SIEMENS

SICAM AK 3
SICAM A8000

Declaration of Security Conformance

Preface, Table of Contents

Introduction 1

BDEW Security Requirements 2

Table of Compliance (TOC) A

List of Reference Documents, Glossary

Date of Issue:
07.2017

Unrestricted
Siemens AG
Energy Automation
Humboldtstraße 59
90459 Nürnberg
Deutschland

Order No.: DC0-161-1.03

Preface

Contents of the Manual

This Declaration of Conformance describes the conformance of the following products

- SICAM AK 3 / SICAM A8000 hardware and firmware, having a delivery release in October 2011 or later (for details see *Scope of Validity*)
- SICAM TOOLBOX II V6.0 or higher.

with the

- *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE Std 1686-2013*
- *BDEW White Paper - Requirements for Secure Control and Telecommunication Systems V1.1* dated 03/2015

This document provides a Table_of_Compliance.

Scope of Validity

This document is valid for SICAM AK 3 and the products of the SICAM A8000 product line (= SICAM RTUs) 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 3
- SICAM A8000: CP-8000 (formerly known as SICAM CMIC), CP-8021/22 (=CP-802x), CP-8050
- SICAM TOOLBOX II and/or SICAM WEB (online tool)

SICAM AK 3 and SICAM A8000 series can be accessed from engineering tools (SICAM TOOLBOX II and/or SICAM WEB for system diagnostics and setting of system parameters):

IED (acting as a server)	Engineering tool (acting as a client)
SICAM AK 3	SICAM TOOLBOXII
SICAM A8000	SICAM WEB or SICAM TOOLBOXII

It is impossible to evaluate the IED (SICAM AK 3 and SICAM A8000 series) on its own, since IED and engineering tools must be considered as related to each other. So, this Conformance Statement refers not only to the IED itself, but also to its engineering tools.

This document only describes product characteristics of SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II. It does not describe any system characteristics that result from system-specific networking and parameterizing of the products into an overall system.

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

- Product development
- Product service

The following fields are not covered in this document:

- System integration (system, consisting of individual SICAM AK 3 / SICAM A8000 components and other components such as network components, protective devices, etc.)
- 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*.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

This document is therefore available in English only.

NOTE

A note provides important information on the product, its handling or the part of the documentation in question to which special attention must be paid.

.

Table of Contents

1 Introduction 7

1.1 General Information 7
1.2 Objectives 7
1.3 Instructions for Use 7

2 BDEW Security Requirements 11

2.1 General Requirements and Housekeeping 12
2.1.1 General 12
2.1.1.1 Secure System Architecture 12
2.1.1.2 Contact Person 13
2.1.1.3 Patching and Patch Management 13
2.1.1.4 Provision of Security Patches for all System Components 14
2.1.1.5 Third Party Support 16
2.1.1.6 Encryption of Sensitive Data during Storage and Transmission 16
2.1.1.7 Cryptographic Standards 17
2.1.1.8 Internal and External Software and Security Tests and Related Documentation 19
2.1.1.9 Secure Standard Configuration, Installation and Start-Up 19
2.1.1.10 Integrity Checks 21
2.1.2 Documentation 21
2.1.2.1 Design Documentation, Specification of Security Relevant System Components and Implementation Characteristics 21
2.1.2.2 Administrator and User Documentation 22
2.1.2.3 Documentation of Security Parameters and Security Log Events or Warnings 22
2.1.2.4 Documentation of Requirements and Assumptions Required for Secure System Operation 22
2.2 Base System 23
2.2.1 System Hardening 23
2.2.2 Anti Virus Software 23
2.2.3 Autonomous User Authentication 24
2.3 Networks /Communication 25
2.3.1 Secure Network Design and Communication Standards 25
2.3.1.1 Deployed Communication Technologies and Network Protocols 25
2.3.1.2 Secure Network Design 30
2.3.1.3 Documentation of Network Design and Configuration 30
2.3.2 Secure Maintenance Processes and Remote Access 31
2.3.2.1 Secure Remote Access 31
2.3.2.2 Maintenance Processes 31
2.3.3 Wireless Technologies: Assessment and Security Requirements 32
2.4 Application 33

2.4.1 User Account Management 33
2.4.1.1 Role-Based Access Model 33
2.4.1.2 User Authentication and Logon Process 38
2.4.2 Authorisation of Activities on User and System Level 39
2.4.3 Application Protocols 43
2.4.4 Web Applications 43
2.4.5 Integrity Checks of Relevant Data 44
2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts 45
2.4.7 Self-Test and System Behaviour 51
2.5 Development, Test and Rollout 52
2.5.1 Secure Development Standards, Quality Management and Release Processes 52
2.5.2 Secure Data Storage and Transmission 54
2.5.3 Secure Development, Test and Staging Systems, Integrity Checks 54
2.5.4 Secure Update and Maintenance Processes 55
2.5.5 Configuration and Change Management, Rollback 56
2.5.6 Fixing Security Vulnerabilities 56
2.5.7 Source Code Escrow 57
2.6 Backup, Recovery and Disaster Recovery 58
2.6.1 Backup: Concept, Method, Documentation and Test 58
2.6.2 Disaster Recovery 58

A Table of Compliance (TOC) 59

A.1 Table of Compliance (TOC)as per Standard IEEE 1686:2013 60

1 Introduction

Contents

1.1 General Information 7
1.2 Objectives 7
1.3 Instructions for Use 7

1.1 General Information

This document describes:

- the conformance of SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II and/or/ SICAM WEB with the security requirements specified in the *BDEW White Paper – "Requirements for Secure Control and Telecommunication Systems"*
- the degree of compliance to *IEEE 1686:2013 - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities*

1.2 Objectives

- To protect control systems including subsystems appropriately against security threats during daily operation, to minimize the consequences of threats to operations, to maintain business operations even in the event of security related incidents and to restore a defined minimum of service and service quality as quickly as possible.
- To continuously adapt these systems to changing security threats 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 specified in the BDEW White Paper. To facilitate the correlation between the requirements set forth in the BDEW White Paper and their implementation in SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II / SICAM WEB, chapter numbers and names from the BDEW White Paper have been applied to this document.

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 table below provides an overview of the areas (product/system development, project planning/implementation, product/system service, control center operation/system operation) relevant for the security requirements set forth by *Oesterreichs Energie and DKE German Commission for Electrical, Electronic & Information Technologies in accordance with 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	✓	✓	-	-
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 Network 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	Authorization of Activities on the User and System Levels	-	-	-	✓

No.	BDEW Security Requirement	Product / System Development	Project Planning / Implementation	Product / System Service	Control Center Operation / System Operation
2.4.3	Application Protocols	✓	✓	✓	✓
2.4.4	Web Applications	✓	-	✓	✓
2.4.5	Integrity Checks of Relevant Data	✓	-	✓	✓
2.4.6	Logging, Audit Trails, Time Stamps, Alarm Concepts	✓	-	✓	✓
2.4.7	Self-Test and System Behaviour	✓	-	✓	✓
2.5	Development, Test and Rollout				
2.5.1	Secure Development Standards, Quality Management and Release Processes	✓	-	✓	✓
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 12
2.1.1 General 12
2.1.2 Documentation 21
2.2 Base System 23
2.2.1 System Hardening 23
2.2.2 Anti Virus Software 23
2.2.3 Autonomous User Authentication 24
2.3 Networks /Communication 25
2.3.1 Secure Network Design and Communication Standards 25
2.3.2 Secure Maintenance Processes and Remote Access 31
2.3.3 Wireless Technologies: Assessment and Security Requirements 32
2.4 Application 33
2.4.1 User Account Management 33
2.4.2 Authorisation of Activities on User and System Level 39
2.4.3 Application Protocols 43
2.4.4 Web Applications 43
2.4.5 Integrity Checks of Relevant Data 44
2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts 45
2.4.7 Self-Test and System Behaviour 51
2.5 Development, Test and Rollout 52
2.5.1 Secure Development Standards, Quality Management and Release Processes 52
2.5.2 Secure Data Storage and Transmission 54
2.5.3 Secure Development, Test and Staging Systems, Integrity Checks 54
2.5.4 Secure Update and Maintenance Processes 55
2.5.5 Configuration and Change Management, Rollback 56
2.5.6 Fixing Security Vulnerabilities 56
2.5.7 Source Code Escrow 57
2.6 Backup, Recovery and Disaster Recovery 58
2.6.1 Backup: Concept, Method, Documentation and Test 58
2.6.2 Disaster Recovery 58

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.* ***Defense-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 AK 3 / SICAM A8000 and SICAM TOOLBOX II and/or/ SICAM WEB 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 AK 3 / SICAM A8000 include the following information:

- Typical system configurations
- Secure basic 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
- Explanation of security specific log and audit messages; possible causes; suitable countermeasures

This information can be used as a basis for the secure design and operation of a 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:

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

An IT security specialist has been appointed by Siemens within the framework of the development process.

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 also installs the patches and updates. Installation and uninstallation of patches and updates shall be authorized by the system owner and must not be performed automatically.*

SICAM AK 3 / SICAM A8000; SICAM TOOLBOX II

For SICAM AK 3 / SICAM A8000 any firmware can be reloaded and updated individually, which ensures the patchability of the system.

Please note that digitally signed firmware can only be loaded incrementally when using major versions (former signed revisions than the latest loaded cannot be used any more).

During a firmware update process the device concerned, at least, is not operational. If an interruption of normal operations is unacceptable, the use of redundant systems can ensure uninterrupted operation.

For SICAM AK 3 / SICAM A8000 product development Siemens has a patch management process in place according to which all firmware releases as well as the enhancements and bug fixes included are documented in a traceable manner.

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

SICAM TOOLBOX II

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

For SICAM TOOLBOX II product development Siemens has a patch management process in place according to which all firmware releases as well as the enhancements and bug fixes included are documented in a traceable manner.

By means of the "Live Update" function of SICAM TOOLBOX II, all firmware updates for SICAM AK 3 / SICAM A8000 can be stored in SICAM TOOLBOX II in an automated manner, which substantially simplifies the updating process.

Firmware for SICAM AK 3 / SICAM A8000 is managed centrally by SICAM TOOLBOX II. New firmware is first stored in SICAM TOOLBOX II and then distributed to SICAM AK 3 / SICAM A8000.

NOTE

Information for project planning/implementation, system service:

Appropriate measures such as redundancy, emergency control level, manual operation, etc. must be taken in order to ensure that the impact of firmware updates for individual system components on the availability of the entire system is reduced to an absolute minimum.

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

Download of configuration settings may trigger a restart of the device, which results in stoppage of functions until the restart is completed.

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 life cycle 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 terms, Siemens provides security updates for SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II throughout a product's entire life cycle.

- Updates are made available within an appropriate time frame to be agreed by contract.
- Patches are only provided after thorough testing.
- Updates must be installed by the operating personnel responsible for the administration of these systems.

- The installation of patches must be authorized by the system operator and must not be performed automatically.

SICAM AK 3 / SICAM A8000

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

SICAM TOOLBOX II

Updates of basic components not developed by Siemens are obtained from the corresponding manufacturers, tested and made available within the scope of new releases (maintenance releases, hotfixes). Within the framework of patch management Siemens also provides a list of released security updates for third-party components of this type. These components were tested for compatibility with SICAM TOOLBOX II.

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 is available during the scheduled product life cycle for system components not developed by Siemens and forming part of SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

The end-of-life terms for SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II define all the relevant deadlines such as "last customer shipping" and "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 AK 3 / SICAM A8000

Current SICAM AK 3 / SICAM A8000 support a https-webserver for remote operation with SICAM TOOLBOX II or WEB-parameterization (encrypted communication).

SICAM TOOLBOX II

Communication from SICAM TOOLBOX II to SICAM AK 3 / SICAM A8000 is implemented via https (encrypted and on device level authenticated communication). File retrieval from the device with SICAM TOOLBOX II is also over this secured channel.

Specific cryptographic features (*IEEE Standard)*

a) Webserver functionality provided by the IED shall be Hypertext Transfer Protocol Secure (HTTPS)

b) SFTP not supported
SICAM WEB (for engineering CP-8000, CP-802x, CP-8050): TFTP can be used to load the SICAM WEB Backup-File from the server.

c) virtual terminal communication not supported, SSH not necessary

d) SNMPv3 integrated in M-CPU

e) NTP v3 and SNTP v3 supported (Port 123); some more time synchronization options, e.g., GPS, DCF77, ...

f) support of IPSec VPN tunnel

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 AK 3 / SICAM A8000 and SICAM TOOLBOX II use only recognized encryption methods with key lengths that, according to the current state of the art at the time when they are manufactured, are considered secure (refer also to recommendations for Cryptographic Key Length https://www.keylength.com):

- Random number generation
  - TRNG via hardware-security-module

- Key establishment
  - Preshared keys and certificates programmed at factory for remote operation (of e.g. SICAM TOOLBOX II)

- SNMPv3:
  - HMAC-MD5-96
  - CBC-DES

- IPSec ciphers
  - IPSec encapsulating security payload (ESP)
  - IKE v1, IKE v2

  -Diffie Hellman Group DH Group 1: 768-bit &DH Group 2: 1024-bit Encryption algorithm AES 128, AES 256, AES 192, 3-DES

  - Authentification algorithm SHA1 MD5

- https: TLS encryption is used for:
  - SICAM TOOLBOX II remote operation with X.509 certificates
  - SICAM WEB with X.509 self signed certificates

SICAM TOOLBOX II V6.0 Client Interface:
For remote operation: https with X.509 certificates:
RSA2048/SHA256 (SICAM TOOLBOX II V5.0: RSA1024/SHA1) ;

SICAM AK 3 / SICAM A8000:
Each device has its specific device X.509 server certificate RSA2048/SHA256 stored on hardware-security-module.

Supported Ciphers:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3-DES_EDE_CBC_SHA
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

This device certificate is part of a secure controller, integrated in our hardware (hardware-security-module).
The material/signatures are loaded during production process.

SICAM WEB:

https with X.509 selfsigned certificates in combination with:

SICAM A8000 CP-8000/21/22 generates a selfsigned Certificate RSA1024/SHA256

SICAM A8000 CP-8050 generates a selfsigned Certificate RSA2048/SHA256

Supported Ciphers (session keys):

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3-DES_EDE_CBC_SHA
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

Cryptographic techniques (*IEEE Standard)*

- Digital signatures:
  SICAM TOOLBOX II installer is digitally signed.
  SICAM A8000 firmware is digitally signed.

- Entity authentication

  SICAM TOOLBOX II *(Remote operation):*
  Encrypted, at device level authenticated https communication (TLS), X.509 certificate based

  SICAM A8000 CP-8000/21/22:

  SICAM TOOLBOX II:

  User authentication via Connection Password (HASH, Challenge Reponse); see above.

  SICAM WEB*:*

  Encrypted https communication (TLS), using selfsigned X.509 certificates.

  User authentication (User Name/Password)

SICAM A8000 CP-8050:

SICAM TOOLBOX II:

Role Based User authentication

SICAM WEB*:*

Encrypted https communication (TLS), using selfsigned X.509 certificates.

User authentication (User Name/Password)

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 corresponding 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 AK 3 / SICAM A8000 and SICAM TOOLBOX II / SICAM WEB the individual system components (firmware, hardware, communication, etc.) and the key functions of an integral SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II / SICAM WEB system are subjected to extensive function, security and stress testing by departments independent of the development teams using representative test configurations.

The test results and the relevant 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 live.*

In the original delivery state, the devices must be initialized by the customer. Only after that the devices are ready for operation. By default, only the connection to SICAM TOOLBOX II is activated in the device. All other Ethernet services and ports are not activated in the device by default and can be activated with SICAM TOOLBOX II. Because of the secure default configuration there are no open interfaces for potential attackers and only services that are really used are activated in the network.

For the engineering of CP-8000, CP-802x via SICAM WEB https port 443 is open.

For the engineering of CP-8050, https port 443 is open.

Communications port access (*IEEE Standard)*

SICAM AK 3: each LAN interface and each service per interface can be (de-) activated.
SICAM A8000 CP-8050: each LAN interface and each service per interface can be (de-) activated.
The network configuration parameters for all SICAM AK 3 / SICAM A8000 components are managed centrally by means of SICAM TOOLBOX II.

Administration and monitoring of SICAM AK 3 / SICAM A8000 network components are carried out by means of SICAM TOOLBOX II.

The network components of SICAM AK 3 / SICAM A8000 are hardened, unnecessary services and protocols are deactivated, management interfaces are available to SICAM TOOLBOX II only.

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

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.

SICAM TOOLBOX II includes neither the hardware nor the operating system nor 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.

CP-8050: Secure Factory Reset

The feature “Secure Factory Reset” allows you to restore all settings of the device when it was first purchased from the manufacturer.

Factory settings: settings of the the CP-8050 when it was first purchased from the manufacturer.

Default settings: settings of the CP-8050 after initial commissioning and configuring via SICAM TOOLBOX II / SICAM WEB.

A factory reset will delete any data, including security data:

Deletion of

- all applications (firmwares), except CPCI85, SWEB00
- all configurations (parameter, user management, users, passwords, keys, certificates)
- all logs und diagnosis information (history, security log)
- all SD-Card data

A secure factory reset is even possible in case of a deactivated SD-card or in case of misconfigured interfaces.

To make the device CP-8050 even more secure it is possible to deactivate DHCP (no one click to connect).

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 AK 3 / SICAM A8000

The firmware versions and parameter blocks of SICAM AK 3 / SICAM A8000 are protected by check sums and continuously subjected to integrity tests during operation.

SICAM TOOLBOX II

SICAM TOOLBOX II can be used to compare firmware versions and parameter states in the target system and in the SICAM TOOLBOX II database in order to detect any possible changes. Within the device, the files are protected against each other by means of different check-sum tests.

SICAM TOOLBOX II is installed using the Windows Installer. Therefore, the security mechanisms of Windows Installer 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 especially characterise 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. cryptographic standards used).*

For SICAM AK 3 / SICAM A8000 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 AK 3 / SICAM A8000.

NOTE

Information for project planning/implementation

These typical system configurations serve as examples and do not cover all possible system configurations.

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

2.1.2.2 Administrator and User Documentation

BDEW 2.1.2.2	*The contractor shall provide separate user and administrator documentation. Both sets of documentation should include a list of security functions and parameters as well as instructions and responsibilities for the 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 AK 3 / SICAM A8000 and SICAM TOOLBOX II, only an administrator documentation (administrator: makes changes to the parameterization / configuration of the system) is available for SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

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 users to 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 SICAM AK 3 / SICAM A8000 documentation mainly includes functional security descriptions, such as security relevant system settings and parameters and their default values, security specific log and audit messages and their possible causes, and suitable countermeasures.

2.1.2.4 Documentation of Requirements and Assumptions Required 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*

The SICAM AK 3 / SICAM A8000 documentation mainly includes functional security descriptions. In addition, it contains typical system configurations under cybersecurity aspects.

2.2 Base System

2.2.1 System Hardening

BDEW 2.2.1	*All the 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 not technically 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 not technically 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 AK 3 / SICAM A8000 and SICAM TOOLBOX II are permanently hardened according to recognized best practice guides. This results in a secure base configuration of SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

The secure base configuration and the measures for system hardening are described in the administrator manuals of SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

Maintenance releases, hotfixes, and firmware that include security patches will be provided in a timely manner for SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

NOTE

Information for project planning/implementation and system service:

SICAM TOOLBOX II includes neither hardware components nor the operating system nor other standard software such as Microsoft Office or Adobe Acrobat Reader.
Basic security and 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 anti virus software on each system component, the contractor may implement a comprehensive anti virus and malware protection concept which provides equivalent protection. The patterns of the anti virus and malware protection software shall be updated automatically and in a timely manner 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 AK 3 / SICAM A8000 components are embedded systems from in-house development for which no virus is known. 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 framework of project planning/implementation. Recommendations are available with regard to compatibility-tested anti virus programs for SICAM TOOLBOX II.

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 A8000 CP-8050 supports Role-Based-Access-Control.

SICAM AK 3 / SICAM A8000 devices have no user management because all the parameters are defined 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 AK 3 / SICAM A8000 with SICAM TOOLBOX II via remote operation, there is an additional user authentication provided:

- SICAM AK 3 / SICAM A8000 CP-8000/21/22 supports "Connection Password"
- SICAM A8000 CP-8050 supports Role-Based-Access-Control

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 regulations.* *b) The system and its network components shall be easily integrable into the network concept of the entire company. Relevant network configuration parameters such as IP addresses can be managed centrally. Secure protocols shall be used for administration and monitoring (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) are to 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 AK 3 / SICAM A8000

a) Standard protocols such as IEC-61850, IEC-60870-5-101, and IEC 60870-5-104 are used for the transmission of process data.
Since these protocols currently do not provide for any authentication and encryption, these requirements can be covered by means of VPN technology, where necessary. All protocols: tunneled in IPSec. Integrity checking is performed based on CRC or check sums.
IEC62351-3 is supported for IEC-60870-5-104 for SICAM A8000 CP-8000/21/22.

b) Integration into the network design is possible and related recommendations and notes are provided in the SICAM AK 3 / SICAM A8000 documentation.
SNMPv3 is integrated in the firmware of the basic system element (M-CPU) and controls the communication between the monitored IEDs (SNMP-Agents) and the monitoring station (SNMP-Manager, e.g.: SICAM TOOLBOX II).
SICAM AK 3 / SICAM A8000 are equipped with communication ports which can be configured to connect to a SCADA system (this is a matter of network configuration and design; system design, product/system service, and control center/system operations.)

c) The network configuration parameters for all SICAM AK 3 / SICAM A8000 components are managed centrally by means of SICAM TOOLBOX II.
Administration and monitoring of SICAM AK 3 / SICAM A8000 network components are carried out by means of SICAM TOOLBOX II
The network components of SICAM AK 3 / SICAM A8000 are hardened, unnecessary services and protocols are deactivated, management interfaces are available to SICAM TOOLBOX II only.
Inventory and patch management of SICAM AK 3 / SICAM A8000 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.
IEC62351-3 is supported for IEC-60870-5-104 for SICAM A8000 CP-8000/21/22 and SICAM AK3.

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

NOTE

Information for project planning/implementation:

Must be taken into consideration in system design.

SICAM TOOLBOX II

a) https – secure channel, TBII Server/Client

The remote administration of SICAM TOOLBOX II is carried out in an secure manner by means of remote operation using a encrypted and at device level authenticated https communication (X.509 certificates provided by Siemens at production)

During communication establishment, the device checks if the configuration software is the official software from Siemens, and likewise SICAM TOOLBOX II checks if the device is an original product, manufactured by Siemens.
In addition, a connecton password can be entered on the device to ensure a user authentication for each device.

b) SNMPv3 controls the communication between the monitored SICAM AK 3 / SICAM A8000 (SNMP-Agents) and the monitoring station (SNMP-Manager, e.g.: SICAM TOOLBOX II). Unused services and ports can be disabled (via the corresponding parameter settings in SICAM TOOLBOX II)

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) Network components are not included in the scope of delivery of SICAM TOOLBOX II. 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 only uses TCP (https) for the transmission of parameter settings.

f) NOTE

NOTE

Information for project planning/implementation:

Must be taken into consideration in system design.

Overview of supervisory monitoring and control (*IEEE Standard)*

SICAM AK 3 / SICAM A8000:

SNMP: this protocol is integrated in the firmware of the basic system element (M-CPU) and controls the communication between the monitored IEDs (SNMP-Agents) and the monitoring station (SNMP-Manager, e.g.: SICAM TOOLBOX II).

SICAM AK 3 / SICAM A8000 are equipped with communication ports which can be configured to connect to a SCADA system (this is a matter of network configuration and design; system design, product/system service, and control center/system operations.).

SICAM TOOLBOX II:

The engineering PC with installed SICAM TOOLBOX II is connected with the IED

- via serial interface directly (local parameterization cable)

or for remote connection via

- LAN/WAN communication (Ethernet, TCP/IP)
- SICAM TOOLBOX II is directly connected to the IED via remote connection using http/https
  (HTTP Port 80 bzw. HTTPS Port 443)

For the remote maintenance of SICAM AK 3 / SICAM A8000 components using "remote operation" a transparent connection is established over TCP/IP, HTTP/HTTPS between the SICAM TOOLBOX II and the SICAM AK 3 / SICAM A8000 component via the protocol element.

SICAM TOOLBOX II establishes a secure point-to-point connection to the IED.

For “remote operation" with SICAM TOOLBOX II (acting as a client) a proprietary Client-Server protocol is used for remote maintenance and remote diagnostics of SICAM AK 3 / SICAM A8000 components (acting as a server).

If several SICAM TOOLBOX II applications attempt to setup a connection at the same time, the first SICAM TOOLBOX II wins, all others are rejected.

It is not possible to perform diagnostic functions and configuration activities at the same time.

If an error is detected during the remote maintenance of SICAM AK 3 / SICAM A8000 components using "remote operation", then the TCP/IP connection is terminated.

There are various possibilities of network installations of SICAM AK 3 / SICAM A8000 systems. Remote stations can be widely distributed in the country, but are controlled from one central control center.

The administrator documentation for SICAM AK 3 / SICAM A8000 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.

Ad: *Information to be monitored and transmitted shall fall into two groups: events and alarms:*

g) Monitored information are not decidedly called alarms and events: entries of the security logbook in SICAM AK 3 / SICAM A8000 are classified by several facility types, severities and **three event types**.

h) Event types “Events” will be sent for authorized/unauthorized activities but not defined as AuditTrail Event/-Alarm.

i) Event types “AuditTrailEvents” are defined as authorized activities which can be expected to occur in the routine use and maintenance of the IED.

j) Event types “AuditTrailAlarms” are defined as activities which may indicate unauthorized activity:

- spontaneous transmission
- alarms with local diagnosis (diagnosis information can be converted/transmitted to process information)

Events (*IEEE Standard)*

SICAM AK 3 / SICAM A8000 offer a security logbook, which can transfer the logged events by means of a syslog client to a syslog server. For the logbook of SICAM TOOLBOX II, refer to 1.2.1.

Event types “AuditTrailEvents” are defined as authorized activities which can be expected to occur in the routine use and maintenance of the IED.

Event points shall have momentary change detect capability so that the occurrence of an event will be reported on the next scan of the IED by the supervisory system. The IED shall report each occurrence as an individual event:

Depending on used protocols logged events will be transmitted either spontaneously or via scan.

Alarms (*IEEE Standard)*

Monitored information are not decidedly called alarms and events: entries of the security logbook in SICAM AK 3 / SICAM A8000 are classified by several facility types, severities and three event types.

Event types “Events” will be sent for authorized/unauthorized activities but not defined as AuditTrail Event/-Alarm.

Event types “AuditTrailEvents” are defined as authorized activities which can be expected to occur in the routine use and maintenance of the IED.

Event types “AuditTrailAlarms” are defined as activities which may indicate unauthorized activity:

- spontaneous transmission

- alarms with local diagnosis (diagnosis information can be converted/transmitted to process information)

Logging entries of specific activities are not called “alarms”, but many security related activities are logged as events of the type **AuditTrailAlarms**:

a) comply

b) comply

c) comply

d) Exception, feature not supported

e) Exception, feature not supported

f) comply

g) comply

Alarm point change detect (*IEEE Standard)*

Depending on used protocols logged events will be transmitted either spontaneously or via scan

Refer to Events

Event and alarm grouping (*IEEE Standard)*

User cannot group events and alarms, but categories of events and alarms are configurable and will be provided as user data, refer to Overview of supervisory monitoring and control

Supervisory permissive control (*IEEE Standard)*

No diagnostic port has the ability to be enabled and disabled remotely.

But SICAM AK3 / SICAM A8000 can control the power of a e.g. separate SWITCH to enable/disable this LAN Interface.

IED functionality compromise (*IEEE Standard)*

Dedicated diagnostic ports are not available. Primary IED functions cannot be compromised by ports or by a communication protocol. Alerts are not written.

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 only be deployed 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 by the customer through a defined process.*

NOTE

Information for project planning/implementation:

This requirement is not relevant to the products and must be taken into consideration during system design and project planning/implementation. For more detailed information refer to chapter 2 of the SICAM AK 3 / SICAM A8000 Security documentation (Typical Plant Configurations).

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 the normal and maximal expected data rate for all network connections.*

NOTE

Information for system development and project planning/implementation:

This requirement is not relevant 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	*a) It shall be possible to perform administration, maintenance and configuration of all network components via out-of-band channels such as local access, serial interfaces, network or direct control of input devices (KVM).* *b) Remote access shall be performed through dedicated centrally administered terminal servers which ensure the 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 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 operation:

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

Encrypting serial communications (*IEEE Standard)*

SICAM TOOLBOX II

For remote access, a serial communication is provided, but it is NOT encrypted.

2.3.2.2 Maintenance Processes

BDEW 2.3.2.2	*a) Interactive remote access users shall use personal accounts. For non-interactive, automated processes restricted accounts shall be used for which interactive access is disabled.* *b) 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 period of time.* *c) Maintenance shall only be performed by defined and trained contractor personnel, 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.* *d) A defined maintenance process (compare above) shall ensure that maintenance personnel can only access systems, services and data they need for maintenance tasks.* *e) The maintenance personnel shall comply with the requirements of SÜFV if it is to be deployed at supra-regional utilities.* *f) Local maintenance by service personnel poses a significant security threat. The 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 being attached. The contractor shall provide evidence that an adequate internal security policy has been implemented.*

NOTE

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

This requirement is not relevant to the products and must be taken into consideration during product / system service and control center / system operation.

2.3.3 Wireless Technologies: Assessment and Security Requirements

BDEW 2.3.3	Wireless technology such as 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.

Since **SICAM AK 3 / SICAM A8000** devices are not equipped with wireless technologies, this requirement is not relevant for SICAM AK 3 / SICAM A8000.

NOTE

Information for project planning/implementation:

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

Since **SICAM TOOLBOX II** is not equipped with wireless technologies, this requirement is not relevant for SICAM TOOLBOX II.

NOTE

Information for project planning/implementation:

If wireless technologies are used on a SICAM TOOLBOX II PC appropriate measures must be taken with regard to the device hardware and/or operating system.

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 use 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 corresponding 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**: A 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 data display role permissions shall be sufficient. Individual user accounts can be disabled without removing them from the system.*

SICAM AK 3 / SICAM CP-8000, CP-802x

SICAM AK 3 / CP-8000, CP-802x does not support user or role management.

SICAM CP-8050 supports RBAC according to IEC 62351-8, BDEW-Whitepaper and IEEE 1686.

SICAM WEB (for engineering CP-8000, CP-802x) provides the roles "administrator" and "guest" (corresponds to "Administrator – read/write" and "Data Display – read only").

SICAM WEB (for engineering CP-8050) reflects eight roles implemented in CP-8050, see table below.

SICAM TOOLBOX II

SICAM TOOLBOX II supports RBAC: Access and authorizations can be defined freely via the concept of a flexible user-role-assignment. All conceivable roles can be defined for particular cases of application and projects. Currently there are 40 authorisation areas defined.

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

SICAM TOOLBOX II (for engineering CP-8050) reflects eight roles implemented in CP-8050, see table below.

A role comprises certain authorizations to execute certain functions. One or more roles and the respective associated rights can be assigned to any user.
The ADMIN role (SICAM TOOLBOX II, SICAM WEB) has all rights.

Predefined Roles in SICAM A8000 Series CP-8050:

- **VIEWER:** can view what objects are present within a Logical-Device by presenting the type ID of those objects.
- **OPERATOR:** can view what objects and values are present within a Logical-Device by presenting the type ID of those objects
  as well as perform control actions.
- **ENGINEER:** can view what objects and values are present within a Logical-Device by presenting the type ID of those objects.
  Moreover, an engineer has full access to DateSets and Files and can configure the server locally or remotely.
- **INSTALLER:** can view what objects and values are present within a Logical-Device by presenting the type ID of those objects. Moreover, an installer can write files and can configure the server locally or remotely.
- **SECADM:** can change subject-to-role assignments (outside the device) and role-to-right assignment (inside the device) and validity periods; change security setting such as certificates for subject authentication and access token verification.
- **SECAUD:** Security auditor can view audit logs.
- **RBACM_MGMT**: can change role-to-right assignment.
- **ADMIN** all rights (SIEMENS specific)

RBAC in SICAM TOOLBOX II

Following functions (more precisely, granted rights to execute certain functions) of SICAM TOOLBOX II are assigned to roles predefined in the device SICAM A8000 Series CP-8050:

Functions \ Defined Roles	VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD	RBAC_MGMT	ADMIN *)
PSR II: ST Emulation	X	X	X	X	X	X	X	X
PSR II: online function: read serial number	X	X	X	X	X	X	X	X
PSR II: online function: memory check	X	X	X	X	X	X	X	X
PSR II online function: stop system element		X	X	X				X
PSR II online function: set time		X	X	X				X
Firmwareloader				X				X
Diagnosis	X	X	X	X	X	X	X	X
Parameterloader: Security Parameter					X			X
Parameterloader: general Parameter			X	X				X
Online Test (CAEx plus)		X	X	X				X
OPM II: display decentral archiving	X	X	X	X	X	X	X	X
Revision interogation	X	X	X	X	X	X	X	X
Message simulation		X	X	X				X
Data flow test: during startup		X	X	X				X
Data flow test: general	X	X	X	X	X	X	X	X

*) "ADMIN" is an additional empirical role in SICAM TOOLBOX II

RBAC in SICAM WEB

Following functions (more precisely, granted rights to execute certain functions) of SICAM WEB are assigned to roles predefined in the device SICAM A8000 Series CP-8050:

Functions \ Defined Roles	VIEWER	OPERATOR	ENGINEER	INSTALLER	SECADM	SECAUD	RBAC_MGMT	ADMIN *)
View Running Firmware	X	X	X	X	X	X	X	X
View Installed Firmware	X	X	X	X	X	X	X	X
Logoff	X	X	X	X	X	X	X	X
Update Firmware				X				X
Restart Device		X	X	X	X			X
Change own Password	X	X	X	X	X	X	X	X
View active Sessions					X		X	X
Local user Management					X		X	X
Feature „one click to support“		X	X	X	X	X	X	X
Set Time		X	X	X				X
View Security Logbook					X	X		X
View Diagnosis Logbook	X	X	X	X	X	X	X	X
View Diagnosis Status	X	X	X	X	X	X	X	X
Device Information	X	X	X	X	X	X	X	X

*) "ADMIN" is an additional empirical role in SICAM WEB

Authorization using role-based access control (RBAC) (*IEEE Standard)*

SICAM AK 3 / SICAM A8000:

The IED itself (SICAM AK 3 / SICAM A8000) does **not** support this feature.

SICAM TOOLBOX II

Access and authorizations can be defined freely via the concept of a flexible user-role-assignment.

A SICAM TOOLBOX II administrator can add roles to the default roles of SICAM TOOLBOX II (Administrator, Professional, Standard). All conceivable roles can be defined for particular cases of application and projects. In addition, SICAM TOOLBOX II administrator can change ID/ passwords and user assignment levels.
Currently there are 40 authorisation areas defined.

SICAM WEB:

SICAM WEB (for engineering CP-8000, CP-802x) provides the roles "administrator" and "guest" (corresponds to "Administrator – read/write" and "Data Display – read only").

View configuration data (*IEEE Standard)*
Change configuration data (*IEEE Standard)*
a) Full access: In full access mode, all functions, including ID/password changes and user assignment levels can be made

SICAM WEB

CP-8000, CP-802x provide the role "guest" (corresponds to "Data Display – read only").

SICAM TOOLBOX II

Access and authorizations can be defined freely via the concept of a flexible user-role-assignment.

The default role “Standard” of SICAM TOOLBOX II corresponds to “unskilled user”.

Any conceivable role can be defined for particular cases of application and projects. Currently there are 40 authorisation areas defined.

In addition, SICAM TOOLBOX II administrator can change ID/ passwords and user assignment levels

Distributed working on one IED by means of the Data Distribution Center (DDC) of SICAM TOOLBOX II :

The system technique of an IED can be exported to the DDC. This backup is in state “read-only). This state has no impact to a live IED.

The process technique (ranges, parameterization) can be exported to the DDC. The entire process-engineering plant then has the Status “*Copy”* . This state has no impact to a live IED.

2.4.1.2 User Authentication and Logon Process

BDEW 2.4.1.2	• *Users shall be identified and authenticated with a personal account.Group accounts shall only be used in precisely defined exceptional cases.* • *Before allowing any actions the system shall require each user to be successfully authenticated.* • *The system shall enforce passwords with configurable strength and expiration periods. The password strength and expiration period shall be configurable by the customer.* • *If technically feasible 2-factor authentication shall be used, for example SmartCards or security tokens.* • *Data used for user identification and authentication shall not be provided solely from sources external to the process network. Integration with a central, process net internal directory service should be considered.* • *Successful and failed log on attempts shall be logged centrally.* If applicable, the following items shall be implemented after the paramount consideration of safe system operation and availability issues. The system should implement mechanisms which allow for a secure and reproducible switching of user sessions 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 AK 3 / SICAM A8000

In SICAM AK 3 / SICAM A8000, 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 AK 3 / SICAM A8000 CP-8000/21/22 for user-authentication. This password is stored in the SICAM AK 3 / SICAM A8000 CP-8000/21/22 and not in the SICAM TOOLBOX II.

SICAM A8000 CP-8050 performs authentication of every user using the role based access model. The usage of “Connection Password” is not supported.
This role-based access information is stored in the CP-8050 and not in the SICAM TOOLBOX II.

When using the WEB parameterization of SICAM A8000 CP-8000/21/22, user authentication and logon are carried out separately for each device via the group accounts "Administrator" and "Guest".

When using the WEB parameterization of SICAM A8000 CP-8050, user authentication and logon are carried out using the role based access model.

In SICAM AK 3 / SICAM A8000 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 AK 3 / SICAM A8000 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.

SICAM WEB

User authentication is carried out separately for each IED. Passwords used for authentification are stored securely in the IED.

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.

Authentication (*IEEE Standard*):

Unauthorized usage of copied software is not 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.*

SICAM AK 3 / SICAM A8000

CP-8000, CP-802x only display process states. Controlling is not possible.

NOTE

Information for project planning/implementation:

Critical actions, e.g., protected command initiation, can be implemented for SICAM AK 3 / SICAM A8000, e.g., by means of a key switch.
Design and implementation are not relevant to the products and are performed within the framework of system design and/or project planning/implementation.

SICAM TOOLBOX II

After the registration to SICAM TOOLBOX II, the user can exercise the rights, set out in its role.

For connection password (SICAM AK3, SICAM A8000 CP-8000/21/22 and RBAC(SICAM CP-8050) refer to 2.4.1.2.

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.

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 are performed within the framework of system design and/or project planning/implementation.

IED access control overview (*IEEE Standard):*

For connection password (SICAM AK3, SICAM A8000 CP-8000/21/22 and RBAC(SICAM CP-8050) refer to 2.4.1.2.

SICAM TOOLBOXII:

The entire parameterization takes place via SICAM TOOLBOX II. SICAM TOOLBOX II manages the access rights by means of a user/role concept.

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

Once a user has configured a proper ID/password combination, it is not possible to gain access to the device without a proper ID/password combination that has been generated by the user.

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.

SICAM WEB:

When using the WEB parameterization of SICAM A8000, user authentication and logon are carried out separately for each device via the group accounts "Administrator" and "Guest".

Exception:

The IED shall meet or exceed the requirements established in IEEE Std 1686, Standard for Intelligent Electronic Device Cyber Security Capabilities, except as noted below:

The IED shall have an open and documented interface to change user accounts, passwords, and roles, which can be enacted through the use of a third party products (for example, a centralized batch process system).

There is an open WEB-XML interface (used for internal automated testing), but the documentation is today not available, since this interface is not intended to be delivered to end-customers.

Password defeat mechanisms (*IEEE Standard):*

For connection password (SICAM AK3, SICAM A8000 CP-8000/21/22 and RBAC(SICAM CP-8050) refer to 2.4.1.2.

User-created ID/password control cannot be circumvented.

Sensitive data including passwords are transmitted and stored in encrypted form.

SICAM AK 3 / SICAM A8000:

Passwords of SICAM WEB can be parameterized by means of SICAM TOOLBOX II. Passwords are stored on SD-card in HASH as part of the parameters.

In SICAM A8000 preshared keys (for IPSec, SNMP and RADIUS), which are used for authentification, are encrypted via Public Key of the SICAM TOOLBOX II and stored securely on SD-card as part of the parameters.

SICAM TOOLBOX II:

The transmission of passwords between client and server is encrypted.

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

SICAM WEB: Comply

In the cause of WEB-parameterization SICAM A8000 transmit passwords encrypted (https) and not as plain text.

Number of individual users (*IEEE Standard)*:

SICAM AK 3 / SICAM A8000: n/a

SICAM TOOLBOX II:

- parallel access of max. 100 users per server (depending on Server Licences)
- 1000 users per server

SICAM WEB:

SICAM A8000 (CP-8000, CP-802x) provides the roles "administrator" and "guest" (corresponds to "Administrator – read/write" and "Data Display – read only"). One *administrator* and two *guest* can be logged in to the device at the same time.

SICAM A8000 CP-8050: The number of individual users stored in the IED is limited to 10.

Password construction (*IEEE Standard)*:

SICAM TOOLBOX II

SICAM TOOLBOX II provides the possibility to define a domain-user for single-sign-on. According to the security policies of the customer’s network, the password may contain alphanumeric characters , both upper- and lower case letters, as well as special characters.

The connection password has a minimum of 8 characters and must include numbers, upper case, lower case, and special characters.

SICAM WEB:

Password policy in SICAM WEB: at least eight characters (case sensitive); at least one uppercase and one lower case letter, at least one number, at least one non-alphanumeric character (e.g., @, %, &, *)

Authorization levels by password (*IEEE Standard)*

SICAM AK 3 / SICAM A8000:

The IED itself (SICAM AK 3 / SICAM A8000) does **not** support this feature, **but**

SICAM TOOLBOX II:

Access and authorizations can be defined freely via the concept of a flexible user-role-assignment.

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

SICAM WEB:

SICAM WEB/ CP-8000, CP-802x only provide the roles "administrator" and "guest" (corresponds to "Administrator – read/write" and "Data Display – read only"): a) through g) not supported

IED main security functions (*IEEE Standard)*

All items a) – g) are covered by the default roles of SICAM TOOLBOX II:

a) and b) covered by STANDARD user.

c) and d) and e) covered by PROFESSIONAL user

f) and g) covered by ADMINISTATOR user

All conceivable roles can be defined for particular cases of application and projects. Currently there are 40 authorisation areas defined.

Password display (*IEEE Standard)*

SICAM AK 3 / SICAM A8000 series can be accessed from engineering tools (SICAM WEB and/or SICAM TOOLBOX II). This access is protected by passwords stored both in the engineering tools and the IEDs in a secure manner.

On the GUI, passwords are never shown in plain text, only bullets or asterisks are displayed.

Passwords are stored as hashed values, preshared keys are stored encrypted.

Access timeout (*IEEE Standard)*

SICAM AK 3 / SICAM A8000, SICAM TOOLBOXII, SICAM WEB

IEDs support a https-webserver for remote operation with SICAM TOOLBOX II or SICAM WEB-parameterization, but this feature is not supported neither by SICAM AK 3 / SICAM A8000 nor SICAM TOOLBOXII / SICAM WEB.

In case of SICAM WEB the timeout feature is implemented (after 30 sec of inactivity the user will be logged out). This period time is not parameterizable.

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 data transferred and ensure correct authentication and authorisation of the communication partners should be preferred. Furthermore the protocols used should provide time stamps or secure sequence numbers to prevent the re-injection of messages previously sent. If applicable, encryption of the protocol data should be implemented. The previous requirements also apply to non-standard, proprietary or in-house developed protocols.*

Standard protocols such as IEC 61850, IEC-60870-5-101 and IEC 60870-5-104 are used for the transmission of process data. For secure communication IEC 62351-3 is supported.

Some SICAM AK 3 / SICAM A8000 protocol elements can transmit a PING by using the WEB-Browser.

NOTE

Information for project planning/implementation:

Since the used standard protocols etc. currently do not provide for any authentication, authorization and encryption, these requirements must be covered using VPN technology if required.

2.4.4 Web Applications

BDEW 2.4.4	*In addition to common secure application programming practise the following topics shall be considered when web applications are being developed:* • *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.* • The web application components shall be configured with the minimum possible privileges, both on the application and the system level. • All parameters which are passed to the web application from the user or his web browser shall be tested extensively for validity, maximum length, correct type and range. This also applies 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. • Secure session management has especially to be taken into account, for example by using signed or encrypted session IDs and session timeouts. The transmission of session IDs shall be secured by encryption. • 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 to internal users only. • Web applications with a high protection requirement shall be tested by a security audit before going productive.

SICAM AK 3 / SICAM A8000

When using SICAM TOOLBOX II, in SICAM AK 3 / SICAM A8000 all WEB applications (WEB parameterization) are disabled.

Current SICAM AK 3 / SICAM A8000 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 AK 3 / SICAM A8000 should be omitted.

SICAM TOOLBOX II

SICAM TOOLBOX II does not provide 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 AK 3 / SICAM A8000

Security relevant actions such as command initiation are checked in SICAM AK 3 / SICAM A8000 prior to processing (plausibility, correct syntax, value range).

SICAM TOOLBOX II

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

SICAM WEB

For the loading of configurations via the network, a backup of all SICAM A8000 device settings can be stored in a file, e.g.:
SICAM_CMIC_BACKUP_<*customer*>_<*plant*>_<*station*>_<*hash value of file*>.*cmc*.

During download the file is checked upon integrity by means of a cryptologic hash function that is calculated over the file. The result is compared with the hash value in the filename. If the file is valid, it is accepted and all settings in the SICAM A8000 device are adapted.

2.4.6 Logging, Audit Trails, Time Stamps and 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, users and systems involved 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 easy automatic analysis.* *e) The central storage location of the log files shall be configurable.* *f) A mechanism for the automatic transfer of the log files to a 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 audit records stored 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 existing alarm management*

SICAM AK 3 / SICAM A8000

a) SICAM AK 3 / SICAM A8000 provide several time synchronization options, e.g., NTP, GPS, DCF77, …

b) SICAM AK 3 / SICAM A8000 offer 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 AK 3 / SICAM A8000 offer a security logbook, which can transfer the logged events by means of a syslog client to a syslog server and are stored encrpyted locally.

c) The history diagnostic is permanently configured in SICAM AK 3 / SICAM A8000, the security logbook including the syslog server can be activated on demand.

d) The history diagnostic in SICAM AK 3 / SICAM A8000 handles all events the same way.
The security logbook in SICAM AK 3 / SICAM A8000 differentiates between several facility types and severities.

e) The history diagnostic in SICAM AK 3 / SICAM A8000 is stored locally and can be read out and stored from remote locations via SICAM TOOLBOX II.
The security logbook entries in SICAM AK 3 / SICAM A8000 are transmitted by means of the syslog client to a syslog server and are stored encrpyted locally.

f) The history diagnostic in SICAM AK 3 / SICAM A8000 is stored locally and can be read out and stored from remote locations via SICAM TOOLBOX II.
The security logbook entries in SICAM AK 3 / SICAM A8000 are transmitted by means of the syslog client to a syslog server and are stored encrpyted locally..

g) The history diagnostic in SICAM AK 3 / SICAM A8000 is stored locally. Entries cannot be modified or deleted.
The security logbook entries in SICAM AK 3 / SICAM A8000 are transmitted by means of the syslog client to a syslog server which protects these data against manipulation and are stored encrpyted locally.

h) The history diagnostic in SICAM AK 3 / SICAM A8000 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 AK 3 / SICAM A8000 are transmitted by means of the syslog client to a syslog server and are stored encrpyted locally.
The user role “Auditor” can be applied on the syslog server and on the SICAM A8000 CP-8050. For SICAM A8000 CP-8000/21/22 and SICAM A8000 the user role “Auditor” is identically with the user role “Administrator”.

i) The history diagnostic in SICAM AK 3 / SICAM A8000 overwrites older entries in cases of overflow. There is no warning option in case of overflow.
The security logbook entries in SICAM AK 3 / SICAM A8000 are transmitted by means of the syslog client to a syslog server. The transmission takes place without acknowledgement via UDP. The security logbook entries in SICAM AK 3 / SICAM A8000 overwrites older entries in case of overflow.

j) SICAM AK 3 / SICAM A8000 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 AK 3 / SICAM A8000 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) 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 AK 3 / SICAM A8000.
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.

The device proactively logs alarms and events and, if engineered, proactively transmits over supervisory protocols to monitoring and control systems, as and when they occur.

Many security related activities are logged as events of the type **AuditTrailAlarms**.

Event types “AuditTrailEvents” are defined as authorized activities which can be expected to occur in the routine use and maintenance of the IED.
Depending on used protocols logged events will be transmitted either spontaneously or via scan.

The following logging features are provided in SICAM AK 3 / SICAM A8000 and meet the requirements of *IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities, IEEE Std 1686-2013:*

- Unsuccessful login attempt: Three incorrect password entries in succession during a single log-in attempt. Successive failed log-in attempts after three generates a single entry into the audit trail listing the time of the last attempt and total number of log-in attempts that have occurred in succession
- Reboot: The rebooting or restarting of the IED by means of removing power or through the use of a device-resident rebooting mechanism such as a reset button, power-up sequence, or access software feature.
- Attempted use of unauthorized configuration software: The detection by the IED of an attempted use of configuration software, accessing computer, or a combination thereof that is not registered as legitimately able to be used for configuration of the IED.
- Time signal out of tolerance: The IED validates time synchronization messages received through protocol or dedicated time synchronization channels and alarm if the time synchronization message is not within the tolerances of the IED's internal/local clock.
- Invalid field hardware changes: The IED validates user-performable (as identified by the vendor) field hardware changes and alarm if the field hardware change is performed improperly (i.e., wrong I/O board inserted in a designated I/O slot).

More logged security events:

SICAM AK 3 / SICAM A8000

- Start of Security Logging
- Load and update of parameters
- Load and update of firmwares
- Login attempts (connection-password for remote operation)
  - successful login attempts
  - failed login attempts
  - Set and change of the connection-password for remote operation
- Connection setup from unknown IP address
- Connection setup with SICAM TOOLBOX II via the local SICAM AK 3 / SICAM A8000 interface
- Connection setup with SICAM TOOLBOX II via remote operation
- Status of the used ports
- Memory card (SD-Card) removed/inserted
- Messages generated from SICAM TOOLBOX II message simulation
- Start/Stop of CAEx online tests

SICAM TOOLBOX II

- SICAM TOOLBOX II User management
  - Define new user
  - Delete user
  - Change user password
  - Define new domain user
  - Delete domain user
- SICAM TOOLBOX II Role management
  - Define new role
  - Delete role
  - Change role
- Import of SICAM TOOLBOX II User/Roles in Data Distribution Center
- Start/Stop of Security Logging
- Configuration of the Syslog-Server
  - Server name
  - Port number
- Firmware updates
  - Firmwares of SICAM AK 3 / SICAM A8000
  - SICAM TOOLBOX II libraries
  - Updates of SICAM 230
  - Updates of SICAM SCALA 250

  (These updates are logged, independent of the tool which is used to do the update. E.g.: Master Data Update, Data Distribution Center, Import/Export Database, SICAM TOOLBOX II Live Update)
- Login attempts
  - successful login attempts
  - failed login attempts

SICAM A8000 CP-8000/21/22, SICAM AK3, SICAM TOOLBOXII

A syslog event is built up with following elements:

Element	Description
Date	Date when the event was received/logged from the syslog server
Time	Time when the event was received/logged from the syslog server
Facility	Source of the event [1)] – Security (RFC 3164: numerical code = 16 = local 0) – Authorization (RFC 3164: numerical code = 17 = local 1) – Application (RFC 3164: numerical code = 18 = local 2)
Severity (Level)	Severity oft the event [1)] – Alert (RFC 3164: numerical code = 1) – Critical (RFC 3164: numerical code = 2) – Error (RFC 3164: numerical code = 3) – Warning (RFC 3164: numerical code = 4) – Notice (RFC 3164: numerical code = 5)
HostName	IP address or Host Name of the device sending the event
Message Text	The message part of a syslog event consist of following elements: – yyyy-mm-dd ..... date when the event was created – Thh:mm:ss.ttt ..... time when the event was created – +hh:mm ..... time deviation from GMT – R#xxx_..... xxx = Region number (0..255) – C#xxx_..... xxx = Component number (0..255) – BSE#xxx_ ..... xxx = BSE number (000-020) – SSE#xxx ..... xxx = SSE number (000-254) Depending on the event the message text can contain variable additional information (%A1%, %A2%, %A3%).

SICAM A8000 CP-8050

A syslog event is built up with following elements:

Element	Description
Date	Date when the event was received/logged from the syslog server
Time	Time when the event was received/logged from the syslog server
Facility	Source of the event [1)] – Log Audit (RFC 3164: numerical code = 13) – LogAlert (RFC 3164: numerical code = 14)
Severity (Level)	Severity oft h event [1)] – Alert (RFC 3164: numerical code = 1) – Warning (RFC 3164: numerical code = 4)
HostName	IP address or Host Name of the device sending the event
Message Text	The message part of a syslog event consist of following elements: – yyyy-mm-dd ..... date when the event was created – Thh:mm:ss.ttt ..... time when the event was created – +hh:mm ..... time deviation from GMT Depending on the event the message text can contain variable additional information (%A1%, %A2%, %A3%).

Detailed information can be found in in the administrator manual for SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

Audit trail background (*IEEE Standard)*

Exception, regarding the IED itself, but

both SICAM AK 3 / SICAM A8000 series and SICAM TOOLBOX II provide a security logbook (syslog-client) which acquires and categorizes security-relevant events (syslog-events) according to their origin and severity.

SICAM AK 3 / SICAM A8000:

In SICAM AK 3 / SICAM A8000 syslog-events are sent from different sources to a central loghandler at the M-CPU.
These data can be sent automatically to an external syslog-server for further investigations.

One SICAM AK 3 / SICAM A8000 automation unit can operate up to 20 syslog-clients (depending on the HW platform, refer to ADMIN BHB, chapter 10).
CP-8000, CP-802x, CP-8050 can operate one syslog-client.

In addition, SICAM AK 3 / SICAM A8000 contain comprehensive functions for monitoring the system (error messages of all automation units located in the network as well as their system elements; 8 diagnostic classes)

SICAM TOOLBOX II

The output (via SICAM TOOLBOX II) is displayed in plaintext on the screen (also printable) and is structured hierarchically in

- Network overview diagnostic
- AU overview diagnostic
- AU individual diagnostic
- History:
  All errors occurring are entered reset-proof chronologically with time and date.
  The diagnostic data are stored locally and can be read out locally or remotely using the SICAM TOOLBOX II.
  Entries cannot be modified or deleted.
  The History diagnostic contains information with time stamp and contains 20 entries for each basic system element (M-CPU, C-CPU). Only the least events are stored, older entries are overwritten.

The logbook of the SICAM TOOLBOX II refers to the recording of events in connection with security relevant user actions.
The logbook entries are stored centrally in the SICAM TOOLBOX II database and can be arbitrarily filtered.
The access rights are defined by the role administration include the right to delete or export data records.
Older logbook entries are not overwritten. A “warning threshold” can be defined for a defined number of entries.

Storage record (*IEEE Standard)*

a) Comply: Syslog event ID is added to the record in case of event viewer of the operating system and a syslog server (matter of configuration of the syslog server), local storage is currently nor supported.
b) Comply
c) Comply: (matter of the syslog server configuration)
d) Comply

Audit trail event types (*IEEE Standard)*

a) Exceed (e.g.: also number of unsuccessful login attempts)
b) Comply
c) Exception
d) Comply, e.g.: Reboot by updating the 'Parameter' (SICAM WEB) or the warning “Parameters loaded”
e) Comply
f) Comply
g) Comply
h) Comply
i) Comply
j) Comply
k) Comply
l) Comply

Change configuration data (*IEEE Standard)*

b) Change tracking: The configuration tool provides change tracking of any and all changes to the IED configuration
c) Use monitoring: The configuration tool logs when a user begins and ends using the tool**.**
d) Download to IED: The configuration tool logs when a user applies (downloads) a configuration and or firmware revision to an IED

All items mentioned above (and many more) are covered by syslog events.

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 at 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 AK 3 / SICAM A8000

At startup and at regular intervals, SICAM AK 3 / SICAM A8000 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 AK 3 / SICAM A8000, 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 and 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 to third parties, as a whole or in parts, 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 measures to 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 condemn insecure programming styles 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 AK 3 / SICAM A8000 and SICAM TOOLBOX II are developed by trustworthy and trained employees.
For example, the entire development team was trained in "secure coding".

b) Siemens develops SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II in accordance with the recognized CMMI development and quality assurance process.

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

c) Siemens maintains a documented development security process for SICAM AK 3 / SICAM A8000 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 has set up a programming guideline for SICAM AK 3 / SICAM A8000 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 for SICAM AK 3 / SICAM A8000 and new releases of the SICAM TOOLBOX II product is based on a specified and documented approval process.
This also applies to security patches for the two products.

Firmware quality assurance (*IEEE Standard)*

Our strict QA process covers the practices recommended by IEEE Std. C37.231:

Siemens AG develops SICAM AK 3 / SICAM A8000 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

SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II are developed by trained and trustworthy personnel. The entire development team, for example, was given extensive training in "secure coding".
Siemens AG has a documented development security process for
SICAM AK 3 / SICAM A8000 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.

Siemens AG has a programming guideline for SICAM AK 3 / SICAM A8000 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.
The approval of new firmware releases of SICAM AK 3 / SICAM A8000 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.*

This requirement is not relevant because no customer data is captured for product development.

NOTE

Information for project planning/implementation and system service:

This requirement is not relevant to the products and must be taken into consideration during project planning / implementation and product / system service. This requirement is not relevant because no customer data is captured for product development.

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 the software packages deployed shall be maintained and allow all software changes to be traced.*

SICAM AK 3 / SICAM A8000

a) Product development for SICAM AK 3 / SICAM A8000 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 the SICAM AK 3 / SICAM A8000 and updates, enhancements and security patches is conducted in a testing environment that is separated from the live system.

c) The source code for SICAM AK 3 / SICAM A8000 is only available from Siemens. No source code is stored on live systems.

d) The integrity of SICAM AK 3 / SICAM A8000 firmware and parameter binaries is verified in the target system to detect unauthorized changes.

e) For SICAM AK 3 / SICAM A8000 a version history for the entire software is maintained and allows all software changes to be traced.

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 updates, enhancements and security patches is conducted in a testing environment that is separated from the live system.

c) The source code for SICAM TOOLBOX II is only available from Siemens. No source code is stored on live systems.

d) Since SICAM TOOLBOX II is installed using an Installer, the Installer's security mechanisms are available to protect the integrity of the application.

e) The version history maintained for the entire software of the SICAM TOOLBOX II product allows all software changes to be traced.

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 well-defined 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 AK 3 / SICAM A8000 and SICAM TOOLBOX II are made available by Siemens.

Systems updates must be defined depending on the individual system and governed by contract.

2.5.5 Configuration and Change Management, Rollback

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

a) SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II are developed on the basis of a configuration and change management process.

b) Note

NOTE

Information for project planning/implementation and system service:

Rollback to older firmware versions of a SICAM AK 3 / SICAM A8000 system configuration can be performed firmware-specifically.

Regular backups created within the scope of project planning/implementation and product/system service enable convenient rollback to older parameter versions of a system configuration.

This requirement must be considered for 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 in place in order 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 and fixed - and how recommended measurements are reported to all system owners. Furthermore the process shall define timelines for each step in the vulnerability management process. The contractor shall inform the customer early about known security vulnerabilities, even if there is no patch available. The customer shall treat this information confidentially.

For SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II, Siemens has set up a documented process to address security vulnerabilities.

Based on this process all the parties involved, and also external parties, can report actual and potential security vulnerabilities for SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

For SICAM AK 3 / SICAM A8000 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 yet become available.

NOTE

Information for project planning/implementation and system service:

SICAM TOOLBOX II is based on the Microsoft Windows operating system.
The consideration of security vulnerabilities of SICAM TOOLBOX II neither covers the operating system nor standard applications of the computer on which SICAM TOOLBOX II is installed as an 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 corresponding source code documentation.*

NOTE

Siemens precludes a source code escrow. As a rule, an escrowed source code is not subject to maintenance and is hardly usable if actually needed in the event of insolvency.

2.6 Backup, Recovery and Disaster Recovery

2.6.1 Backup: Concept, Method, Documentation and Test

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

Backups must be created by the customer for systems set up using SICAM TOOLBOX II. Online parameter changes in the SICAM AK 3 / SICAM A8000 device can be undone by installing the parameter sets stored in the SICAM TOOLBOX II.

Data backup and recovery procedures of the various applications and the entire system, respectively, and of the respective configurations are documented in the administrator manual for SICAM AK 3 / SICAM A8000 and SICAM TOOLBOX II.

The configuration parameters of decentral SICAM AK 3 / SICAM A8000 components are stored centrally in SICAM TOOLBOX II.

NOTE

Information for project planning/implementation and system operation:

Concepts and procedures must be created within the framework of system development in order to enable the backup and restoration of the entire system including e.g. the automation of the backup process.

Within the framework of project planning/implementation it must be defined which persons are responsible for which system operation tasks and when the transfer of responsibility takes place (e.g. site acceptance test, end of test operation, end of the warranty period, etc.).

Backup and restoration procedures must be tested at cyclical intervals during system operation and the status of backup creation must be continuously monitored.

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 not relevant to the products and must be taken into consideration during project planning / implementation and system service.

A Table of Compliance (TOC)

A.1 Table of Compliance (TOC)as per Standard IEEE 1686:2013

This section provides a table of compliance (TOC) to illustrate the proper construction of the table and to indicate the possible range of responses that might be expected from a vendor who is citing compliance for its product to this standard.

The TOC lists every subclause of Clause 5 of the standard IEEE_Std_1686-2013 on a separate line. For each subclause, the level of compliance for the product in question is indicated. The following responses are used:

- Acknowledge: Used as a placeholder when no requirement is presented in the subclause
- Exception: Product fails to meet one or more of the stated requirements of the subclause
- Comply: Product fully meets the stated requirements of the subclause
- Exceed: Product exceeds one or more of the stated requirements of the subclause

In the column for comments links to the respective chapters of this document are provided for more detailled information.

Clause number	Clause/subclause title	Status	Comment
5	IED cyber-security features	Acknowledge	
5.1	Electronic access control	Acknowledge	
5.1.1	IED access control overview	Comply	Refer to chapter 2.4.2 Authorisation of Activities on User and System Level; but no open and documented interface to change user accounts, passwords, and roles,
5.1.2	Password defeat mechanisms	Comply	Refer to chapter 2.4.2 Authorisation of Activities on User and System Level
5.1.3	Number of individual users	Exceed (SICAM TOOLBOXII for SICAM A8000 CP-8050)	Refer to chapter 2.4.2 Authorisation of Activities on User and System Level but Exception in case of SICAM WEB (for SICAM A8000 CP-8000/21/22): 3 individual users only
5.1.4	Password construction	Comply	Refer to chapter 2.4.2 Authorisation of Activities on User and System Level
5.1.5	IED access control	Acknowledge	
5.1.5.1	Authorization levels by password	Comply (SICAM TOOLBOXII for SICAM A8000 CP-8050)	Refer to chapter 2.4.2 Authorisation of Activities on User and System Level but Exception in case of SICAM WEB (for SICAM A8000 CP-8000/21/22).
5.1.5.2	Authorization using role-based access control (RBAC)	Exceed (SICAM TOOLBOXII for SICAM A8000 CP-8050)	Refer to chapter 2.4.1.1 Role-Based Access Model but Exception in case of SICAM WEB (for SICAM A8000 CP-8000/21/22).
5.1.6	IED main security functions	Acknowledge	Refer to chapter 2.4.2 Authorisation of Activities on User and System Level
5.1.6 a)	View data	Comply	All items a) – g) are covered by the default roles of SICAM TOOLBOX II

Clause number	Clause/subclause title	Status	Comment
5.1.6 b)	View configuration settings	Comply	All items a) – g) are covered by the default roles of SICAM TOOLBOX II
5.1.6 c)	Force values	Comply	All items a) – g) are covered by the default roles of SICAM TOOLBOX II
5.1.6 d)	Configuration change	Comply	All items a) – g) are covered by the default roles of SICAM TOOLBOX II
5.1.6 e)	Firmware change	Comply	All items a) – g) are covered by the default roles of SICAM TOOLBOX II
5.1.6 f)	ID/password or RBAC management	Comply	All items a) – g) are covered by the default roles of SICAM TOOLBOX II
5.1.6 g)	Audit trail	Comply	All items a) – g) are covered by the default roles of SICAM TOOLBOX II
5.1.7	Password display	Comply	Refer to chapter 2.4.2 Authorisation of Activities on User and System Level
5.1.8	Access timeout	Exception	Refer to chapter 2.4.1.2 User Authentication and Logon Process; this feature is not supported or period time is not parameterizable
5.2	Audit trail	Acknowledge	
5.2.1	Audit trail background	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.2	Storage capability	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.3	Storage record	Acknowledge	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.3 a)	Event record number	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.3 b)	Time and date	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.3 c)	User identification	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.3 d)	Event type	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4	Audit trail event types	Acknowledge	
5.2.4 a)	Log in	Exceed	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts also number of unsuccessful login attempts
5.2.4 b)	Manual log out	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 c)	Timed log out	Exception,	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts Timed log out: Log out of user after a predefined period of inactivity elapses; feature not supported
5.2.4 d)	Value forcing	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 e)	Configuration access	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts

Clause number	Clause/subclause title	Status	Comment
5.2.4 f)	Configuration change	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 g)	Firmware change	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 h)	ID/password creation or modification	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 i)	Password deletion	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 j)	Audit log access	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 k)	Time/date change	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.2.4 l)	Alarm incident	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.3	Supervisory monitoring and control	Acknowledge	
5.3.1	Overview of supervisory monitoring and control	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.2	Events	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.3	Alarms	Acknowledge	
5.3.3 a)	Unsuccessful login attempt	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.3 b)	Reboot	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.3 c)	Attempted use of unauthorized configuration software	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.3 d)	Invalid configuration or firmware download	Exception	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols feature not supported
5.3.3 e)	Unauthorized configuration or firmware file	Exception	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols feature not supported
5.3.3 f)	Time signal out of tolerance	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.3 g)	Invalid field hardware changes	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.4	Alarm point change detect	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.3.5	Event and alarm grouping	Exception	Refer to chapter 2.3.1.1 Deployed Communication Technologies and

Clause number	Clause/subclause title	Status	Comment
			Network Protocols user cannot group events and alarms
5.3.6	Supervisory permissive control	Exception	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols no diagnostic port has the ability to be enabled and disabled remotely
5.4	IED cyber security features	Acknowledge	
5.4.1	IED functionality compromise	Neither comply nor Exception:	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols Primary IED functions cannot be compromised by ports or by a communication protocol.
5.4.2	Specific crytographic features	Acknowledge	Refer to chapter 2.1.1.6 Encryption of Sensitive Data during Storage and Transmission
5.4.2 a)	Webserver functionality	Comply	Refer to chapter 2.1.1.6 Encryption of Sensitive Data during Storage and Transmission
5.4.2 b)	File transfer functionality	Exception	Refer to chapter 2.1.1.6 Encryption of Sensitive Data during Storage and Transmission SFTP not supported
5.4.2 c)	Text-oriented terminal connections	n/a	Refer to chapter 2.1.1.6 Encryption of Sensitive Data during Storage and Transmission SSH not necessary, because virtual terminal communication not supported
5.4.2 d)	SNMP network management	Comply	Refer to chapter 2.1.1.6 Encryption of Sensitive Data during Storage and Transmission
5.4.2 e)	Network time synchronization	Exceed	Refer to chapter 2.1.1.6 Encryption of Sensitive Data during Storage and Transmission some more time synchronization options, e.g. GPS, DCF77, ...
5.4.2 f)	Secure tunnel functionality	Comply	Refer to chapter 2.1.1.6 Encryption of Sensitive Data during Storage and Transmission
5.4.3	Cryptographic techniques	Comply	Refer to chapter 2.1.1.7 Cryptographic Standards
5.4.4	Encrypting serial communications	Exception	Refer to chapter 2.3.2.1 Secure Remote Access NOT encrypted serial communication is provided
5.4.5	Protocol-specific security features	Comply	Refer to chapter 2.3.1.1 Deployed Communication Technologies and Network Protocols
5.5	IED configuration software	Acknowledge	
5.5.1	Authentication	Comply	Refer to chapter 2.4.1.2 User Authentication and Logon Process
5.5.2	Digital signature	Comply	Refer to chapter 2.1.1.7 Cryptographic Standards

Clause number	Clause/subclause title	Status	Comment
5.5.3	ID/password control	Comply	Refer to chapter 2.4.1.2 User Authentication and Logon Process and chapter 2.4.2 Authorisation of Activities on User and System Level
5.5.4	ID/password controlled features	Comply	Refer to chapter 2.4.1.2 User Authentication and Logon Process and chapter 2.4.2 Authorisation of Activities on User and System Level
5.5.4.1	View configuration data	Comply	Refer to chapter 2.4.1.1 Role-Based Access Model and chapter 2.4.2 Authorisation of Activities on User and System Level
5.5.4.2	Change configuration data	Comply	Refer to chapter 2.4.1.1 Role-Based Access Model
5.5.4.2 a)	Full access	Comply	Refer to chapter 2.4.1.1 Role-Based Access Model
5.5.4.2 b)	Change tracking	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.5.4.2 c)	Use monitoring	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.5.4.2 d)	Download to IED	Comply	Refer to chapter 2.4.6 Logging, Audit Trails, Time Stamps and Alarm Concepts
5.6	Communications port access	Comply	Refer to chapter 2.1.1.9 Secure Standard Configuration, Installation and Start-Up
5.7	Firmware quality assurance	Comply	Refer to chapter 2.5.1 Secure Development Standards, Quality Management and Release Processes

List of Reference Documents

BDEW White Paper - Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Requirements for Secure Control and Telecommunication Systems)	V1.1
IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities	IEEE Std 1686™-2013 (Revision of IEEE Std 1686-2007)
SICAM RTUs / SICAM TOOLBOX II - Administrator Security Manual	DC0-115-2
SICAM AK 3 User Manual	DC2-028-2
SICAM RTUs ▪ Ax 1703 Common Functions Protocol Elements	DC0-023-2
SICAM AK 3 System Description	MC2-025-2

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 White Paper

"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.

I

IED

Intelligent **E**lectronical **D**evice

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 AK 3 / SICAM A8000 systems to Ethernet LAN according to IEEE 802.3

P

Patch

A patch (also referred to as a "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 of 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 has been developed further and standardized under its new name of TLS. Thus, version 1.0 of TLS corresponds to version 3.1 of SSL.