SIEMENS

Secure Substation
Declaration of Security Conformance
IEC 62443-3-3

V1.00

Manual

E50417-T1040-C644-A1

NOTE

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

Document version: E50417-T1040-C644-A1.01

Edition: 02.2020

Version of the product described: V1.00

Preface

Purpose of the Manual

This Declaration of Conformance describes the conformance of a typical Siemens substation automation and protection system based on the Siemens secure substation blueprint with the IEC 62443-3-3 system security requirements and security levels.

Target Group

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

- Procurement of systems
- Sales of systems and equipment
- Project planning/implementation
- System service
- System operation

Scope

This manual applies to the substation automation systems based on SICAM, SIPROTEC, and SIMEAS products.

Additional Support

For questions about the system, contact your Siemens sales partner.

Customer Support Center

Our Customer Support Center provides a 24-hour service.

Siemens AG
Customer Support Center
Humboldtstrasse 59
90459 Nuremberg
Germany
E-mail: *support.energy@siemens.com*

Training Courses

Inquiries regarding individual training courses should be addressed to our Training Center:

Siemens AG
Siemens Power Academy TD
Humboldtstrasse 59
90459 Nuremberg
Germany

Phone: +49 (911) 433-7415
Fax: +49 (911) 433-7929
E-mail: *poweracademy@siemens.com*
Internet: *www.siemens.com/poweracademy*

Notes on Safety

This document is not a complete index of all safety measures required for operation of the equipment (module or device). However, it comprises important information that must be followed for personal safety, as well as to avoid material damage. Information is highlighted and illustrated as follows according to the degree of danger:

DANGER

DANGER means that death or severe injury **will** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

WARNING

WARNING means that death or severe injury **may** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid death or severe injuries.

CAUTION

CAUTION means that medium-severe or slight injuries **can** occur if the specified measures are not taken.

✧ Comply with all instructions, in order to avoid moderate or minor injuries.

NOTICE

NOTICE means that property damage **can** result if the measures specified are not taken.

✧ Comply with all instructions, in order to avoid property damage.

NOTE

Important information about the product, product handling or a certain section of the documentation which must be given attention.

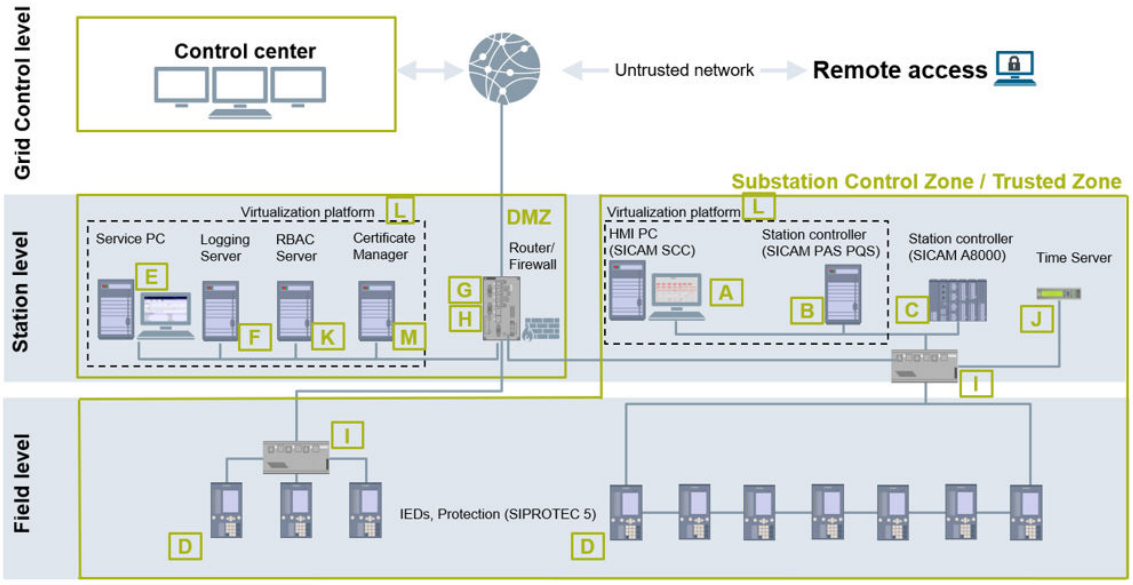
Table of Contents

1 Overview

1.1 Overview

The system in scope is a typical Siemens substation automation system that bases on the Siemens secure substation blueprint. The system comprises a substation control zone and a demilitarized zone (DMZ) protecting the substation control zone. These reside in the same physical location (site).

All IP-based communication to and from the substation control zone passes through the substation firewall (G/H in *Figure 1-1*). This communication comprises process-control related communication with a connected trusted control center zone and optional remote access connecting remote users. These external zones are not described in this document.



[sc_IEC_secure_substation_architecture, 1, en_US]

Figure 1-1 Secure Substation Architecture

Table 1-1 The reference system contains the following components:

Reference No.	Description
A	SICAM SCC Human Machine Interface (HMI) for local control and monitoring, hosted on a Windows operating system. This is the single point of control and monitoring inside the substation.
B	SICAM PAS/PQS Station Controller application hosted on a Windows operating system, as alternative to C
C	SICAM A8000 Station Controller RTU, as alternative to B
D	SIPROTEC 5 Protection and control IEDs
E	Service PC Host of all engineering tools and single point of all engineering accesses, hosted on a Windows operating system. The Service PC acts as jump host for remote access.
F	Substation central security logging server Collects all security logs from the components of the system. Source for all security logs for a superordinate SIEM system (not in scope)
G	Router with firewall, RUGGEDCOM firewall hosted on a ROX operating system
H	Router with firewall and integrated Intrusion Detection System (IDS)

Reference No.	Description
I	Network switch
J	Timer server
K	Active Directory Server and RADIUS Server Build as Read Only Domain Controller (RODC) hosted on a Windows operating system
L	Virtualization platform Microsoft HyperV hosted on a Windows operating system Optional implementation instead of dedicated hardware
M	Certificate Manager, SICAM GridPass hosted on a Windows operating system

The implementation in line with a secure integration process-compliant or adherent to IEC 62443-2-4 Security program requirements for IACS service provider is a prerequisite to ensure the overall security.

The statements given in this document are based on the assumption, that the implementation is in line with the architecture and the components in this chapter.

2 IEC 62443-3-3 Security Requirements

2.1 FR 1 – Identification and Authentication Control

2.1.1 SR 1.1 – Human User Identification and Authentication

The system design allows engineering and administrative access from the Service PC within the substation DMZ only. Access for operation is given through the HMI PC in the trusted zone. For both user authentication based on Windows account management is enforced.

In addition, centralized Role-Based Access Control (RBAC) via Active Directory (for Windows OS and applications) and RADIUS (IEDs, RTUs and network devices) is supported.

Requirement Enhancements

SR 1.1 RE 1 – Unique identification and authentication

All human user accounts are created with a unique identity. The system uses the unique identity to identify every authentication session to a single system user account.

Centralized Role-Based Access Control (RBAC) via Active Directory (for Windows OS and applications) and RADIUS (IEDs and network devices) is supported.

SR 1.1 RE 2 – Multifactor authentication for untrusted networks

Based on the architecture of the secure substation blueprint, remote access for all human users through the untrusted networks is provided by a Service called cRSP (common Remote Service Platform) hosted by Siemens. The remote access solution is used to gain access to the Service PC in the DMZ only. The cRSP enforces two-factor authentications with PKI (Public Key Infrastructure) for Siemens service engineers. For customer access a two-factor authentication with mobile PIN is default.

SR 1.1 RE 3 – Multifactor authentication for all networks

Human user access for configuration and operation is foreseen on Service PC and HMI PC. A two-factor authentication with smart cards can be deployed by the means of Windows operating system.

2.1.2 SR 1.2 – Software Process and Device Identification and Authentication

All device communication that traverses the secure substation zone boundary is controlled by a firewall with tight firewall configuration.

Requirement Enhancements

SR 1.2 RE 1 – Unique identification and authentication

The communication that traverses the secure substation zone boundaries is the process communication from the substation controller to the control center. The IEC 60870-5-104 communication is secured according to the IEC 62351 standard.

The remote access communication is secured by an IPsec VPN tunnel from the remote cRSP location to the secure substation. The remote access session terminates on the Service PC with additional authentication capabilities.

2.1.3 SR 1.3 – Account Management

Role-Based Access Control (RBAC) is supported in the control system for all user accounts and for all user access to the control system (Service PC, HMI). This includes capabilities to assign appropriate rights to users administering the user accounts for the system. Appropriate roles for the system, including operators, engineers, viewers can be configured.

Management of user accounts will require special authorization (administrator authorization) and cannot be performed by regular users.

Centralized RBAC via Active Directory (for Windows OS and applications) and RADIUS (IEDs, RTUs and network devices) is supported.

Requirement Enhancements

SR 1.3 RE 1 – Unified Account Management

All user accounts can be integrated in a centralized account management with Active Directory and RADIUS.

2.1.4 SR 1.4 – Identifier Management

Role-Based Access Control (RBAC) is supported in the system for all user accounts and for all user accesses to the control system (Service PC, HMI), with the possibility to provide a unique identifier to each entity. This includes capabilities to assign appropriate rights to users administering the user accounts for the system. Appropriate roles for the system, including operators, engineers, viewers, can be configured.

Centralized RBAC via Active Directory (for Windows OS and applications) and RADIUS (IEDs, RTUs and network devices) is supported.

Requirement Enhancements

None

2.1.5 SR 1.5 – Authenticator Management

For all Windows operating system-based systems, the required capabilities are provided through the operating system capabilities. Also, the applications on these systems support the capabilities.

For the embedded devices and the network devices, it is also possible to initialize, change, and refresh all passwords and further credentials.

SIPROTEC 5 protection relays and SICAM A8000 substation controller RTUs store locally managed passwords as salted hashes. Other critical authenticators (cryptographic keys) are stored securely in the on-board hardware security modules (HSMs) of the SIPROTEC 5 relays and A8000 RTUs.

Requirement Enhancements

SR 1.5 RE 1 – Hardware security for software process identity credentials

SIPROTEC 5 protection relays and SICAM A8000 substation controller RTUs store locally managed passwords as salted hashes. Authenticators (cryptographic keys) for firmware signature verification are stored securely in the on-board hardware security modules (HSMs) of the SIPROTEC 5 relays and A8000 RTUs.

Hardware security for PC-based systems is not part of the standard solution. This can be discussed on a project-specific basis.

2.1.6 SR 1.6 – Wireless Access Management

In order to reduce the risk, the secure substation blueprint avoids wireless communication.

Requirement Enhancements

SR 1.6 RE 1 – Unique identification and authentication

In order to reduce the risk, the secure substation blueprint avoids wireless communication.

2.1.7 SR 1.7 – Strength of Password-Based Authentication

The secure substation system design allows engineering access from the Service PC within the substation DMZ. Access for operation is only allowed from the HMI PC in the trusted zone. For both user authentication is enforced. The Service PC in DMZ and the HMI PC are based on Windows operating system. Microsoft Windows operation system has the capability to enforce password strength.

For IEDs, RTUs and network components password strength can be enforced via centralized management with RADIUS.

Requirement Enhancements

SR 1.7 RE 1 – Password generation and lifetime restrictions for human users

Windows operating system is configured to enforce policies to avoid password reuse and support lifetime restrictions.

SR 1.7 RE 2 – Password lifetime restrictions for all users

As system to system communication, the system uses IEC 60870-5-104 communication between the substation and the control center. The IEC 60870-5-104 communication is secured according to the IEC 62351 standard. This uses asymmetric cryptography and digital certificates with a limited lifetime as specified and recommended in the IEC 62351 standard.

2.1.8 SR 1.8 – Public Key Infrastructure (PKI) Certificates

Certificates can be obtained from an existing PKI. SICAM and SIPROTEC products use X.509 certificates for secure communication. Certificates can either be obtained automatically over the EST protocol (Enrollment over Secure Transport – RFC 7030) or via manual creation and import. Both of these options are supported by the SICAM GridPass certificate management product. SICAM GridPass can also be used to issue X.509-conformant certificates with IEC 62351-8 role extensions. IT offers support for CRLs (Certificate Revocation List) by hosting a CRL Distribution Point service.

Requirement Enhancements

None

2.1.9 SR 1.9 – Strength of Public Key Authentication

Secure process communication for IEC 60870-5-104 is supported in the system-based on IEC 62351. Validation capabilities are supported, including certificate chain validation and CRLs. Security configuration including the above certificate/key activities can only be performed through the configuration tools.

Access to the tools is only possible from the Service PC, and only authorized users on the Service PC with suitable rights are allowed to perform these activities.

Requirement Enhancements

SR 1.9 RE 1 – Hardware security for public key authentication

Critical authenticators are stored securely in the on-board hardware security modules (HSMs) of the SIPROTEC 5 relays and A8000 RTUs.

Hardware security for PC-based systems is not part of the standard solution. This can be discussed on a project-specific basis.

2.1.10 SR 1.10 – Authenticator Feedback

The default configuration in the system is to obscure password entry-related feedback. The system does not provide any hint in case of an authentication failure.

Requirement Enhancements

None

2.1.11 SR 1. 11 – Unsuccessful Login Attempts

Role-based access control is supported in the control system for all user accounts and for user access to the control system (Service PC, HMI). The Service PC in the DMZ and the HMI PC are based on Windows operating system. Windows operating system is configured to limit the number of invalid access attempts with the Account lockout threshold policy setting. For IEDs, RTUs, and network components this is realized via Active Directory through RADIUS.

Requirement Enhancements

None

2.1.12 SR 1.12 – System Use Notification

The Service PC in the DMZ and the HMI PC are based on the Windows operating system. Windows operating systems have the capability to enforce a use notification with the **LegalNoticeCaption** function. In the case of remote access to the system, human user authentication is centrally performed through the Service PC in the substation DMZ.

Requirement Enhancements

None

2.1.13 SR 1.13 – Access via Untrusted Networks

System access via untrusted networks (remote access, communication with the control center) is controlled and monitored by firewalls that support communication restrictions to the needed protocols, IP addresses and support logging and monitoring functions.

Requirement Enhancements

SR 1.13 RE 1 – Explicit access request approval

All remote access is monitored and controlled by a terminal server. cRSP remote access solution is supported to provide additional access control.

NOTE

Explicit Access Request Approval:

- Requirement is met by a network switch in the DMZ through which the untrusted network is connected. The network switch can be powered on/off by the control center via an RTU.
- Requirement is met by an administrator in the control center who adds or deletes a user in the remote access user group on the Service PC in the DMZ.

2.2 FR 2 – Use Control

2.2.1 SR 2.1 – Authorization Enforcement

Role-based access control is supported in the system for all user accounts and for all user accesses to the control system (Service PC, HMI, IEDs, RTUs, and network devices). This includes capabilities to assign appropriate rights to users administering the user accounts for the system. Appropriate roles for the system, including operators, engineers, viewers can be configured.

Requirement Enhancements

SR 2.1 RE 1 – Authorization enforcement for all users

In addition, authorization for software processes and devices is provided through enforcing secure zones and tight firewall configuration for access to secure zones.

SR 2.1 RE 2 – Permission mapping to roles

Management of user accounts will require special authorization (administrator authorization) and cannot be performed by regular users.

Account permissions can be enforced via the Active Directory server or applications.

SR 2.1 RE 3 – Supervisor override

The main objective of the substation automation and protection system is to protect the primary assets from damage. In case of a primary fault all automated and user interaction will be interrupted by the protection functionalities.

The control center can override the local rights to perform actions.

SR 2.1 RE 4 – Dual approval

Additional authorization depends on the configuration of the individual component for dual approval.

Dual approvals can be implemented for different serious functionalities. For example via a command interlocking a dedicated switch command can be programmed, that a release from control center is needed.

2.2.2 SR 2.2 – Wireless Use Control

In order to reduce the risk, the secure substation blueprint avoids wireless communication.

Requirement Enhancements

SR 2.2 RE 1 – Identify and report unauthorized wireless devices

In order to reduce the risk, the secure substation blueprint avoids wireless communication.

2.2.3 SR 2.3 – Use Control for Portable and Mobile Devices

The system design only allows engineering access from the Service PC within the substation DMZ. Access from other sources will be prevented by the DMZ/Firewall configuration.

No wireless technologies are used or enabled in the system. Hence, engineering/maintenance access with wireless devices is not possible.

Hardening measures in addition include the hardening of unused Ethernet and USB ports within the secure zone through configuration and physical protection.

Requirement Enhancements

SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices

Uncontrolled connection of portable devices is prevented through appropriate hardening measures, see *2.3 FR 3 – System Integrity*. All engineering/maintenance access has to be performed through the substation DMZ that ensures an appropriate level of compliance for connection attempts of temporary devices to the substation zones.

2.2.4 SR 2.4 – Mobile Code

In general, mobile code exchange from outside the system with the system is not needed and not allowed. System-wide hardening limits the attack surface that would allow malware to enter the system. Examples are the secure zone concept including firewalls at the zone borders, and deactivation of USB and network ports. Deinstallation of unneeded software and secure configuration of application software reduces the risk of malware introduction through mobile code (for example in PDF files, Javascript).

For Windows-based systems malware protection (classical antivirus or application whitelisting) is in place.

Requirement Enhancements

SR 2.4 RE 1 – Mobile code integrity check

In addition to the enforcement of digitally signed updates for the Windows-based systems, for the SIPROTEC 5 relays and SICAM A8000 RTUs, firmware images are protected by digital signatures generated by Siemens. This ensures cryptographically secured integrity verification and prevents the installation of unauthorized software (for example malware) on the IEDs and RTUs.

2.2.5 SR 2.5 – Session Lock

Session time-out is supported by network devices, IEDs, RTUs, and the Microsoft operating system.

Requirement Enhancements

None

2.2.6 SR 2.6 – Remote Session Termination

The Siemens remote access tool cRSP allows the configuration of a defined idle time. In addition, a session timeout can be enforced on the Service PC that terminates all remote access and enforces additional remote user authentication and authorization based on the Windows operating system.

Requirement Enhancements

None

2.2.7 SR 2.7 – Concurrent Session Control

The secure substation system design only allows engineering access from the Service PC within the substation DMZ. Access from other sources will be prevented by the DMZ/Firewall configuration. The default configuration of the Windows client operating system is to allow only one session.

For process communication a one-to-one communication is configured.

For the network devices and the Windows server-based system, a maximum number of concurrent sessions can be configured.

Requirement Enhancements

None

2.2.8 SR 2.8 – Auditable Events

Security-related events are logged across the whole system. All components support security logging. A security-logging server acts as central destination and collects the security logs via the syslog protocol.

Requirement Enhancements

SR 2.8 RE 1 – Centrally managed, system-wide audit trail

To ensure that security logs are kept for a specified number of days and to provide them for further analysis, a security logging server acts as central destination and collects the security logs via the syslog protocol. This server can be connected to a superordinate SIEM system without interfering with the substation component configuration.

2.2.9 SR 2.9 – Audit Storage Capacity

The Windows-based systems (engineering PC, HMI, station controller SICAM PAS) support the Windows event log. The maximum log capacity can be configured via the Windows GPO (group policy objects). A percentage threshold can be configured for the security event log at which the system will generate a warning. For SIPROTEC 5 relays and SICAM A8000 RTUs, a ring buffer for the security log is supported (adherent to IEEE 1686). The storage capacity on the syslog server is limited by the disc space only. The logging server has the capability to send a message to a SIEM if a threshold (disk space) is reached. The logging server has the capability to automatically delete old log entries after sending those to a SIEM.

Requirement Enhancements

SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached

The Windows-based systems generate a warning in case a capacity threshold is reached. The IEDs and RTUs work with a device-internal security event ring buffer. The newest entry overwrites the oldest entry once the ring buffer becomes full. All components are configured to send the security-events information continuously to the syslog server. The syslog server itself generates a warning to a SIEM if a configurable capacity threshold is reached.

2.2.10 SR 2.10 – Response to Audit Processing Failures

The control system prevents the loss of information with several measures depending on the dedicated component.

- Configuration of enough storage capacity on the PC-based systems
- Implementation of security log ring buffer in embedded components.

The security log information will be sent to a syslog server in near-real-time manner. The syslog server on substation level acts as an intermediate storage between the single components and a superordinate SIEM system. Failures between the syslog server and SIEM are recognized and lead to a log entry.

Requirement Enhancements

None

2.2.11 SR 2.11 – Timestamps

All audit records and operational logs of the substation automation system contain a timestamp.

Requirement Enhancements

SR 2.11 RE 1 – Internal time synchronization

Time synchronization can be performed within the secure substation for all components. Related protocols (NTP) do not traverse zone boundaries to untrusted networks. Time information can only be exchanged and handled within the secure substation. The time server is synchronized via an external source, for example GPS (Global Position System).

SR 2.11 RE 2 – Protection of time source integrity

Access to the local time server is protected by the RBAC. Changes in date and time lead to an audit log entry.

2.2.12 SR 2.12 – Non-Repudiation

User authentication and authorization is enforced for engineering and operations on the Service PC, on the HMI PC and in the IEDs, RTUs, and network devices in the substation. Logging of security relevant actions in the system is realized both at OS level (Windows security event log) as well as at the application and component level. Process-related actions like state changes are logged and are centrally collected. They can be displayed by the HMI components like SICAM SCC and they are logged in the Syslog server.

Requirement Enhancements

SR 2.12 RE 1 – Non-repudiation for all users

Process-related actions from non-human users, like protection trips and automated reclose sequences are logged in detail in the fault log of the protection relays. Access to the fault logs is restricted by tied access control and account management configurations.

2.3 FR 3 – System Integrity

2.3.1 SR 3.1 – Communication Integrity

The secure substation is based on secure zones and tight firewall configuration for access to secure zones. The equipment withstands the harsh environmental conditions in the substation. This avoids violation of communication integrity due to electromagnetic impact.

Requirement Enhancements

SR 3.1 RE 1 – Cryptographic integrity protection

All communication traversing untrusted zones is cryptographically secured. Remote-access connections via untrusted networks terminate on a service computer acting as terminal server in the substation's DMZ. The remote-access solution is based on Siemens cRSP (common Remote Service Platform). The approach includes state-of-the-art secure communication based on an IPsec VPN. In addition, IEC 62351 security for IEC 60870-5-104 process communication can be deployed.

2.3.2 SR 3.2 Malicious Code Protection

For Windows-based systems, antivirus and application whitelisting solutions are released. For the secure substation it is recommended to use Microsoft Windows Defender Antivirus and Microsoft Windows Defender Application Control. Updates for antivirus signatures can be deployed via WSUS offline (Windows Server Update Services).

SIPROTEC 5 protection IEDs and SICAM A8000 RTUs use digitally signed firmware as a malicious code prevention mechanism.

Requirement Enhancements

SR 3.2 RE 1 – Malicious code protection on entry and exit points

Apart from the available malware protection capabilities, additional IDS (Intrusion Detection System) can be configured at network boundaries for more protection.

Requirement Enhancements

SR 3.2 RE 2 – Central management and reporting for malicious code protection

Windows-based malware protection can be centrally managed via Windows GPOs. Security-related events in the substation automation solution are collected by the specific mechanisms of the different components. The security logs can be provided to a centralized logging server for further analysis.

2.3.3 SR 3.3 – Security Functionality Verification

Verification of correct implementation of security functions to address the security requirements is performed according to the security tests described in the FAT/SAT test book that is part of the secure substation blueprint. The test cases cover all security controls, including system hardening, malware protection, account management, access control, security logging, and monitoring among others.

Requirement Enhancements

SR 3.3 RE 1 – Automated mechanisms for security functionality verification

The secure substation supports manual and automated security functionality verification during FAT, SAT and maintenance. Manual tests and automated tests with test tools, for example

- SiESTA Siemens Extensible Security Testing Appliance, which includes NMAP (port scanner), NESSUS (vulnerability scanner) and other security inspection tools
- MBSA (Microsoft Baseline Security Analyzer)
- EICAR (European Institute for Computer Antivirus Research)

are documented in the FAT/SAT test book.

Requirement Enhancements

SR 3.3 RE 2 – Security functionality verification during normal operation

SiESTA (Siemens Extensible Security Testing Appliance) can be used to execute regular security tests during normal operation. The described test profiles were tested in a substation test bed to ensure minimized impact on availability of the tested system and can be adjusted to exclude critical functions for regular scans during operation.

2.3.4 SR 3.4 – Software and Information Integrity

The integrity checks are based on digitally signed software and component capabilities. Microsoft and application software updates (for example SICAM PAS) are protected by digital signatures. Firmware updates for SIPROTEC 5 and SICAM A 8000 devices are digitally signed.

Requirement Enhancements

SR 3.4 RE 1 – Automated notification about integrity violations

The security-relevant integrity violations of the mechanisms stated in *2.3.4 SR 3.4 – Software and Information Integrity* are logged and can be used for notifications.

2.3.5 SR 3.5 – Input Validation

As standard capability, the substation components perform verification of process-related input values, for example regarding allowed ranges.

The component communication interfaces undergo robustness tests as part of the component development process.

All engineering tools (for example DIGSI 5, Toolbox II) and the HMI (SICAM SCC) check out-of-range and data types of all input values as a basic function for an industrial automation system. Input validation is one of the basic test cases in the product development process.

Requirement Enhancements

None

2.3.6 SR 3.6 – Deterministic Output

In case of abnormal communication, the protection relays (SIPROTEC 5) will continue to provide protection, independent of the state of the substation network or other substation components. In cases where communication modules of protection relays are impacted due to network issues, the degradation in communication between protection relays, station controller, and control center is tolerable in order to continue providing the core protection function for the energy distribution process.

Requirement Enhancements

None

2.3.7 SR 3.7 – Error Handling

The system has the capability to restrict error message content to authorized roles (for example for forensics purposes in case of incident handling). The content and structure of error messages in the system follow established guidelines.

Requirement Enhancements

None

2.3.8 SR 3.8 – Session Integrity

Communication via untrusted interfaces is protected by TLS in line with IEC 62351 or VPN with state-of-the-art security implementation that ensures integrity as well as correct and secure session ID handling.

Requirement Enhancements

SR 3.8 RE 1 – Invalidation of session IDs after session termination

Web interfaces (for example for the router and switch configuration) undergo regular penetration testing and follow a secure development process to ensure correct implementation of TLS-based integrity protection in the component Web servers and correct session cookie handling within the https based sessions.

Session ID handling includes verification of uniqueness, randomness, and invalidation of session IDs as part of session termination.

Requirement Enhancements

SR 3.8 RE 2 – Unique session ID generation

Web interfaces (for example for the router and switch configuration) undergo regular penetration testing and follow a secure development process to ensure correct implementation of TLS-based integrity protection in the component Web servers and correct session cookie handling within the https based sessions.

Session ID handling includes verification of uniqueness, randomness, and invalidation of session IDs as part of session termination.

Requirement Enhancements

SR 3.8 RE 3 – Randomness of session IDs

Web interfaces (for example for the router and switch configuration) undergo regular penetration testing and follow a secure development process to ensure correct implementation of TLS-based integrity protection in the component Web servers and correct session cookie handling within the https based sessions.

Session ID handling includes verification of uniqueness, randomness, and invalidation of session IDs as part of session termination.

2.3.9 SR 3.9 – Protection of Audit Information

Capabilities to protect audit-log data and files from unauthorized access and modification are available through Windows operating system features, and through role-based access control to the IEDs, RTUs, and network devices.

The central logging server is protected by tied access control and account management capabilities.

Requirement Enhancements

SR 3.9 RE 1 – Audit records on write-once media

This is not part of the standard solution. This can be discussed on a project-specific basis.

2.4 FR 4 – Data Confidentiality

2.4.1 SR 4.1 – Information Confidentiality

Confidentiality of sensitive data like user authorization and certificate information is ensured in the system by applying appropriate access protection mechanisms.

Windows-based systems use the Windows build-in data protection architecture. The SIPROTEC 5 relays and SICAM A 8000 RTUs use a hardware security module (HSM) based protection mechanism for that purpose.

Requirement Enhancements

SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks

Remote access to the system is available only through Siemens' cRSP (common Remote Service Platform), which terminates in Substation DMZ. The cRSP communication channel is secured by a VPN tunnel. The communication is reduced to a remote desktop connection.

SR 4.1 RE 2 – Protection of confidentiality across zone boundaries

The communications that traverse zone boundaries are the communications to the control center. Both IEC 60870-5-104 and IEC 61850 communication can be secured by TLS based on IEC 62351.

Depending on the control center solution a VPN tunnel is an alternative solution.

2.4.2 SR 4.2 – Information Persistence

In Windows-based systems and portable media, common mechanisms for data sanitizing (wipe hard drives/ portable media and drives with appropriate tools) can be used. BIOS reset to factory defaults can be performed.

In embedded systems, full reset of all sensitive data can be performed. The IEDs SIPROTEC 5 and SICAM A8000 support secure factory reset functionality.

Requirement Enhancements

SR 4.2 RE 1 – Purging of shared memory resources

This is related to Windows-based systems, where shared memory is a use case. The confidential data like credentials are not stored in plain text.

2.4.3 SR 4.3 – Use of Cryptography

The secure substation does not use own/proprietary cryptographic algorithms. Standardized mechanisms, including X.509 certificates, SSL/TLS, IPsec, and IEC 62351 profiles are used.

Common best practices regarding crypto algorithms and key lengths are constantly monitored from diverse international sources (for example NIST, BSI) and adopted in the components.

Requirement Enhancements

None

2.5 FR 5 – Restricted Data Flow

2.5.1 SR 5.1 – Network Segmentation

The architecture of the secure substation blueprint separates control system networks from non-control system networks. The zoning concept is a result from a threat and risk analysis (TRA). All essential functions of the substation automation system are located in the substation control zone. Zones are separated with firewalls with tied firewall configurations.

Requirement Enhancements

SR 5.1 RE 1 – Physical network segmentation

The network zones can be physically separated with firewalls.

SR 5.1 RE 2 – Independence from non-control system networks

The substation system is designed to continue independent operation without relying on external network services. This also ensures robustness in situations where connectivity to other zones and external networks cannot be maintained.

Design examples are the RBAC Server implemented as RODC in the substation and the Logging Server in the DMZ. Base protection and automation functions can be ensured inside the substation control zone.

SR 5.1 RE 3 – Logical and physical isolation of critical networks

The critical part of the substation is the substation control zone including the SIPROTEC 5 protection relays and the station controller.

Based on the criticality of the substation, this can be further separated into a station controller zone and a protection zone by an additional router/firewall.

2.5.2 SR 5.2 – Zone Boundary Protection

The network segmentation is accomplished by separating the networks using dedicated network elements such as firewalls or routers with firewall functionality. The firewalls control all inbound and outbound communication. All blocked traffic will be logged for further analysis.

Requirement Enhancements

SR 5.2 RE 1 – Deny by default, allow by exception

The default recommended firewall configuration only allows the required communication and protocols. This is based on the minimal needs of all communication endpoints in the secure substation.

"Deny by default, allow by exception" is a basic design rule in the secure implementation process according to IEC 62443-2-4.

SR 5.2 RE 2 – Island mode

The secure substation architecture is designed to continue independent operation. It does not rely on external network services from outside the secure zone to execute the base protection and automation functions.

Design examples are the RBAC Server implemented as RODC in the substation and the Logging Server in the DMZ. Base protection and automation functions can be ensured inside the substation control zone.

SR 5.2 RE 3 – Fail close

The secure substation architecture is designed to continue independent operation. It does not rely on external network services from outside the secure zone to execute the base protection and automation functions.

2.5.3 SR 5.3 – General purpose person-to-person communication restrictions

Secure zone boundaries are protected by firewalls. The default recommended firewall configuration only allows the required communication and protocols. All other communication like unnecessary protocols carrying person-to-person communication is denied.

Requirement Enhancements

SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications

Secure zone boundaries are protected by firewalls. The default recommended firewall configuration only allows the required communication and protocols. All other communication like unnecessary protocols carrying person-to-person communication is denied.

The system-wide hardening measures include the removing of all unnecessary software for person-to-person communication.

2.5.4 SR 5.4 – Application partitioning

Partitioning of different functions, applications, or data are supported.

Critical automation and protection functions are located in the substation control zone. Management functionality (for example engineering) is located in the DMZ instead of placing it directly in the secure substation zone. Additional secure zones can be realized to meet specific customer needs or specific secure design policies.

Requirement Enhancements

None

2.6 FR 6 – Timely Response to Events

2.6.1 SR 6.1 – Audit Log Accessibility

All components of the substation automation system provide security audit log capabilities. The audit logs can be accessed by authorized users.

The type of access varies depending on the nature of the component's operating system and application.

Requirement Enhancements

SR 6.1 RE 1 – Programmatic access to audit logs

Unattended / automated population of audit records is made possible at a central server by activating Syslog protocol on all components.

The logging server is foreseen as a single point of access to all audit records of the system.

2.6.2 SR 6.2 – Continuous Monitoring

The dedicated logging server acts as a single point of access to all security logs of the system. This logging server is foreseen to send all syslog information to a superordinated SIEM system. The substation automation system is therefore SIEM-ready. In order to increase the transparency an optional IDS (Intrusion Detection System) can be implemented in the substation.

Requirement Enhancements

None

2.7 FR 7 – Resource Availability

2.7.1 SR 7.1 – Denial of Service Protection

Denial-of-Service (DoS) protection is realized with the defense-in depth approach.

Firewalls at the zone borders protect the secure substation zone and prevent direct communication with the substation control zone from untrusted networks.

SIPROTEC 5 protection relays are designed to work autonomously without depending on other components of the substation system.

All components undergo security tests that include robustness tests of communication interfaces.

Requirement Enhancements

SR 7.1 RE 1 – Manage communication loads

To manage unexpected communication loads at the substation zone border, the substation firewall configuration does not allow direct communication from untrusted networks into the substation control zone. The firewall provides protection capability for flooding and protection against SYN flooding attacks.

SR 7.1 RE 2 – Limit DoS effects to other systems or networks

Besides required communication to the control center and remote access to the substation, the substation firewall blocks all other network traffic. Therefore, general DoS attacks from the substation to other connected networks are made difficult. No other control system networks are connected, so there is a limited risk of affecting other control system networks from the substation.

2.7.2 SR 7.2 – Resource Management

Critical automation and protection functions are located in the substation control zone. Management functionality (for example engineering) is located in the DMZ instead of placing it directly in the secure substation zone. The substation system is designed to continue independent basic operation without relying on external network services.

Requirement Enhancements

None

2.7.3 SR 7.3 – Control System Backup

All components of the substation automation system have the capability to back up and restore critical files like configuration and real time data that are needed to restore the system. The critical process protection is provided by the SIPROTEC 5 relays and is not affected by backup operations. The latest relay firmware and configuration are backed up via the engineering tool and are available on the Service PC (no backup directly from the relay is needed during operation).

Requirement Enhancements

SR 7.3 RE 1 – Backup verification

The verification and validation of the backup process is part of the FAT/SAT test book and therefore part of the FAT/SAT.

SR 7.3 RE 2 – Backup automation

Automated backups can be realized with the means of the Windows operating system.

2.7.4 SR 7.4 – Control System Recovery and Reconstitution

Disaster recovery capabilities and strategies based on the backup and restore capabilities stated for SR 7.3. The capabilities include backup and recovery of software, configuration and operational data. This includes also the secure configuration like implemented hardening, updates and patches.

Requirement Enhancements

None

2.7.5 SR 7.5 – Emergency Power

For the system in scope, the capability is provided as due to loss of power supply no degradation of security will occur. Loss of power supply for the substation firewall or Service PC will result in temporary unavailability from remote, not in allowing any-to-any communication.

Requirement Enhancements

None

2.7.6 SR 7.6 – Network and Security Configuration Settings

The substation system can be configured according to the recommended system security and hardening guidelines. The system can be configured to provide alarms and syslog support to interface with external monitoring systems of the asset owner.

Requirement Enhancements

SR 7.6 RE 1 – Machine-readable reporting of current security settings

The system has the capability to generate reports of its configuration (for example Windows operating system capabilities for the Windows-based systems; export of firewall configuration).

The components support this with the respective engineering tools.

2.7.7 SR 7.7 – Least Functionality

Capabilities to set configuration options to a secure state (hardening) are provided by all components, for example disabling of ports, removal of unneeded software, or restricted account configuration. The recommended settings are described in the system hardening guide.

Requirement Enhancements

None

2.7.8 SR 7.8 – Control System Component Inventory

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, reducing documentation time and efforts on information gathering, facilitating evaluation of patch management procedures.

Requirement Enhancements

None

Literature

/1/ IEC 62443-3-3: System security requirements and security levels

/2/ IEC 62443-2-4: Security Program Requirements for IACS Service Providers

/3/ IEC 62351 series: Power systems management and associated information exchange – Data and communications security

/4/ Secure Substation Manual – System Hardening for Substation Automation and Protection
can be downloaded under: *www.siemens.com/gridsecurity* (Cyber Security General Downloads > Manuals)

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 **I**nfrastructure **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 **o**f **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 **I**nstitute for **C**omputer **A**ntivirus **R**esearch

EST

Enrollment over **S**ecure **T**ransport

GPO

Group **P**olicy **O**bject

HSM

Hardware **S**ecurity **M**odule

Identifier

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

IDS

Intrusion **D**etection **S**ystem

IEC

International **E**lectrotechnical **C**ommission, standards organization; communication standard for substations and protection equipment

IEEE

Institute of **E**lectrical and **E**lectronics **E**ngineers, organization for electronic and electrical engineering

Malware

or malicious code = malicious software

MBSA

Microsoft **B**aseline **S**ecurity **A**nalyzer

NERC

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

NTP

Network **T**ime **P**rotocol

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 **K**ey **I**nfrastucture

RBAC

Role-**B**ased **A**ccess **C**ontrol

RODC

Read-Only Domain Controller

SIEM

Security **I**nformation and **E**vent **M**anagement

SiESTA

Siemens **E**xtensible **S**ecurity **T**esting **A**ppliance

SSL

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

TLS

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

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