOX II log can be filtered as necessary.
The entries of the SICAM TOOLBOX II security logbook differentiate several facility types and severities.

e) The SICAM TOOLBOX II log is stored centrally in the SICAM TOOLBOX II database.
The security logbook entries in SICAM TOOLBOX II are transmitted by means of the syslog client to the syslog server.

f) The SICAM TOOLBOX II log is stored centrally in the SICAM TOOLBOX II database. This applies also to the use of several SICAM TOOLBOX II clients with a network database.
The security logbook entries in SICAM TOOLBOX II are transmitted by means of the syslog client to the syslog server.

g) The SICAM TOOLBOX II log is controlled via the role management of SICAM TOOLBOX II. Access rights and thus also the right to delete data records can be assigned by the SICAM TOOLBOX II administrator.
The security logbook entries in SICAM TOOLBOX II are transmitted by means of the syslog client to the syslog server which protects these data against manipulation.

Note

Information for project planning/implementation:

In cases of high security requirements, the right to delete data records of the SICAM TOOLBOX II log (=configure log) is to be withdrawn from all roles.

h) The SICAM TOOLBOX II log is controlled via the role management of SICAM TOOLBOX II. Access rights and thus also the right to archive (=export + delete) data records can be assigned by the SICAM TOOLBOX II administrator.
The security logbook entries in SICAM TOOLBOX II are transmitted by means of the syslog client to the syslog server. The user role “Auditor” can be applied on the syslog server.

i) The SICAM TOOLBOX II log does not overwrite older entries. At a defined number of entries, a "warning threshold" can be defined. The SICAM TOOLBOX II log cannot be integrated into a central alarm management.
The security logbook entries in SICAM TOOLBOX II are transmitted by means of the syslog client to the syslog server. The transmission takes place without acknowledgement via UDP.

j) Since SICAM TOOLBOX II is a parameterization and diagnostics tool, rather than a process management system, SICAM TOOLBOX II has no impact on system functions. The alarm management for the system is available in SICAM RTUs.
The security logbook entries in SICAM TOOLBOX II are transmitted by means of the syslog client to the syslog server.

Note

Information for project planning/implementation:

If necessary, the SICAM TOOLBOX II log can be read out via a system solution by means of Oracle access and can be integrated into a central alarm management.

2.4.7 Self-Test and System Behaviour

BDEW 2.4.7	*The system or the security modules, respectively, should perform integrity checks of security relevant settings and data at start-up and in regular intervals. If the security modules or the integrity checks fails, the system shall fall back into a system state which maintains the primary system functions as long as the prevention of personal injury or equipment damage can be ensured.*

SICAM RTUs

At startup and at regular intervals, SICAM RTUs carries out internal consistency checks of security relevant settings and data. If these consistency checks or security relevant components fail, the respective module is deactivated in order to prevent hazards for or damage to equipment and persons.

Due to the modular design of SICAM RTUs, only directly affected parts are deactivated, while all other functions continue to be active (e.g., the control module continues to be active in the case of a defect in the communication module).

SICAM TOOLBOX II

For the consistency check, SICAM TOOLBOX II uses functions of the operating system and database levels.

Since SICAM TOOLBOX II is a parameterization and diagnostics tool, rather than a process management system, SICAM TOOLBOX II has no impact on system functions.

2.5 Development, Test und Rollout

2.5.1 Secure Development Standards, Quality Management and Release Processes

BDEW 2.5.1	*a) On the contractor side, the system shall be developed by trained and trustworthy personnel. Outsourcing of the system development as a whole or in parts to third parties shall require the written approval of the customer. The third party shall at least comply with the same security requirements as the original contractor.* *b) The system shall be developed according to well known development standards and quality management/assurance processes. Development and testing of the system shall be done by independent teams. Test plans, test concepts, expected and actual test results shall be documented in a comprehensible way, they shall be available for inspection by the customer.* *c) The contractor shall have a documented development security program that covers the physical, procedural and personnel security measuresto protect the integrity and confidentiality of the system's design and implementation. The contractor shall be available for an external audit of the effectiveness of the security program.* *d) The contractor shall have a programming guideline which covers security requirements and secure programming practice. The guideline should deprecate insecure programming style and the use of insecure functions. Data input shall be verified to avoid buffer overflows. If applicable, security enhancing compiler options and libraries shall be used.* *e) System release and the release of updates and security patches shall be managed and controlled through a well-defined and documented release process.*

a) SICAM RTUs and SICAM TOOLBOX II are developed by trained and trustworthy personnel. The entire development team, for example, was given extensive training in "secure coding".

b) Siemens AG develops SICAM RTUs and SICAM TOOLBOX II according to the recognized CMMI development and quality assurance process.

   Development and testing are done by different persons. Test plans and procedures as well as expected and actual test results are documented and are comprehensible.

c) Siemens AG has a documented development security process for SICAM RTUs and SICAM TOOLBOX II, which covers physical, organizational and personnel security and protects the integrity and confidentiality of the system. The effectiveness of the above mentioned process can be checked by an external audit.

d) Siemens AG has a programming guideline for SICAM RTUs and SICAM TOOLBOX II, which explicitly addresses security relevant requirements: for example, insecure programming methods and functions are avoided. Data input is verified, e.g., to prevent buffer overflow errors. Where possible, security enhancing compiler options and libraries are used.

e) The approval of new firmware releases of SICAM RTUs and of new releases of SICAM TOOLBOX II takes place based on a specified and documented approval process. The same applies to security patches for the two products.

2.5.2 Secure Data Storage and Transmission

BDEW 2.5.2	*Sensitive customer data, which is used or produced during development and maintenance, shall be transmitted encrypted if it is sent over public networks. If the data is stored on mobile devices it shall be stored in encrypted form. Sensitive data may include, but is not limited to, internal customer information and documents, log files, error logs, and relevant system documentation. The amount of stored data and the storage time shall be limited to the necessary minimum.*

Note

Information for project planning/implementation and product/system service:

This requirement is of no relevance to the products and must be taken into consideration during project planning/implementation and product/system service.

2.5.3 Secure Development, Test and Staging Systems, Integrity Checks

BDEW 2.5.3	*a) Development shall be conducted on secure computer systems, the development environment, the source code and binaries shall be protected against unauthorised access.* *b) Development and testing of the system and of updates, enhancements and security patches shall be conducted on staging environments which shall be separated from the live system.* *c) No source code shall be installed on live systems.* *d) It shall be possible to verify the integrity of the system source code and binaries to detect unauthorised changes. For example, the integrity might be checked by secure check sums.* *e) A version history of all deployed software packages shall be maintained, which allows to trace all software changes.*

SICAM RTUs

a) Product development for SICAM RTUs is conducted on secure systems. The development environment, the source code, and binaries are protected against unauthorized access. The development computers are always kept updated through the use of continuously updated anti virus scanners and central update mechanisms for operating system and application patches.

b) Product development and testing of SICAM RTUs and of updates, enhancements, and security patches is conducted in a staging environment that is separated from the live system.

c) The source code of SICAM RTUs is available only at Siemens AG. On live systems, no source code is stored.

d) The integrity of SICAM RTUs firmware and parameter binaries is verified in the target system to detect unauthorized changes. For this purpose, all binaries are protected by check sums.

e) For SICAM RTUs, a version history for the entire software is maintained, which allows to trace all software changes.

SICAM TOOLBOX II

a) Product development for SICAM TOOLBOX II is conducted on secure systems. The development environment, the source code, and binaries are protected against unauthorized access.
The development computers are always kept updated through the use of continuously updated anti virus scanners and central update mechanisms for operating system and application patches.

b) Product development and testing of SICAM TOOLBOX II and of updates, enhancements, and security patches is conducted in a staging environment that is separated from the live system.

c) The source code of SICAM TOOLBOX II is available only at Siemens AG. On live systems, no source code is stored.

d) SICAM TOOLBOX II is installed using the Windows Installer. Therefore, the security mechanisms Windows Installer contains are available to protect the integrity of the application.

e) For SICAM TOOLBOX II, a version history for the entire software is maintained, which allows to trace all software changes.

2.5.4 Secure Update and Maintenance Processes

BDEW 2.5.4	*a) Provision and Installation of updates, enhancements and patches shall be carried out in consultation with the customer according to a welldefined process..* *b) .On the contractor side, maintenance shall be carried out by dedicated and trained personnel, using particularly secured systems.*

Note

Information for project planning/implementation and system service:

Product updates for SICAM RTUs and SICAM TOOLBOX II are provided by Siemens EA PRO.

Updates of systems, however, must be defined system specifically and be regulated by contract.

2.5.5 Configuration and Change Management, Rollback

BDEW 2.5.5	*a) The system shall be developed and maintained using a configuration and change management.* *b) The system shall support rollback of a specified number of configuration changes.*

a) SICAM RTUs and SICAM TOOLBOX II are developed using a configuration and change management.

b) **Note**

Information for project planning/implementation and system service:

Rollback to older firmware versions of a system configuration can be done firmware-specifically for SICAM RTUs, as older firmware revisions are contained in the SICAM TOOLBOX II database.

Rollback to older parameter versions of a system configuration is easy thanks to the regular creation of backups within the scope of project planning/implementation and

product/system service.

This requirement is of no relevance to the products and must be taken into consideration in project planning/implementation and system service.

2.5.6 Fixing Security Vulnerabilities

BDEW 2.5.6	The contractor shall have a well-defined vulnerability management process to address security vulnerabilities. The process allows all involved and external parties to report actual or potential vulnerabilities. Furthermore the contractor shall obtain up-to-date information about security problems and vulnerabilities which might affect the system or its components. The vulnerability management process shall define how a potential vulnerability is verified, classified, fixed and how recommend measurements are reported to all system owners. Furthermore the process shall define timelines for each step in the vulnerability management process. The contractor shall early inform the customer about known security vulnerabilities, even if there is no patch available. The customer shall treat this information confidentially.

SICAM RTUs and SICAM TOOLBOX II, Siemens AG has a documented process to address security vulnerabilities.

This process allows all involved parties, but also external parties, to report actual or potential security vulnerabilities for SICAM RTUs and SICAM TOOLBOX II.

For SICAM RTUs and SICAM TOOLBOX II, up-to-date information on security problems is available, even if a patch for the elimination of the problem has not become available yet.

Note

Information for project planning/implementation and system service:

SICAM TOOLBOX II builds on Microsoft Windows as operating system.
The consideration of security vulnerabilities of SICAM TOOLBOX II does not cover the operating system nor standard applications of the computer on which SICAM TOOLBOX II is installed as application.

2.5.7 Source Code Escrow

BDEW 2.5.7	*If applicable, a source code escrow agreement should be considered, to ensure security updates in case of failure of the contractor. The agreement should cover the system source code and the according source code documentation.*

Note

Siemens precludes a source code escrow. Generally, a deposited source code will not undergo maintenance and is, if really needed in the event of insolvency, rarely useable.

2.6 Backup, Recovery and Disaster Recovery

2.6.1 Backup: Concept, Method, Documentation, Test

BDEW 2.6.1	*There are documented backup and recovery procedures which cover single applications and the entire system, respectively, together with the according configuration data. Configuration data of distributed systems can be saved in a central repository. The backup and recovery processes shall be tested by the client regularly. Documentation and tests shall be adjusted after relevant system updates and the procedures shall be re-tested. The backup process should provide a verify operation and shall take into account the protection requirements of the backup data (e. g.. by encrypting sensitive data).*

SICAM RTUs and SICAM TOOLBOX II, there are data backup and recovery procedures of the various applications and the entire system, respectively, and of the respective configurations. They are documented in the administrator manual for SICAM RTUs and SICAM TOOLBOX II.

The configuration parameters of decentral SICAM RTUs components are stored centrally in SICAM TOOLBOX II.

Note

Information for project planning/implementation and system operation:

Within the scope of system development, concepts and procedures for backup and restore of the entire system must be created such as: the automation of the backup process.

Within the scope of project planning/implementation, it must be defined who has what responsibilities in system operation and where the transitions between responsibilities are (e.g.: site acceptance test, end of trial operation, end of warranty, ...).

Within the scope of system operation, the procedures for backup and restore must be subjected to cyclic testing. Furthermore, the status of the generation of backups must be monitored on a continuous basis.

2.6.2 Disaster Recovery

BDEW 2.6.2	*The contractor shall provide documented operational concepts and tested disaster recovery concepts and procedures for defined emergency and crisis scenarios. The recovery concepts shall include a specification of the recovery time objectives. The documentation and procedures are adjusted after relevant system updates and the procedures are re-tested during system release acceptance procedures.*

Note

Information for project planning/implementation and system operation:

This requirement is of no relevance to the products and must be taken into consideration during project planning/implementation and system service.

Literature

White Paper - Requirements for Secure Control and Telecommunication Systems	Version 1.0
Oesterreichs Energie and DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE Common instructions for the application of the BDEW White Paper	Working version 2.01

Glossary

A

AAA Server

An AAA Server (authentication, authorization and accounting) is a system that manages fundamental system access functions, i.e., authentication, authorization and use, as well as the related accounting.

Authentication

Procedure used to verify the identity of a person.

B

BDEW

***B**undesverband **d**er **E**nergie- und **W**asserwirtschaft (*German Federal Association of Energy and Water Management*)*

BDEW Whitepaper

"BDEW White Paper – Requirements for Secure Control and Telecommunication Systems",

This document defines fundamental security measures and requirements for IT-based control, automation and telecommunication systems, taking the general technical and operational conditions into consideration.

C

CIP

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

CRC

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

D

DoS

Denial **o**f **S**ervice

In digital data processing, this is the term use to denote the consequence of the overloading of infrastructure systems. This can be caused by inadvertent overloading of or by a deliberate attack on a host (server), a computer, or other components in a data network.

M

Malware

or malicious code = malicious software

N

NERC

North American **E**lectric **R**eliability **C**orporation

NIP

Network **I**nterface **P**rocessor

Used to couple SICAM RTU systems to ethernet LAN according to IEEE 802.3

P

Patch

A patch (also called "bug fix") is a small program that repairs bugs (flaws) in generally large application programs.

S

SSL

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

T

TLS

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

TLS, more widely known under its old name Secure Sockets Layer (SSL), is a hybrid encryption protocol for the secure transmission of data in the Internet. Since version 3.0, the SSL protocol is being developed further and standardized under its new name TLS. Thus, version 1.0 of TLS corresponds to version 3.1 of SSL.