

SIEMENS

SICAM PAS/PQS,
SICAM SCC,
SICAM PQ Analyzer
Security Conformance
Self-Assessment

SICAM PAS/PQS V8.20/SICAM SCC
V9.12/SICAM PQ Analyzer V3.20

Manual

Preface

Table of Contents

General Information

Objectives

Instructions for Use

BDEW Whitepaper Security Requirements

IEC 62443-4-2 Security Requirements

Literature

Glossary

1

2

3

4

5

**NOTE**

For your own safety, observe the warnings and safety instructions contained in this document, if available.

Disclaimer of Liability

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

Document version: E50417-T1040-C542-A4.01

Edition: 03.2023

Version of the product described: SICAM PAS/PQS V8.20/
SICAM SCC V9.12/SICAM PQ Analyzer V3.20

Copyright

Copyright © Siemens 2023. All rights reserved.

The disclosure, duplication, distribution and editing of this document, or utilization and communication of the content are not permitted, unless authorized in writing. All rights, including rights created by patent grant or registration of a utility model or a design, are reserved.

Trademarks

SIPROTEC, DIGSI, SIGRA, SIGUARD, SIMEAS, SAFIR, SICAM, and MindSphere are trademarks of Siemens. Any unauthorized use is prohibited.

Preface

Purpose of the Manual

This document describes the conformance assessment of the following products:
with relevant parts (product focus) of the security requirements of the:

- BDEW Whitepaper – Requirements for Secure Control and Telecommunication Systems, Version 2.0
- IEC 62443-4-2

as set forth in the subsequent chapters.

Scope

This document applies to the products of the SICAM PAS product line.
These are in detail:

- SICAM PAS/PQS, Version V 7.0 and higher
- SICAM SCC, Version V 7.0 and higher
- SICAM PQ Analyzer, Version V 2.0 and higher

This document only describes product characteristics of the SICAM PAS product line. 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:

- Product development
- Product service

The following fields are not covered in this document:

- System integration (entire system consisting of SIPROTEC 4, DIGSI 4 and other automation components, network components, protection devices, etc.)
- Project planning / implementation
- System service
- Control center operation/system operation

Target Group

This document is primarily intended for persons working in the following areas:

- Sales of systems and equipment
- Project planning/implementation

Security Information

Siemens provides products and solutions with security functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber-threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept.

Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyberthreats.

For more information about grid security, visit: <https://www.siemens.com/gridsecurity>

Table of Contents

	Preface.....	3
1	General Information.....	7
2	Objectives.....	8
3	Instructions for Use.....	9
4	BDEW Whitepaper Security Requirements.....	10
4.1	General Requirements.....	11
4.1.1	Secure System Architecture.....	11
4.1.2	Patching and Patch Management.....	12
4.1.3	Provision of Security Patches for all System Components.....	12
4.1.4	Support for Deployed System Components.....	12
4.1.5	Encryption of Sensitive Data during Storage and Transmission.....	13
4.1.6	Cryptographic Mechanisms.....	13
4.1.7	Secure Standard Configuration.....	13
4.1.8	Integrity Testing.....	13
4.1.9	Use of Cloud Services.....	14
4.1.10	Documentation Requirements.....	14
4.2	Project Management.....	15
4.2.1	Contacts.....	15
4.2.2	Security and Acceptance Testing.....	15
4.2.3	Secure Data Storage and Transmission.....	15
4.2.4	Delivery of Project-Specific Modification.....	16
4.3	Base System	16
4.3.1	System Hardening.....	16
4.3.2	Malware Protection.....	17
4.3.3	Autonomous User Authentication.....	17
4.3.4	Virtualization Technologies.....	18
4.4	Network and Communications	19
4.4.1	Used Protocols and Technologies.....	19
4.4.2	Secure Network Structure.....	20
4.4.3	Documentation of Network Structure and Configuration.....	20
4.4.4	Secure Remote Access.....	21
4.4.5	Wireless Technologies.....	21
4.5	Application	22
4.5.1	Role Concepts.....	22
4.5.2	User Authentication and Login.....	23
4.5.3	Authorization of Actions at the User and System Levels.....	23

4.5.4	Web Applications and Web Services.....	23
4.5.5	Integrity Testing.....	24
4.5.6	Logging.....	24
4.6	Development.....	25
4.6.1	Secure Development Standards, Quality Management and Approval Processes.....	25
4.6.2	Secure Development, Test and Staging Systems, Integrity Testing.....	26
4.7	Maintenance.....	27
4.7.1	Maintenance Process Requirements.....	27
4.7.2	Secure Update Processes.....	27
4.7.3	Configuration and Change Management, Rollback.....	27
4.7.4	Handling of Vulnerabilities.....	28
4.8	Data Back-Up and Emergency Planning.....	28
4.8.1	Back-up: Concept, Method, Documentation, Testing.....	28
4.8.2	Emergency Concept and Recovery Plans.....	29
5	IEC 62443-4-2 Security Requirements.....	30
5.1	SICAM PAS/PQS.....	31
5.1.1	FR1.....	31
5.1.1.1	Identification and Authentication Control.....	31
5.1.2	FR2.....	32
5.1.2.1	Use Control.....	32
5.1.3	FR3.....	34
5.1.3.1	System Integrity.....	34
5.1.4	FR4.....	35
5.1.4.1	Data Confidentiality.....	35
5.1.5	FR5.....	36
5.1.5.1	Restricted Data Flow.....	36
5.1.6	FR6.....	36
5.1.6.1	Timely Response to Events.....	36
5.1.7	FR7.....	36
5.1.7.1	Resource Availability.....	36
5.2	SICAM SCC.....	37
5.2.1	FR1.....	37
5.2.1.1	Identification and Authentication Control.....	37
5.2.2	FR2.....	40
5.2.2.1	Use Control.....	40
5.2.3	FR3.....	42
5.2.3.1	System Integrity.....	42
5.2.4	FR4.....	44
5.2.4.1	Data Confidentiality.....	44
5.2.5	FR5.....	44
5.2.5.1	Restricted Data Flow.....	44
5.2.6	FR6.....	45
5.2.6.1	Timely Response to Events.....	45
5.2.7	FR7.....	45
5.2.7.1	Resource Availability.....	45
	Literature.....	48
	Glossary.....	49

1 General Information

This document describes:

- The conformance of the SICAM software product line with the security requirements specified in the **BDEW Whitepaper – Requirements for Secure Control and Telecommunication Systems**

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.

3 Instructions for Use

Chapter 4 *BDEW Whitepaper 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 software products, chapter numbers and names from the BDEW White Paper have been applied to this document.

4 BDEW Whitepaper Security Requirements

4.1	General Requirements	11
4.2	Project Management	15
4.3	Base System	16
4.4	Network and Communications	19
4.5	Application	22
4.6	Development	25
4.7	Maintenance	27
4.8	Data Back-Up and Emergency Planning	28

4.1 General Requirements

4.1.1 Secure System Architecture

<p>BDEW 4.1.1</p>	<p>ISO/IEC 27002:2013: 9.4.1, 13.1.3, 14.2.5, 14.2.7, 17.2.1</p> <p>Individual components and the entire system shall be designed and developed to support secure operations. Secure system design principles include:</p> <p>Security by design: The entire system and its individual components are designed on the basis of and with a focus on security. Deliberate attacks and unauthorized actions are explicitly taken into account while any repercussions arising from a security event are minimized by the system's inherent design.</p> <p>Minimal need-to-know principle: Each component and each user is only assigned the rights they need to execute a desired action. Applications and network services, for examples, are not run under administrator privileges, but only with the bare minimum of required system access rights.</p> <p>Defence-in-depth principle: Security risks are not tackled via single protection measures, but limited through the implementation of staggered, multi-level and complementary security measures.</p> <p>Redundancy principle: The entire system is designed to ensure that the failure of individual components does not impair security-related functions. The system's design lowers the likelihood and impact of issues caused by unrestricted requests for system resources such as e.g. main memory (RAM) or network bandwidth (so-called resource consumption or DoS attacks).</p>
------------------------------	---

The SICAM software products support techniques for the implementation of system designs that ensure the secure operation of the entire system. SICAM PAS/PQS, SICAM SCC and SICAM Analyzer fulfill the Siemens SI Security Baseline Requirements and follow the certified IEC 62443-4-1 ML-4 process.



NOTE

Information for project planning / implementation:

As a basis for secure system design and secure system operation, the manuals for the SICAM PAS product line 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)
- 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 an entire system.

The products support person-related user accounts which can be assigned role-based rights.

The *SICAM PAS/PQS Security Manual* describes supported and recommended security measures for the implementation of a security architecture within the system according to the defense in depth principle.

The products of the SICAM software product line support many different types of redundancy. On the one hand, these products support redundant communication connections to the control center and the bay devices. On the other hand, they enable the redundant operation of applications on different computers. For a detailed description, refer to the *SICAM PAS/PQS Redundancy manual*.

4.1.2 Patching and Patch Management

<p>BDEW 4.1.2</p>	<p>ISO/IEC 27002:2013 / 27019:2017: 12.6.1</p> <p>All system components shall be patchable. The supplier shall support a patch management process for both the individual components and the entire system, designed to enable the control and management of security patch testing, installation and documentation.</p> <p>The operator himself resp. the assigned service provider shall be able to install the security patches and updates. Patch installations resp. uninstalls shall be authorised by the operator and shall not occur automatically. Any installation resp. uninstall shall be recorded in a transparent and tamper-proof way within the system.</p> <p>The integrity of security patches and updates shall be verifiable using a cryptographic mechanism.</p>
-------------------------------------	--

The products of the SICAM software product line fully support the installation of patches. The typical Windows software installation functions are provided for this purpose. Siemens regularly checks the security updates for software components provided by third party manufacturers (including the operating system or the database) in order to ensure their compatibility with the SICAM software. Siemens provides a list of released security updates at regular intervals. Any patches which have not been released due to incompatibility are separately indicated in this list.

4.1.3 Provision of Security Patches for all System Components

<p>BDEW 4.1.3</p>	<p>ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 12.6.1</p> <p>The supplier shall ensure that security updates are available for all system components throughout the entire contractually stipulated operating timeframe.</p> <p>The contractor shall obtain, test and – where necessary – forward updates from the respective manufacturers for basic components that were not developed by the contractor himself such as the operating system, libraries or database management systems. All update testing, approval and delivery shall take place within an adequate, contractually stipulated timeframe.</p>
-------------------------------------	---

Depending on the contractual terms, Siemens provides security updates for SICAM software products throughout a product's entire life cycle.

- Updates are made available within an appropriate time frame governed by contract.
- Patches are only provided after careful 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.

4.1.4 Support for Deployed System Components

<p>BDEW 4.1.4</p>	<p>ISO/IEC 27002:2013 / 27019:2017: 12.6.1, 14.2.7</p> <p>The supplier shall ensure that within the planned and contractually stipulated operating timeframe, manufacturer support and security updates are available for system components developed by both the supplier and third-parties (e.g. operating system, database management system etc.). A binding agreement should cover the discontinuation procedure as well as relevant minimum terms like e.g. last customer shipping and end of support.</p>
-------------------------------------	---

Manufacturer support and the delivery of security updates for the third party software components used is monitored within the framework of the patch management process implemented for SICAM software products. Siemens focuses on particularly long-lasting components. If required, Siemens provides information on the end of life of old versions and provides support for the migration to later versions.

The end-of-life terms for the SICAM software product line define all the relevant deadlines such as **last customer ship date** and **end of support**.

4.1.5 Encryption of Sensitive Data during Storage and Transmission

BDEW 4.1.5	ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 12.4.2, 13.1.2, 18.1.3, 18.1.4 Confidential data shall only be stored resp. transmitted encrypted.
-----------------------------	---

The contractor is not responsible for the secure archiving of data records (device delivery).

Passwords are stored in a protected manner in the data records.

In addition, central user management components (e.g. Microsoft Active Directory Server) can be used for storing passwords and user information.

The cryptographic keys are transmitted in secure PKCS#12 containers.

SICAM PAS and SICAM PQS do not use the Windows Integrated Login.

Logon to the Sybase database is performed via Integrated Authentication Mode. Passwords are not protected in the SICAM PAS and SICAM PQS application.

Windows user management is used for the administrator, user and the network protocols.

4.1.6 Cryptographic Mechanisms

BDEW 4.1.6	ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 10.1.2, 13.1.4 ENR, 18.1.5 When selecting cryptographic mechanisms, national legislation shall be taken into account. Only approved mechanisms and minimum key sizes shall be used that are considered secure for the foreseeable future according to state-of-the-art technological knowledge. The supplier shall not use custom cryptographic algorithms.
-----------------------------	--

For the SICAM software product line, use only recognized encryption algorithms (**Windows cryptography provider**, OpenSSL) with key lengths that are considered as secure according to the current state of the art and to the IEC 62351-3 standard. No proprietary procedures are used.

Encrypted versions of the IEC 61850 MMS, DNP 3i and IEC 60870-5-104 protocols in accordance with IEC 62351 are available for the communication between SICAM PAS and the telecontrol center and also between SICAM PAS and the bay device.

4.1.7 Secure Standard Configuration

BDEW 4.1.7	ISO/IEC 27002:2013 / 27019:2017: 9.4.4, 12.5.1, 14.3.1 After initial installation, resp. at start-up or restart, the entire system shall be configured for a secure operating state. This defined basic configuration shall be documented. Services and functions as well as data that are only needed for development or testing shall be removed demonstrably resp. permanently deactivated before delivery resp. before the switch to live operations.
-----------------------------	---

All security relevant services (for example remote maintenance) are switched off by default in the SICAM software products. Any services required must be enabled in case of need. To do this, any default passwords must be modified as per the instructions in the respective manuals.

Any further security mechanisms (for example firewalls) must be provided by the system manufacturer. For more detailed information on security mechanisms, refer to the *SICAM PAS/PQS Security manual*. The user manual includes a description as to how the system is transferred to a secure state following installation.

4.1.8 Integrity Testing

BDEW 4.1.8	ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 14.2.1, 14.2.4 It shall be possible to check system files, applications, configuration files and application parameters for integrity, for example through cryptographic checksums.
-----------------------------	--

The integrity of both the data and the installed operating system and the applications can be checked and even protected using the corresponding whitelisting software as for example McAfee Application Control.

4.1.9 Use of Cloud Services

BDEW 4.1.9		ISO/IEC 27002:2013 / 27019:2017: 15.1.1, 15.1.2, 15.2.1
		Where cloud services are used, the following requirements apply:
	a)	Agreements shall be made with the cloud service provider about security-related processes for cloud infrastructure operations.
	b)	Functions for the control of Critical Infrastructures, where manipulations could threaten the energy supply, shall not be realized in external cloud services.
	c)	Downtime of a cloud service resp. access to this service shall not lead to significant restrictions of the system's defined basic function. Cloud service disruptions or outages shall also be considered in the emergency concept and restoration plans (see 4.8.2).

4.1.10 Documentation Requirements

BDEW 4.1.10	ISO/IEC 27002:2013 / 27019:2017: 7.2.2, 12.1.1, 14.1.1, 14.2.7
	<p>At the latest, the client shall receive project-specific documentation at the system's handover. For individual components and entire systems, the documentation shall cover a description of all security-related system settings and parameters as well as their standard values. Furthermore, the documentation shall list and briefly describe security-specific implementation details (like the employed cryptographic mechanisms).</p> <p>The documentation shall also comprise additional information on the entire system's system architecture. This includes the system's basic and fundamental structure as well as interactions between all involved components. In particular, this part of the documentation shall highlight security-related or sensitive system components as well as their mutual dependencies and interactions.</p>

For SICAM software products, the high-level design and the basic system structure, including interaction of the components involved, is described by the example of typical system configurations in the manuals. See, for example, the typical system configurations in the administrator manual for SICAM PAS and SICAM PQS.

A series of manuals is provided for SICAM PAS and SICAM PQS. These manuals are structured according to different topics and contents relevant for the following users:

- Administrators
- System designers and integrators
- Commissioners
- Users

The following manuals are particularly relevant for security issues:

- *SICAM PAS/PQS Installation*
- *SICAM PAS/PQS, Security*

The Security manual explains all the security-relevant functions implemented and also provides information on the secure commissioning and configuration of SICAM PAS and SICAM PQS within the framework of a system.



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. The system design of the individual customer can differ from these typical configurations.

4.2 Project Management

4.2.1 Contacts

BDEW 4.2.1	ISO/IEC 27002:2013 / 27019:2017: 6.1.1, 6.1.5, 15.1.2 The supplier shall define a contact who is responsible for IT security during the tender process and the system development phase as well as throughout the planned operations and maintenance timeframe.
----------------------	---



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 product development process.

4.2.2 Security and Acceptance Testing

BDEW 4.2.2	ISO/IEC 27002:2013 / 27019:2017: 14.2.7, 14.2.8, 14.2.9, 15.2.1 Prior to delivery, the entire system's components and key functions shall be subjected to security and stress testing by the contractor – in a representative configuration and by an organizational unit independent of the development team. The actual procedure shall be discussed and agreed in coordination with the client. The results of these tests as well as the associated documentation (software versions, test configuration etc.) shall be made available to the client. In addition, the client shall have the right to undertake these tests himself or to have them carried out by an external service provider. The type and scope of the acceptance tests shall be defined by the client. For these tests, the client resp. the assigned service provider shall be given system access with a maximum of technologically possible access rights.
----------------------	---

During product development, the individual system components (firmware, hardware, communication, etc.) and the key functions of an integral SICAM 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.

Security assessments are performed by Siemens Product-CERT at regular intervals.

4.2.3 Secure Data Storage and Transmission

BDEW 4.2.3	ISO/IEC 27002:2013 / 27019:2017: 6.2.1, 8.3.3, 10.1.1, 13.2.2, 13.2.3, 13.2.4, 14.3.1 Confidential client data that is required or processed during the development and maintenance process shall be encrypted during transmission via insecure connections. When saved on mobile storage media or systems, such data shall only be stored encrypted. The amount and duration of data storage shall be limited to a contractually specified 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. No contractor data is captured for product development.

4.2.4 Delivery of Project-Specific Modification

BDEW 4.2.4	ISO/IEC 27002:2013 / 27019:2017: 14.2.7 For custom projects and project- resp. client-specific expansions, adjustments and engineering services, all project-specific parameterizations, changes and adaptations shall be comprehensively documented and supplied to the client in full.
----------------------	--



NOTE

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

4.3 Base System

4.3.1 System Hardening

BDEW 4.3.1	ISO/IEC 27002:2013 / 27019:2017: 9.4.4, 12.6.2, 13.1.2, 14.2.4, 14.2.10 ENR All components of the base system shall be permanently hardened according to recognized best practice guidelines and the latest service packs and security patches shall be installed. Unnecessary users, default users, software, network protocols and services shall be uninstalled or – where an uninstall isn't possible – permanently deactivated and protected from accidental reactivation. The entire system's secure basic configuration shall be reviewed and documented.
----------------------	--

All the components of the SICAM software product line are permanently hardened according to well-known best-practice guides, which enables the secure basic configuration of all the products of the SICAM software product line.

The *Security manual* provides important information and demonstrates options for system hardening. The commissioner or system integrator is responsible for the execution of these hardening measures which must be checked before handing over the system for live operation.

Maintenance releases and hotfixes including security patches are made available for the SICAM software products in a timely manner. A security patch management process is available for this purpose.

Security advisories and bulletins are published on the Siemens Product-CERT website (www.siemens.com/cert/) to inform customers about security vulnerabilities affecting Siemens products and to recommend applicable remediation measures.



NOTE

Information for project planning/implementation and system service:

SICAM software products include 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 other default software must be designed, implemented, and maintained within the scope of system development, project planning/implementation and system service.

4.3.2 Malware Protection

BDEW 4.3.2	ISO/IEC 27002:2013 / 27019:2017: 12.2.1 All networked systems shall be equipped with malware protection at the appropriate location. Alternatively to malware protection provided on all system components, the supplier can submit a comprehensive malware protection concept that provides equal protection. Where the use of a pattern-based solution is intended, these pattern files shall be updateable in a timely and automated manner. Such updates shall not take place via direct connection to update servers on external networks like the internet. For terminal systems, the time of updates needs to be configurable.
-----------------------------	--

Recommendations for released antivirus software are provided for SICAM software products. In addition, the Security manual provides configuration notes and suggestions for automatic pattern distribution.

Recommendations for released antivirus software are provided for SICAM products.



NOTE

Information for project planning/implementation and system service:

SICAM software products include neither hardware components nor the operating system nor other standard software such as Microsoft Office or Adobe Acrobat Reader. The virus protection must be designed and implemented within the framework of project planning/implementation.

4.3.3 Autonomous User Authentication

BDEW 4.3.3	ISO/IEC 27002:2013 / 27019:2017: 9.2.1, 9.2.2, 9.4.2 Data required for user identification and authentication shall not be obtained exclusively from outside the process network.
-----------------------------	---

User authentication can be performed via both local user management on the corresponding computer and centrally (for example, via a Microsoft Active Directory Domain Service in the internal process network).

4.3.4 Virtualization Technologies

BDEW 4.3.4	ISO/IEC 27002:2013 / 27019:2017: 12.1.3, 12.3.1, 12.6.1, 13.1.3, 17.2.1	
	The following requirements govern the use of virtualization technologies:	
	a)	Virtualized components assigned to different security or trust zones (e.g. internal components and DMZ components) shall not be operated on the same virtualization servers. It shall not be possible to bypass the network segmentation of segregated security zones via virtualization servers.
	b)	Networks used for management and administration services as well as data storage of the virtualization infrastructure shall be segregated from other networks by firewalls with only the minimum of required network services enabled in a restrictive manner. Access to the management and administration services and the above-mentioned networks shall be restricted to administrators only.
	c)	The virtualization layer, the management and administration interfaces as well as the associated infrastructure shall be configured, secured and hardened identically and according to manufacturer recommendations. They shall also be included in the patch management and backup concept.
	d)	The virtualization servers shall have sufficient resources for operating all of the virtualized components they are running. This is especially important for high-load operating situations.
e)	Any outage of virtualization servers or of other components of the virtualization infrastructure shall have no negative impact on the defined availability requirements. Disruptions and outages of the virtualization environment shall also be covered and considered in the emergency concept and restoration plans (see 4.8.2 Emergency Concept and Recovery Plans).	

SICAM software products can be installed in virtualization systems as described in the respective installation and operation manuals. Securing the virtualization environment and ensuring the availability of the necessary computational resources are measures that need to be addressed during the project planning/implementation and system service activities.

4.4 Network and Communications

4.4.1 Used Protocols and Technologies

BDEW 4.4.1	ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 9.4.2, 10.1.1, 10.1.2, 12.9.1 ENR, 13.1.1, 13.1.2, 13.1.3, 13.1.4 ENR
	a) In general, only secure communication standards and protocols that include integrity protection, authentication and, if applicable, encryption shall be used if and where the technology allows. This is a non-negotiable requirement for any protocols used for remote administration and parameterization and shall also be taken into account where non-standard resp. proprietary protocols are used.
	b) It shall be possible to integrate the entire system and any associated network components into the overall company's network concept. Central administration for relevant network configuration parameters like IP addresses shall be possible. For administration and monitoring secure protocols that ensure integrity protection, authentication and encryption shall be used. Network components shall be hardened, unnecessary services and protocols deactivated and management interfaces protected via ACLs.
	c) Network components provided by the supplier shall be capable of integrating into a central inventory and patch management.
	d) Where the technology allows it, WAN connections shall use the IP protocol and unencrypted application protocols shall be secured by encryption on the lower network layers (e.g. via TLS encryption or encrypted VPN technology).
	e) Where network infrastructure components are shared (e.g. by the use of VLAN or MPLS technologies), the network with the highest protection requirement level shall indicate the respective hardware and parameterization requirements. The shared use of network components shall only be shared in case of different protection requirements when this shared use can in no way decrease the protection level or availability.

SICAM PAS, SICAM PQS, and SICAM SCC

a)	Standard protocols such as DNP3, IEC 61850 MMS and IEC 60870-5-104 are used for the transmission of process data. Transport layer security is implemented in SICAM PAS in accordance with IEC 62351 for the DNP3, IEC 61850 MMS and IEC 60870-5-104 protocols. No passwords are transmitted in clear text.
b)	SNMPv3 is used as a network protocol. Management interfaces are protected via ACL. The network components of SICAM PAS and SICAM PQS are hardened; unnecessary services and protocols are deactivated.
c)	The products of the SICAM software product line should be operated in a secure, autonomous process network and not in a corporate network.
d)	The following IP-based protocols are available for WAN communication in SICAM PAS: IEC 61850, IEC 60870-5-104, and DNP3i. VPN-based techniques can be used for encryption, or TLS encryption in accordance with IEC 62351 in the case of IEC 61850 MMS, IEC 60870-5-104 and DNP3i.
e)	The IEC 61850, IEC 60870-5-104, and DNP3i standard protocols use TCP. UDP is used for time synchronization in accordance with NTP.
f)	For examples of secure network configurations refer to the <i>Security manual</i> .



NOTE

Information for project planning/implementation:
Must be taken into consideration in system design.

4.4.2 Secure Network Structure

BDEW 4.4.2	ISO/IEC 27002:2013 / 27019:2017: 9.4.1, 12.9.1 ENR, 13.1.1, 13.1.2, 13.1.3, 13.1.4 ENR, 13.1.5 ENR
	a) Vertical network segmentation: Where applicable and technologically feasible, the system’s underlying network structure shall be divided into zones with different functions and protection requirements. Where the technology allows it, these network zones shall be separated by firewalls, filtering routers or gateways. Communications with other networks shall only occur via the communication protocols approved by the client and in compliance with the applicable security guidelines.
	b) Horizontal network segmentation: Where applicable and technically feasible, the system’s underlying network structure shall also be subdivided horizontally, into independent zones (e.g. according to sites) that are also separated by firewalls, filtering routers or gateways.



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 configuration examples and further information, refer to [/2/ Secure Substation Manual – System Hardening for Substation Automation and Protection](#).

4.4.3 Documentation of Network Structure and Configuration

BDEW 4.4.3	ISO/IEC 27002:2013 / 27019:2017: 8.1.1 The following shall be documented: network design and configuration; all physical, virtual and logical network connections and the employed protocols, IP addresses and ports; and any network perimeters that are part of the system or interact with it. Any changes, e.g. via updates, shall be included in the documentation as part of the overall change management. This documentation shall also cover information on normal and maximum expected data transmission rates, to allow for limiting data transmission rates on the network components to prioritize traffic and prevent DoS issues, where necessary.
-------------------	--

For more detailed information on firewall rules, refer to the *SICAM PAS/PQS security manual* and the *Secure Substation manual*. However, the data transmission rates to be expected depend on the individual configuration.



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.

4.4.4 Secure Remote Access

BDEW 4.4.4	ISO/IEC 27002:2013 / 27019:2017: 9.1.2, 9.4.1, 9.4.2	
	a)	It shall be possible to administrate, maintain and configure all components via an out-of-band network, e.g. via local access, a serial port, a network or direct control of the input devices (KVM).
	b)	Any remote access shall take place via centrally administrated access servers that are under control of the system operator. These access servers shall be operated within a DMZ and ensure isolation of the process network. Here, two factor authentications is mandatory.
	c)	Strictly no direct dial in access to terminal devices.
	d)	Any remote access shall be logged centrally; recurring failed attempts shall be reported.
	e)	All remote access options 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.

4.4.5 Wireless Technologies

BDEW 4.4.5	ISO/IEC 27002:2013 / 27019:2017: 10.1.1, 13.1.1, 13.1.2, 13.1.3	
	Short-range wireless technologies (e.g. Wi-Fi, Bluetooth, ZigBee, RFID etc.) shall only be used after assessment of the related risks, under consideration of the following minimum-security measures and after consultation with and approval by the client:	
	<ul style="list-style-type: none"> • Wireless transmission technology shall to be secured with state-of-the-art measures. • Wi-Fi technology shall only be operated in dedicated network segments that are separated by firewalls and application proxies. • Wi-Fi networks shall be configured in a way that ensures that existing Wi-Fi networks are not affected, disrupted or impaired. 	

Since SICAM software products are not equipped with wireless technologies, this requirement is not relevant.



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 (for example wireless modem).

4.5 Application

4.5.1 Role Concepts

BDEW 4.5.1	ISO/IEC 27002:2013 / 27019:2017: 6.1.2, 9.2.1, 9.2.3, 9.2.6, 9.4.1 The entire system shall support granular access control to data and resources. To this end, it shall support user concept that covers at least the following user roles: <ul style="list-style-type: none">• Administrator: User who installs, maintains and manages the system. Among others, this gives the administrator the right to change security and system configurations.• User: User who operates the system according to the intended usage scenario, including the right to change operationally relevant settings.• Read-only user: User permitted to access the system status and pre-defined operating data without the right to make any changes. The standard access rights shall reflect a secure system configuration. Only the administrator role shall be able to read and change security-related system settings and configuration values. Regular system use shall only require user or read-only user rights. It shall be possible to deactivate user accounts individually without having to remove them from the system.
-------------------	--

Users can be assigned 8 predefined roles in SICAM PAS, SICAM PQS, and SICAM PQ Analyzer:

- Administrator
- System engineer
- Data engineer
- Switch operator
- Guest
- Security administrator
- RBAC manager
- Security auditor

By assigning these roles, the system use by the individual users can be restricted depending on their responsibilities. For detailed instructions including recommendations, refer to the *SICAM PAS/PQS Security manual*. The corresponding roles are described in the manual *SICAM PAS/PQS Configuration and Operation*, chapter **User Administration**.

In addition, SICAM SCC allows the configuration of user-defined roles. The role concept of SIMATIC WinCC is applied for this purpose.

SICAM PQ Analyzer supports Role-Based access control (RBAC) to PQ archive. The rights are classified according to the user roles which provide access to perform various operations in the archive. For more details, refer to the *SICAM PQ Analyzer manual*.

4.5.2 User Authentication and Login

BDEW 4.5.2	ISO/IEC 27002:2013 / 27019:2017: 9.3.1, 9.4.2, 9.2.1, 9.2.2, 9.4.3, 12.4.1
	The application shall use personal users to identify and authenticate each individual user; group accounts require special permission by the client and shall only be used in narrowly defined exceptional cases.
	a) Without successful user authentication, the system shall only allow a range of narrowly defined actions.
	b) The system shall support a state-of-the-art password policy.
	c) Where technologically possible, strong two factor authentication shall be employed, e.g. via tokens or smart cards.
	d) Data required for user identification and authentication shall not be obtained exclusively from outside the process network.
e) Any successful or failed login attempts shall be centrally logged. It shall also be possible to centrally alarm in case of unsuccessful login attempts.	

SICAM software products, as well as the Windows operating systems used, support user management as described above. The customer is responsible for their implementation for daily operation.

SICAM software products have implemented a logging service for the recording of failed and successful logon attempts in a log. During the integration of the user management feature provided by the operating system, it is also possible to configure additional functions such as 2-factor authentication or organization-specific password policies.

4.5.3 Authorization of Actions at the User and System Levels

BDEW 4.5.3	ISO/IEC 27002:2013 / 27019:2017: 9.4.1, of.4.4
Certain security-related or safety-critical actions shall require prior authorization of the requesting user resp. the requesting system component. Such actions might also include a read-out of process data points or configuration parameters.	

Critical operations are protected against inadvertent user inputs through dialogs. Windows user rights are required.

4.5.4 Web Applications and Web Services

BDEW 4.5.4	ISO/IEC 27002:2013 / 27019:2017: 14.2.5
For web applications, web interfaces and web services, the recommendations of the OWASP TOP 10 and OWASP Application Security Verification Standard projects as well as the BSI Guideline on the Development of Secure Web Applications shall be applied.	
Any deviations from these guidelines require justification and prior approval by the client.	

The SICAM PAS web application is implemented by means of a layer model. Data processing is performed via the DAL service. The DAL service is installed by default with a specific user with no administrator rights. These rights can be modified. Inputs are validated using the DAL service.

For more detailed information on secure commissioning, refer to the manual.

The Web Navigator used by SICAM SCC is a SIMATIC WinCC product. For more detailed information, refer to the *SIMATIC WinCC Web Navigator* documentation.

4.5.5 Integrity Testing

BDEW 4.5.5	ISO/IEC 27002:2013 / 27019:2017: 14.2.5 The integrity of data processed as part of security-related activities shall be verified prior to processing (e.g. checked for plausibility, correct syntax and value range).
-------------------	---

SICAM PAS and SICAM PQS

The integrity of the application data is ensured by the integrated self-monitoring mechanisms on the operating system level.

At startup and at regular intervals, SICAM PAS/PQS product 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 to prevent hazards for or damage to equipment and persons.

Security-relevant activities (for example issuing of commands) in local operation can be secured by password and an integrated multi-stage principle (for example SICAM PAS Value Viewer, SICAM PAS/PQS UI – Operation). All the configuration data in SICAM PAS and SICAM PQS is checked for plausibility.

In addition, the SICAM setup software is digitally signed by an official code-signing certificate to support integrity checking.

4.5.6 Logging

BDEW 4.5.6	ISO/IEC 27002:2013 / 27019:2017: 12.4.1, 12.4.2, 12.4.3, 12.4.4, 18.1.3	
	a)	The entire system shall have a uniform system time as well as an option for synchronizing this system time with an external secure time source.
	b)	The system shall log user actions as well as security-related actions, events and errors in a format that is suitable for later and central processing. For a configurable minimum time period, these logs shall record date and time, the users and systems involved as well as the actual event and result.
	c)	Log files shall be stored centrally at a freely configurable location. A mechanism for the automated transfer of the log file to central components shall be available.
	d)	The log file shall be protected from subsequent modification.
	e)	Older entries shall be overwritten on the log file overflow. The system shall send an alert before the log storage runs out of space.
	f)	It shall be possible to include security-related log messages in a pre-existing alarm management.

a)	All SICAM software products support synchronization via an external radio clock such as an NTP server.
b)	SICAM software products can be configured to log user activities with a time stamp.
c)	The configuration of the logging, including the recommended setting, is described in the <i>Security manual</i> . For SICAM PQ Analyzer, configuration of syslog parameters is described in the <i>SICAM PQ Analyzer manual</i> .
d)	SICAM PAS/PQS and SICAM PQ Analyzer keep a separate event log for security relevant events. SICAM SCC logs security relevant events in its audit log database with the WinCC Audit option enabled.
e)	Transmission to a central syslog server is supported in SICAM PAS/PQS and PQ Analyzer. For configuration of syslog parameters, refer to the <i>SICAM PAS/PQS Configuration and Operation manual</i> .
f)	Possible using additional software
g)	The log file can only be deleted by the administrator and security auditor.
h)	A Windows circular buffer mechanism is used; there is no alarming.
i)	Using additional software by reading out the event log

4.6 Development

4.6.1 Secure Development Standards, Quality Management and Approval Processes

BDEW 4.6.1	ISO/IEC 27002:2013 / 27019:2017: 9.4.5, 14.2.2, 14.2.3, 14.2.4, 14.2.5, 14.2.6, 14.2.7, 14.2.8, 14.2.9, 14.3.1
	a) The system shall be developed by reliable and professionally trained employees. Where the development or parts thereof are subcontracted to a third party, this requires written permission by the client. The subcontractor shall meet at least the same security requirements as the supplier.
	b) The supplier shall develop the system in line with recognized development standards and quality management/assurance processes. As part of the development process, the following security-related development steps require special attention: <ul style="list-style-type: none"> • Definition of the security requirements • Threat modeling and risk analysis • Deduction of requirements for system design and implementation • Secure programming • Requirement testing • Security checks before commissioning
	c) Testing shall be subject to the dual control principle: Development and testing shall be carried out by different people. Testing plans and procedures as well as expected and actual test results shall to be documented and comprehensible. It shall be ensured that they can be reviewed by the client as needed.
	d) The supplier shall have a documented development security process in place that covers physical, organizational and personal security and protects the system's integrity and confidentiality. The effectiveness of the above-stated process may be verified by an external audit.
	e) The supplier shall have a programming guideline in place that explicitly covers security-related requirements, e.g. avoiding insecure programming techniques and functions or the verification of input data to avoid buffer overflow errors. Where possible, security-enhancing compiler options and libraries shall be used.
	f) The approval of the system resp. of updates/security patches needs to follow a specified and documented approval process.

The following table provides details on the secure development practices of SICAM software:

a)	SICAM software products are developed by trustworthy and trained employees. For example, the entire development team is thoroughly trained in secure coding .
b)	Siemens develops the products of the SICAM software product line 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. SICAM software is developed according to a process which is certified against IEC 62443-4-1 ML-4.
c)	The independence of testers is part of the IEC 62443-4-1 certification process. This is attested to the certified process of SICAM software by the external certification body. Tests and test results are essential parts of the software release.
d)	Siemens maintains a documented development security process for the products of the SICAM software product line 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. SICAM software is developed in a Siemens department which is certified against IES/IEC 27001.

e)	Siemens has set up a programming guideline for the products of the SICAM software product line 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.
f)	New releases for SICAM software products are made available using a specified and document release process. The categorization of security defects according to the Common Vulnerability Score (CVS) and severity are part of the defect-handling work instruction which defines the sort of release which is necessary (hot-fix, patch, or release). The sort of a release defines the process.

4.6.2 Secure Development, Test and Staging Systems, Integrity Testing

BDEW 4.6.2	ISO/IEC 27002:2013 / 27019:2017: 9.4.5, 12.1.4, 14.2.7, 14.3.1	
	a)	Development shall take place on secure systems; the development environment, source code and binary data all shall be protected from external access. All development systems shall be hardened according to recognized state-of-the-art and best practice specifications. Up-to-date malware protection shall be employed on the systems and all the latest security patches shall be installed.
	b)	Development and testing of the system, updates, extensions and security patches shall take place in a testing environment that is separated from the productive system.
	c)	No source code (except for interpreted scripting languages) shall be stored on productive systems.
	d)	It shall be possible to check the integrity of source code and binary data for unauthorized changes, for example via secure checksums.
	e)	A version history that tracks any changes to the software shall be kept for all employed software.

The following table provides details on the secure development practices of SICAM software:

a)	Product development for the SICAM software product line is conducted on secure systems. The development environment, the source code and binaries are protected against unauthorized access. The development computers are always kept up to date through the use of continuously updated antivirus scanners and central update mechanisms for operating system and application patches.
b)	Product development and testing of the SICAM software product line and updates, enhancements and security patches are conducted in a testing environment that is separated from the live system.
c)	The source code for the SICAM software product line is only available from Siemens. No source code is stored on live systems.
d)	The integrity of the parameter binaries of the SICAM software products can be checked for unauthorized changes on the target system using 3P tools.
e)	For the SICAM software products a version history for the entire software is maintained and allows all software changes to be traced.

4.7 Maintenance

4.7.1 Maintenance Process Requirements

BDEW 4.7.1	ISO/IEC 27002:2013 / 27019:2017: 9.1.2, 9.2.1, 9.2.2, 15.1.1, 15.1.2	
	a)	Any remote and on-site access shall only be carried out by a predefined and properly trained group of people and only originating from secured systems. Access systems and IT infrastructures used for remote and on-site access need to be hardened according to recognized state-of-the-art standards and best practice specifications. Up-to-date malware protection shall be employed and all the latest security patches shall be installed.
	b)	A pre-defined maintenance process shall be established to ensure that maintenance personnel only receives access to the systems, services and data as well as the respective physical premises that are actually required to carry out the related maintenance activities.
	c)	Interactive remote access shall occur via personalized accounts and using two factor authentication. Special user IDs shall be established for automated processes – these shall only be able to execute specific functions and not have interactive access.
d)	Technical measures shall ensure that remote access is only possible if and where the responsible operator has explicitly approved this access. Each remote access session by external service providers shall require individual approval and disconnection. Sessions shall automatically disconnect after a reasonable amount of time. Access systems used for remote access, in particular, shall be logically or physically isolated from other networks during remote access. Here, a physical separation is preferable to logical uncoupling.	



NOTE

Information for project planning/implementation and system service:
Product updates for the SICAM software product line are made available by Siemens.
However, the update of systems must be defined for the individual system and governed by contract because maintenance is not performed by the contractor.

4.7.2 Secure Update Processes

BDEW 4.7.2	ISO/IEC 27002:2013 / 27019:2017: 12.5.1, 14.2.2, 14.2.3, 14.2.7, 14.2.9	
	The provision and installation of updates, extensions and patches needs to occur according to a defined process and in coordination with the client.	



NOTE

Information for project planning/implementation and system service:
Product updates for the SICAM software product line are made available by Siemens.
Systems updates must be defined depending on the individual system and governed by contract.

4.7.3 Configuration and Change Management, Rollback

BDEW 4.7.3	ISO/IEC 27002:2013 / 27019:2017: 12.1.2, 12.5.1, 12.6.2, 12.9.1 ENR, 14.2.2, 14.2.9	
	a)	The system shall be developed and operated with a configuration and change management in place.
b)	The system shall support rollback to a pre-defined number of configuration states.	

SICAM software products are developed based on a configuration and change management process.



NOTE

Information for project planning/implementation and system service:
Regular backups created within the scope of project planning/implementation and product/system service enable convenient rollback to older parameter versions.
This requirement is not relevant to the products and must be taken into consideration during project planning/implementation and system service.

4.7.4 Handling of Vulnerabilities

BDEW 4.7.4	ISO/IEC 27002:2013 / 27019:2017: 12.6.1, 16.1.2, 16.1.3 The supplier shall have a documented vulnerability handling process in place. Within this process, all concerned – including external parties – shall be able to report actual or potential vulnerabilities. In addition, the supplier shall stay up-to-date on current security issues that might affect the system or individual components. The vulnerability handling process defines how and in what timeframe a known or reported vulnerability shall be reviewed, classified, remedied and reported to all affected clients, including respective recommended measures. When the supplier finds out about a vulnerability, he shall inform the client in a timely manner and under consideration of the necessary confidentially restrictions, even when no patch to fix the issue is available yet.
-------------------	---

For its SICAM software products, 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 the SICAM software product line.
For the SICAM software products, up-to-date information on security problems is available even if a patch for the elimination of the problem has not yet become available.

4.8 Data Back-Up and Emergency Planning

4.8.1 Back-up: Concept, Method, Documentation, Testing

BDEW 4.8.1	ISO/IEC 27002:2013 / 27019:2017: 12.1.1, 12.3.1 Documented and tested procedures for data back-up and recovery of the individual components resp. the entire system and the respective configurations shall exist. There shall be the possibility for central back-up of the configuration parameters of distributed components. After relevant system updates, the documentation and procedures shall be updated and retested accordingly.
-------------------	---

For SICAM software products procedures are available for the backup and recovery of the individual applications, the entire system and the corresponding configuration. These procedures are documented in the respective manuals.
SICAM PAS and SICAM PQS provide various data backup procedures: Conventional Windows backup programs can be used in order to back up entire data carriers or partitions.
An additional option is to export configuration data from the SICAM software databases, and back them up accordingly. All these options are described in the respective manuals.



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.

4.8.2 Emergency Concept and Recovery Plans

BDEW 4.8.2	ISO/IEC 27002:2013 / 27019:2017: 17.1.1, 17.2.1 The supplier shall provide documented and tested procedures and recovery plans – including expected restoration times – for relevant emergency and crisis scenarios. After relevant system updates, this documentation and these procedures shall be updated and retested as part of the approval process for release changes.
-----------------------------	--

The manuals of the SICAM software product line include descriptions on how to back up system files, applications, and files and restore them in an emergency case. The plant operator can use these descriptions as a basis for creating emergency plans.



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.

5 IEC 62443-4-2 Security Requirements

Legend:



n.a.



exception



comply



partial



exceed

CR	Component requirement which is common to all types of components
SAR	Software application requirement
EDR	Embedded device requirement
HDR	Host device requirement
NDR	Network device requirement

5.1	SICAM PAS/PQS	31
5.2	SICAM SCC	37

5.1 SICAM PAS/PQS

5.1.1 FR1

5.1.1.1 Identification and Authentication Control

			Security Level				Comment
			1	2	3	4	
CR 1.1		Human user identification and authentication					SICAM PAS/PQ supports user-based authentication with Role-Based Access Control (RBAC) authorization. Authentication is supported. RBAC is not supported for the UI-OperationClient application
	RE (1)	Unique identification and authentication					User management is supported by the local user management or by the central user management.
	RE (2)	Multifactor authentication for all interfaces					Implemented through an operating system that requires to log on to the system running SICAM PAS using a smartcard.
CR 1.2		Software process and device identification and authentication					TLS-based authentication support for DNP Master/Slave, 104 Master/Slave, IEC-61850 Client/Server protocols MMS authentication support for IEC-61850 Client/Server The user-administration application has local and central user management in place. UI Configuration, UI Operate, Valueviewer, PASFeature Enabler, and VersionScan applications use binaries that are digitally signed. These signatures can be incorporated into the Windows application whitelisting solution.
	RE (1)	Unique identification and authentication					TLS-based authentication support for DNP Master/Slave, 104 Master/Slave, IEC-61850 Client/Server protocols UI Configuration, UI Operate, Valueviewer, PASFeature Enabler, and VersionScan applications use binaries that are digitally signed. These signatures can be incorporated into the Windows application whitelisting solution.
CR 1.3		Account management					SICAM PAS/PQ supports local and centrally managed user accounts.
CR 1.4		Identifier management					SICAM PAS/PQ supports user ID management locally and centrally.
CR 1.5		Authenticator management					Supported by Windows active directory for centrally managed users accounts
	RE (1)	Hardware security for authenticators					Supported by Windows active directory for centrally managed users accounts
NDR 1.6		Wireless access management					Not applicable
	RE (1)	Unique identification and authentication					Not applicable
CR 1.7		Strength of password-based authentication					Supported by Windows active directory for centrally managed users accounts

			Security Level				Comment
			1	2	3	4	
	RE (1)	Password generation and lifetime restrictions for human users					Supported by Windows active directory for centrally managed users accounts
	RE (2)	Password lifetime restrictions for all users (human, software process, or device)					Supported by Windows active directory for centrally managed users accounts
CR 1.8		Public key infrastructure certificates					TLS support for DNP Master/Slave, 104 Master/Slave, IEC 61850 client/server protocols relies on PKI certificates.
CR 1.9		Strength of public key-based authentication					TLS support for DNP Master/Slave, 104 Master/Slave, IEC 61850 client/server includes the required certificate validation checks.
	RE (1)	Hardware security for public key-based authentication					Supported for centrally managed users accounts
CR 1.10		Authenticator feedback					The password is hidden when entering. A wrong credentials input leads to a general message that the password or user name is possibly wrong.
CR 1.11		Unsuccessful login attempts					Supported by Windows active directory for centrally managed users accounts
CR 1.12		System use notification					Not applicable
CR 1.13 NDR 1.13		Access via untrusted networks					Not applicable
	RE (1)	Explicit access request approval					Not applicable
CR 1.14		Strength of symmetric key-based authentication					Not applicable
	RE (1)	Hardware security for symmetric key-based authentication					Not applicable

5.1.2 FR2

5.1.2.1 Use Control

			Security Level				Comment
			1	2	3	4	
CR 2.1		Authorization enforcement					RBAC is supported
	RE (1)	Authorization enforcement for all users (humans, software processes, and devices)					Only implemented for users, not for software processes and devices
	RE (2)	Permission mapping to roles					Fixed role for permission assignment implemented
	RE (3)	Supervisor override					Not implemented
	RE (4)	Dual approval					Not implemented

			Security Level				Comment
			1	2	3	4	
CR 2.2		Wireless use control	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable
CR 2.3		Use control for portable and mobile devices	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable
CR 2.4 SAR 2.4 EDR 2.4 HDR 2.4 NDR 2.4		Mobile code	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable
	RE (1)	Mobile code authenticity check	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Not applicable
CR 2.5		Session lock	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	After the passage of configured amount of time, the user will be signed off.
CR 2.6		Remote session termination	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The user can terminate the UI OperationClient session in the Web browser. The controlling station can terminate the process communication session over IEC 104, DNP3i, and IEC 61850 MMS.
CR 2.7		Concurrent session control	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The number of concurrent sessions can be configured in the Windows IIS settings.
CR 2.8		Auditable events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Implemented for syslog and MS event viewer
CR 2.9		Audit storage capacity	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Centralized logging via syslog
	RE (1)	Warn when audit record storage capacity threshold reached	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable Windows application; capacity threshold does not apply
CR 2.10		Response to audit processing failures	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Windows event logs support the setting of an appropriate response to audit processing failures.
CR 2.11		Timestamps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Implemented according to the syslog format (RFC 5424)
	RE (1)	Time synchronization	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Components have the ability to create a time stamp that is synchronized with the system-wide time source (NTP server).
	RE (2)	Protection of time source integrity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Secure NTP supports a time-source integrity. Detected alterations are not logged.
CR 2.12		Non-repudiation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Critical actions are logged with the userID.
	RE (1)	Non-repudiation for all users	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Logging for critical actions: <ul style="list-style-type: none"> • For all human users • If RBAC is activated • for IEC 61850 MMS clients, IEC 104/DNP3i Master, if secure communication is activated
EDR 2.13 HDR 2.13 NDR 2.13		Use of physical diagnostic and test interfaces	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable
	RE (1)	Active monitoring	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Not applicable

5.1.3 FR3

5.1.3.1 System Integrity

			Security Level				Comment
			1	2	3	4	
CR 3.1		Communication integrity					TLS support for DNP Master/Slave, 104 Master/Slave, IEC 61850 client/server protocols including communication integrity check
	RE (1)	Communication authentication					TLS support for DNP Master/Slave, 104 Master/Slave, IEC 61850 client/server protocols including communication authentication check
CR 3.2 SAR 3.2 DER 3.2		Protection from malicious code					The setup of SICAM PAS/PQ is signed with an official certificate. The compatibility with a dedicated virus scanner is tested and documented.
HDR 3.2		Protection from malicious code					Not applicable
	RE (1)	Report version of code protection					Not applicable
CR 3.3		Security functionality verification					Siemens offers a freely available security substation manual for a tested and recommended secure configuration. Siemens tests all products with the latest MS updates and publishes the result.
	RE (1)	Security functionality verification during normal operation					Supports logging capability and response to the intended operation
CR 3.4		Software and information integrity					SICAM PAS/PQ binaries are digitally signed.
	RE (1)	Authenticity of software and information					The digital signature of SICAM PAS/PQS binaries enables the application to be whitelisted.
	RE (2)	Automated notification of integrity violations					Not applicable It is a whitelisting topic.
CR 3.5		Input validation					Input validation is in place.
CR 3.6		Deterministic output					Not applicable
CR 3.7		Error handling					Error messages are written to syslog and the Windows event viewer without disclosing the exploitable information.
CR 3.8		Session integrity					TLS support for DNP Master/Slave, 104 Master/Slave, IEC 61850 client/server protocols, and the UI OperationClient includes a session integrity check.
CR 3.9		Protection of audit information					Supported by Windows as logs are written to the event viewer where access control can be enforced. Audit information is also sent to a centralized logging server via syslog.
	RE (1)	Audit records on write-once media					Not implemented in SICAM software but could be implemented with 3rd party tools on operating system level
CR 3.10 EDR 3.10 HDR 3.10 NDR 3.10		Support for updates					SICAM PAS/PQ supports a redundancy feature through which switch over can be made to the redundant partner The current embedded device (station unit) can be patched without any availability issues.

			Security Level				Comment
			1	2	3	4	
	RE (1)	Update authenticity and integrity					During installation of the software update for the setup procedure
CR 3.11 EDR 3.11 HDR 3.11 NDR 3.11		Physical tamper resistance and detection					Not applicable
	RE (1)	Notification of a tampering attempt					Not applicable
CR 3.12 EDR 3.12 HDR 3.12 NDR 3.12		Provisioning product supplier roots of trust					Not applicable
CR 3.13 EDR 3.13 HDR 3.13 NDR 3.13		Provisioning asset owner roots of trust					Not applicable
CR 3.14s EDR 3.14 HDR 3.14 NDR 3.14		Integrity of the boot process					Not applicable
	RE (1)	Authenticity of the boot process					Not applicable

5.1.4 FR4

5.1.4.1 Data Confidentiality

			Security Level				Comment
			1	2	3	4	
CR 4.1		Information confidentiality					Data in rest are protected via database credentials. TLS support for DNP Master/Slave, 104 Master/Slave, IEC 61850 client/server protocols includes information confidentiality for data in transit.
CR 4.2		Information persistence					In SICAM PAS/PQ, if any data is deleted, it will be deleted permanently from the non-volatile storage. SICAM PAS/PQ supports a feature [File-> New Database] to restore the database to the deployment state in which case all data configured by the user will be erased.
	RE (1)	Erase of shared memory resources					Supported
	RE (2)	Erase verification					If SICAM PAS/PQS is uninstalled, it deletes any and all information that is protected by authorization. Verification can be performed at the windows level.
CR 4.3		Use of cryptography					SICAM PAS/PQ supports TLS 1.2 (default), TLS1.1, AES-256, RSA, EDH, and ECC.

5.1.5 FR5

5.1.5.1 Restricted Data Flow

			Security Level				Comment
			1	2	3	4	
CR 5.1		Network segmentation					SICAM PAS/PQ runs in routable networks over DMZ because of dedicated ports and firewall-friendly protocols.
CR 5.2 NDR 5.2		Zone boundary protection					Not applicable
	RE (1)	Deny all, permit by exception					Not applicable
	RE (2)	Island mode					Not applicable
	RE (3)	Fail close					Not applicable
CR 5.3 NDR 5.3		General-purpose person-to-person communication restrictions					Not applicable
CR 5.4		Application partitioning					Not applicable

5.1.6 FR6

5.1.6.1 Timely Response to Events

			Security Level				Comment
			1	2	3	4	
CR 6.1		Audit log accessibility					MS event viewer or syslog (unstructured messages for human readable)
	RE (1)	Programmatic access to audit logs					SIEM systems can analyze the standardized syslog messages.
CR 6.2		Continuous monitoring					The SICAM PAS/PQ application can be monitored by 3rd party products.

5.1.7 FR7

5.1.7.1 Resource Availability

			Security Level				Comment
			1	2	3	4	
CR 7.1		Denial of service protection					Communication stacks are proofed against DoS during test. Operating system must be hardened according to hardening rules.
	RE (1)	Manage communication load from component					Redundancy mode is possible.
CR 7.2		Resource management					SICAM PAS/PQ supports a feature (watch dog) to protect against resource exhaustion.
CR 7.3		Control system backup					SICAM PAS/PQ supports a feature (Archive) to back up the complete configuration.
	RE (1)	Backup integrity verification					In SICAM PAS/PQ, backup integrity verification is performed using the database vendor tool.

			Security Level				Comment
			1	2	3	4	
CR 7.4		Control system recovery and reconstitution					SICAM PAS/PQ supports a feature (Dearchive) to recover and reconstitute to a known secure state.
CR 7.5		Emergency power					Not applicable
CR 7.6		Network and security configuration settings					Siemens offers a freely-available secure substation manual for a network and security setup.
	RE (1)	Machine-readable reporting of current security settings					Data are stored in a SQL database to get information about the settings.
CR 7.7		Least functionality					All needed communication ports and services are documented.
CR 7.8		Control system component inventory					All components are versioned and signed.

5.2 SICAM SCC

5.2.1 FR1

5.2.1.1 Identification and Authentication Control

			Security Level				Comment
			1	2	3	4	
CR 1.1		Human user identification and authentication					SICAM SCC allows access to only authorized users. Segregation of duties and least privilege access is attained by creating specific user groups and adding users to it via the User Administrator section in the SIMATIC WinCC Configuration Studio. Additionally, SICAM SCC supports integration with the Windows Active Directory Domain Controller through the SIMATIC logon (additional license required) to identify and authenticate authorized users.
	RE (1)	Unique identification and authentication					All users are identified uniquely. Unique IDs are used to authenticate the users. Role-based access to user groups and users is also supported. By default, 2 user groups are created as Administrator and Operator . Users can also be assigned additional/individual rights based on operational requirements.
	RE (2)	Multifactor authentication for all interfaces					SICAM SCC runs with a Microsoft Windows PC. Multifactor authentication is allowed either through the Windows native user-account management or through an active directory domain controller. Using the PM Logon addon, customers can additionally enable a 2-factor authentication for the user logon.

			Security Level				Comment
			1	2	3	4	
CR 1.2		Software process and device identification and authentication					SICAM SCC establishes the communication with SICAM PAS/PQS, SICAM Network Manager, the SICAM RTUs, IEC 61850 devices, and IEC 60870-5-104 devices. The identification of SICAM PAS is done through a compatibility key generated dynamically during the integration process in SICAM PAS. During runtime, it checks whether the compatibility keys of the SICAM SCC and the SICAM PAS project are identical. SICAM RTUs, IEC 61850, and IEC 60870-5-104 devices, the device name and the IP address are used for identification in the XML configuration file. Security for IEC 61850, IEC 60870-5-104, and other IP-based protocols can be achieved with VPN for systems connected from outside the trusted network in which SICAM SCC is deployed. Security can be achieved with a Virtual Private Network (VPN) between the systems. Network devices use SNMPv3 for identification and authentication.
	RE (1)	Unique identification and authentication					SICAM SCC communicates over TCP protocol and identifies all components uniquely through the device name and IP addresses.
CR 1.3		Account management					SICAM SCC uses SIMATIC WinCC for user management. The account management includes the creation of user groups, assigning users to the group, and assigning individual rights to the user. By default, the operator and administrator groups are created and can be edited for changing authorization levels.
CR 1.4		Identifier management					User accounts created in the SICAM SCC support mapping of user authorizations based on roles. The roles are identified using IDs under authorization levels.
CR 1.5		Authenticator management					SICAM SCC with a SIMATIC WinCC user administrator manages user groups and user authorizations. When the user calls a function, the user administrator checks whether the user has been assigned the required rights. If not, the access to the function is prevented. The authorizations are updated when there is a change in the user group or a revocation of individual authorizations.
	RE (1)	Hardware security for authenticators					In case of a 2-factor authentication with PM logon, the user password is protected on the smartcard chip.
NDR 1.6		Wireless access management					Not applicable
	RE (1)	Unique identification and authentication					Not applicable
CR 1.7		Strength of password-based authentication					User access in SICAM SCC requires a password with a length between 6 and 24 unicode characters. Standard security guidelines shall be adhered for secure passwords. Further, password strength is also displayed in the password creation pop-up window.

			Security Level				Comment
			1	2	3	4	
	RE (1)	Password generation and lifetime restrictions for human users					SICAM SCC allows Windows user-account management to be used for user management. Password policies such as complexities, password life, password reuse restriction, and a password expiry notice can be configured in Windows using the SIMATIC logon.
	RE (2)	Password lifetime restrictions for all users (human, software process, or device)					This is supported with an active-directory integration. All password policies are enforced with an active directory for the domain accounts.
CR 1.8		Public key infrastructure certificates					For MMS security (IEC 62351-4), X.509 certificates are used.
CR 1.9		Strength of public key-based authentication					All security ciphers that are considered strong algorithms are used, as well as sufficiently long hashes and keys.
	RE (1)	Hardware security for public key-based authentication					Currently, SICAM SCC uses the software-based Microsoft certificate store to store keys and certificates.
CR 1.10		Authenticator feedback					The user administrator ensures that the authenticator feedback for passwords is obscured. Also the feedback on an unsuccessful login is secured against disclosing sensitive information.
CR 1.11		Unsuccessful login attempts					The SIMATIC logon for WinCC allows the configuration of the Account lockout threshold policy in the Windows operating system to limit unsuccessful login attempts.
CR 1.12		System use notification					The system use notification can be configured with the Windows Legal notice caption function.
CR 1.13 NDR 1.13		Access via untrusted networks					Sessions traversing the trusted zones are secured with the required security mechanisms such as VPN for remote access. Additional security controls are recommended such as firewall, IDS, and IPS.
	RE (1)	Explicit access request approval					Access via an untrusted network is not provided directly and is only available through a service PC or a terminal server in substations. Siemens cRSP is a secure remote-access solution which terminates, authenticates, and authorizes sessions in the substation DMZ.
CR 1.14		Strength of symmetric key-based authentication					Currently SICAM SCC supports symmetric key encryption only in case of a SNMPv3 communication with SNMP agents (for example IEDs, switches).
	RE (1)	Hardware security for symmetric key-based authentication					Symmetric key-based authentication is not supported by SICAM SCC.

5.2.2 FR2

5.2.2.1 Use Control

			Security Level				Comment
			1	2	3	4	
CR 2.1		Authorization enforcement	■	■	■	■	User authorization in SICAM SCC is provided through the WinCC user administrator. The authorizations are mapped to user groups or individual users. If a registered user calls up a function, the user administrator checks whether the user has been assigned the required user rights. Additionally, the SIMATIC logon can also be used for advanced user management and authorization (separate license required).
	RE (1)	Authorization enforcement for all users (humans, software processes, and devices)		■	■	■	User authorization is achieved with the WinCC user administrator in SICAM SCC. Authorization for software to software communication for SICAM PAS is achieved with a compatibility key generated dynamically during integration with SICAM SCC. For SICAM RTUs, IEC 61850, and IEC 60870-5-104 devices authorization is not supported by the protocols. VPN can be used for SICAM RTUs and IEC 61850 devices. Additional encrypted communication in accordance with IEC 62351 is possible for IEC 60870-5-104. For network devices, SNMPv3 is being used for Identification, authentication, and authorization.
	RE (2)	Permission mapping to roles		■	■	■	SICAM SCC supports Role-Based Access (RBAC) through the WinCC user administrator. Authorizations are mapped to rights for user groups or individual users.
	RE (3)	Supervisor override			■	■	Execution of critical operations can be protected with the electronic signature of a user through the WinCC/ Audit option. Dual approval can be configured to confirm the operation with an electronic signature before the action is executed.
	RE (4)	Dual approval				■	Execution of critical operations can be protected with the electronic signature of a user through the WinCC/ Audit option. Dual approval can be configured to confirm the operation with their electronic signature before the action is executed.
CR 2.2		Wireless use control	■	■	■	■	Not applicable
CR 2.3		Use control for portable and mobile devices					Not applicable
CR 2.4 SAR 2.4 EDR 2.4 HDR 2.4 NDR 2.4		Mobile code	■	■	■	■	Not applicable
	RE (1)	Mobile code authenticity check		■	■	■	Not applicable
CR 2.5		Session lock	■	■	■	■	An auto-session logout can be configured for users via the user administrator in SICAM SCC. Additionally, the SIMATIC logon can be used with the active directory domain controller for additional security.

			Security Level				Comment
			1	2	3	4	
CR 2.6		Remote session termination					A remote session shall only be allowed via the service PC or the terminal server in a demilitarized zone. Secure VPN shall be used to allow remote access to the service PC. The session shall have an expiry time and a multifactor authentication (additional components required to implement).
CR 2.7		Concurrent session control					A concurrent user can be limited by restricting client computers(WinCC project).
CR 2.8		Auditable events					Process-critical events are logged in SICAM SCC with WinCC such as commands, user access, errors, alarms, and incidents. Security event logging is configured using WinCC/Audit in Windows. Time stamp is supported with the NTP Daemon running in the background in Windows, automatically installed during the SICAM SCC installation.
CR 2.9		Audit storage capacity					In SICAM SCC, the Windows circular buffer is used for storage in the database, which ensures continued availability of storage space for audit logs.
	RE (1)	Warn when audit record storage capacity threshold reached					The Windows circular buffer mechanism is used for storage. Thus, an alarm is not generated.
CR 2.10		Response to audit processing failures					SICAM ensures continuity of service as events of audit procedures anticipated and addressed during the application development phase itself – with use of the Windows circular buffer for storage, redundant SICAM SCC systems or with WinCC/Audit.
CR 2.11		Timestamps					SICAM SCC is a Human Machine Interface component (HMI) and a correct time stamp for all components and it is very important. A radio clock shall be used as timer distributed through the network. Time stamps are used for all process alarms and user-access logs.
	RE (1)	Time synchronization					SICAM SCC time synchronization is based on the Network Time Protocol Daemon (NTPD) software. The NTPD services are automatically installed together with SICAM SCC. They run in the background in the Windows operating system. A precision of approximately 0.1 ms is achieved in the Windows operating system.
	RE (2)	Protection of time source integrity					Addressed at the substation solution level
CR 2.12		Non-repudiation					SICAM SCC logs all user actions for audit trails. Additionally, security can be enhanced using electronic signatures with WinCC/Audit for critical actions.
	RE (1)	Non-repudiation for all users					User authentication and authorization can be enforced for engineering and operations on the SICAM SCC PC. Logging of security-relevant actions in the system is realized both at the OS level (Windows security event log) as well as at the application and component level. Process-related actions like state changes can be logged and centrally collected.

			Security Level				Comment
			1	2	3	4	
EDR 2.13 HDR 2.13 NDR 2.13		Use of physical diagnostic and test interfaces		■	■	■	Not applicable
	RE (1)	Active monitoring			■	■	Not applicable

5.2.3 FR3

5.2.3.1 System Integrity

			Security Level				Comment
			1	2	3	4	
CR 3.1		Communication integrity	■	■	■	■	SICAM SCC established communication with SICAM PAS, SICAM RTUs, IEC 61850 devices, IEC 60870-5-104 devices, and the SICAM Network Manager (NWM). The SICAM NWM and the network devices are protected via SNMPv3. Secure VPN connection can be used to ensure the process communication security.
	RE (1)	Communication authentication		■	■	■	MMS security (IEC 62351-4) is based on X.509 certificate-based mutual authentication.
CR 3.2 SAR 3.2 DER 3.2		Protection from malicious code	■	■	■	■	SICAM SCC is a software application that runs on a Windows operating system. A malicious code-protection mechanism is a system-level requirement addressed through the application whitelisting, endpoint protection, and network-zone protection using firewalls.
HDR 3.2		Protection from malicious code	■	■	■	■	Not applicable
	RE (1)	Report version of code protection		■	■	■	Not applicable
CR 3.3		Security functionality verification	■	■	■	■	The security functionality verification requirement relates to an overall functionality of security measures. The logging mechanism supported by SICAM SCC, WinCC/Audit, and the SIMATIC logon enables the verification of security events.
	RE (1)	Security functionality verification during normal operation				■	Not applicable
CR 3.4		Software and information integrity	■	■	■	■	All installation files for SICAM SCC are digitally signed using SHA256 by Siemens. The integrity is ensured by verifying the certificates. The integrity of configuration files can be ensured with cryptographic hashes using an additional software. The database of SICAM SCC shuts down in case of an inconsistency error.
	RE (1)	Authenticity of software and information		■	■	■	All installation files for SICAM SCC are digitally signed using SHA256 by Siemens. The integrity is ensured by verifying the certificates. Recording and reporting of verification failures are conducted by the Windows operating system.
	RE (2)	Automated notification of integrity violations			■	■	Not in the scope of the secure substation blueprint

			Security Level				Comment
			1	2	3	4	
CR 3.5		Input validation					Siemens uses the secure coding guidelines for the development of SICAM products which explicitly addresses security-relevant requirements. For example, insecure programming methods and functions are avoided. Data input is verified, for example to prevent buffer-overflow errors. If possible, security-enhancing compiler options and libraries are used.
CR 3.6		Deterministic output					SICAM SCC is a Human Machine Interface (HMI). Siemens provides product-functionality documents. The interaction of SICAM SCC is performed through the tags. The output in the HMI depends upon the configuration of these tags. A detailed process-operation chart shall be prepared at the substation for expected behaviors of the tags.
CR 3.7		Error handling					Siemens uses the secure coding guidelines for development of SICAM products which explicitly addresses security-relevant requirements, for example error handling.
CR 3.8		Session integrity					Communication via untrusted interfaces can be using Windows-inbuilt VPN technologies with state-of-the-art security implementation that ensures integrity as well as correct and secure session ID handling.
CR 3.9		Protection of audit information					All log information is protected from unauthorized modification. Only administrators or users with explicit authorization levels can delete or modify log data. User-access events configured with additional tools such as the SIMATIC logon and WinCC/Audit provide additional protection using electronic signatures and dual approvals.
	RE (1)	Audit records on write-once media					Not implemented in SICAM software but could be implemented with 3rd party tools on operating system level.
CR 3.10 EDR 3.10 HDR 3.10 NDR 3.10		Support for updates					Not applicable
	RE (1)	Update authenticity and integrity					Not applicable
CR 3.11 EDR 3.11 HDR 3.11 NDR 3.11		Physical tamper resistance and detection					Not applicable
	RE (1)	Notification of a tampering attempt					Not applicable
CR 3.12 EDR 3.12 HDR 3.12 NDR 3.12		Provisioning product supplier roots of trust					Not applicable
CR 3.13 EDR 3.13 HDR 3.13 NDR 3.13		Provisioning asset owner roots of trust					Not applicable

			Security Level				Comment
			1	2	3	4	
CR 3.14 EDR 3.14 HDR 3.14 NDR 3.14		Integrity of the boot process					Not applicable
	RE (1)	Authenticity of the boot process					Not applicable

5.2.4 FR4

5.2.4.1 Data Confidentiality

			Security Level				Comment
			1	2	3	4	
CR 4.1		Information confidentiality					Confidentiality of information is ensured with role-based access using the user administrator in WinCC and the SIMATIC logon. Information such as backup and audit logs can be secured through user-authorization permissions. Information traveling outside the trusted zone shall be protected with additional measures using VPN, zone-boundary protection devices such as firewalls, IDS, and IPS.
CR 4.2		Information persistence					The requirement pertains to a safe disposal policy of the organization. As a capability the database file can be erased from the project folder of any SICASM SCC project by privileged users.
	RE (1)	Erase of shared memory resources					Confidential data like credentials are not stored in plain text via shared-memory resources.
	RE (2)	Erase verification					User actions are logged in WinCC. The audit trail can verify the erasure of information. Additional security is ensured using WinCC/Audit with electronic signature and dual approval for critical execution by the user. Non-repudiation is ensured through audit trails.
CR 4.3		Use of cryptography					Siemens recommends the use of internationally recommended cryptographic standards such as SHA256 for digital signatures and AES for encryption in SICAM NWM. The use of secure cryptographic standards in additional tools such as VPN, and TLS shall be used where ever required.

5.2.5 FR5

5.2.5.1 Restricted Data Flow

			Security Level				Comment
			1	2	3	4	
CR 5.1		Network segmentation					Connection to IEC60870-5-104 and IEC61850 devices can be set to a dedicated connection or identified by Windows routing algorithm automatically. SICAM SCC can be configured to work with different subnetworks for different services.
CR 5.2 NDR 5.2		Zone boundary protection					Not applicable

			Security Level				Comment
			1	2	3	4	
	RE (1)	Deny all, permit by exception					Not applicable
	RE (2)	Island mode					Not applicable
	RE (3)	Fail close					Not applicable
CR 5.3 NDR 5.3		General-purpose person-to-person communication restrictions					Not applicable
CR 5.4		Application partitioning					Not applicable

5.2.6 FR6






















5.2.6.1 Timely Response to Events








			Security Level				Comment
			1	2	3	4	
CR 6.1		Audit log accessibility					Access control in SICAM SCC can be used to restrict access to logs. Only an administrator can modify the audit logs. Additional security measures such as electronic signatures and dual approval with WinCC/Audit are advised to be deployed.
	RE (1)	Programmatic access to audit logs					SICAM SCC supports logging of security-relevant events with the WinCC/Audit option. This feature also logs the events in the Windows Event Viewer, from where the logs can be configured to be automatically forwarded to central logging servers.
CR 6.2		Continuous monitoring					Continuous monitoring can be achieved with system-wide security solutions such as a SIEM.

5.2.7 FR7

5.2.7.1 Resource Availability

			Security Level				Comment
			1	2	3	4	
CR 7.1		Denial of service protection					Protection against DoS requires additional components and a security design strategy. The concept of defence-in-depth shall be applied in consonance with the Secure Substations security guidelines: https://www.siemens.com/gridsecurity
	RE (1)	Manage communication load from component					Communication load in a substation shall be managed via network-level security devices such as the NextGen firewall, the Intrusion Detection System (IDS), and the Intrusion Prevention System (IPS). Additionally, host-based firewalls for the Windows system shall be enabled to secure the application.

			Security Level				Comment
			1	2	3	4	
CR 7.2		Resource management					SICAM SCC is based on a Windows operating system. The Windows native task manager shall be used to monitor resources of the host system. Additionally, to have broader access to the system wide resource +K31nagement third-party components shall be used in the substation.
CR 7.3		Control system backup					3 types of backups are required for SICAM SCC based on the data type: application, configuration, and real-time. An application backup needs a full image backup and is backed up via the operating system. The configuration backup for SICAM SCC is achieved with the SIMATIC WinCC Explorer. The real-time process data can be backed up with the SICAM SCC message archives.
	RE (1)	Backup integrity verification					The integrity of the image is based on the Windows in-built mechanisms. Additional measures such as digital signatures and hash calculations can be used for enhanced security of the configuration file backup and the runtime backups (third-party software is required).
CR 7.4		Control system recovery and reconstitution					SICAM SCC is based on SIMATIC WinCC. Product procedures are available for the backup and recovery of the individual applications, the entire system and the corresponding configuration. These procedures are documented in the SIMATIC WinCC manual.
CR 7.5		Emergency power					Not applicable
CR 7.6		Network and security configuration settings					Siemens adheres to secure substation control and management. Defense in depth requirements is supported by all Siemens devices and applications. The security configurations for Windows-based applications can be accessed via the Windows mechanisms.
	RE (1)	Machine-readable reporting of current security settings					The SIMATIC security controller can show and export settings which are set by the SIMATIC WinCC setup (user groups, registry, firewall, DCOM, file system). SICAM SCC is based on the Windows operating system. The security policies on Windows can be exported using "secpol.msc" in Windows.

			Security Level				Comment
			1	2	3	4	
CR 7.7		Least functionality					Siemens ensures continued availability of SICAM applications using secure design guidelines (refer to E50414-U0000-U001-05-76A1), defense-in-depth strategy and redundant SICAM SCC servers. In case of a failure of SICAM SCC, critical energy-automation functionalities such as protection continue to be provided by IEDs in the field level.
CR 7.8		Control system component inventory					With the SIMATIC Assessment Suite – Data Collector (SAS-DC) you can simply and easily collect diagnostics and system information from computers or other devices. iSDM, a Siemens solution for automated auditing of the substation components, can be used to collect asset management-related data through protocols like SNMP and IEC 61850. iSDM can generate reports, reduce documentation time and efforts on information gathering, and facilitate evaluation of patch management procedures.

Literature

- /1/ BDEW: Whitepaper – Anforderungen an sichere Steuerungs- und Telekommunikationssysteme (Requirements for Secure Control and Telecommunication Systems)
Version 2.0
- /2/ Secure Substation Manual – System Hardening for Substation Automation and Protection
V1.41
- /3/ SICAM PAS/PQS Security
V8.20

Glossary

AAA Server

An AAA Server (**A**uthentication, **A**uthorization and **A**ccounting) 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.

BDEW

Bundesverband **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.

CIP

Critical Infrastructure **P**rotection

CRC

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

CRL

Certificate **R**evocation **L**ist

cRSP

Common **R**emote **S**ervice **P**latform

DMZ

De-**M**ilitarized **Z**one

DoS

Denial of **S**ervice

In digital data processing, this is the term used 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.

EICAR

European Institute for **C**omputer **A**ntivirus **R**esearch

EST

Enrollment over **Secure Transport**

GPO

Group Policy Object

HSM

Hardware Security Module

Identifier

Symbol, unique within its security domain, that identifies, indicates, or names an entity which makes an assertion or claim of identity.

IDS

Intrusion Detection System

IEC

International Electrotechnical Commission, standards organization; communication standard for substations and protection equipment

Malware

or malicious code = malicious software

MBSA

Microsoft Baseline Security Analyzer

Mesh topology

Network setup where each node is interconnected to every other node.

MMS

Manufacturing Message Specification

NERC

North American Electric Reliability Corporation

NTP

Network Time Protocol

OTP

One Time Password

Patch

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

PKI

Public Key Infrastructure

RBAC

Role-Based Access Control

RODC

Read-Only Domain Controller

SDA

Secondary Distribution Automation

SIEM

Security Information and Event Management

SIESTA

Siemens Extensible Security Testing Appliance

SSL

Secure Sockets Layer -> TLS

TLS

Transport Layer Security

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.