SIEMENS

SICAM A8000 Series
SICAM RTUs
SICAM TOOLBOX II
SICAM Device Manager

ADMINISTRATOR
Security-Manual

Preface, Table of Contents

Introduction 1

Typical Plant Configurations 2

Measures for System Hardening 3

Communication Protocols 4

Patch Management 5

Virus Protection 6

Encryption and Authentication processes 7

Backup & Restore 8

Logging 9

Remote Maintenance 10

User Administration 11

Hardware Interfaces 12

Security Measure Plan for Oracle Database A

Licensing agreement B

Literature

DC0-115-2.23

Document version: DC0-115-2.23
Edition: 07.2021

Siemens AG
Energy Automation
Humboldtstraße 59
90459 Nürnberg
Germany

Order Number.: DC0-115-2.23

Preface

Contents of the Manual

As a basis for a secure system design and operation the following information about SICAM RTUs and SICAM A8000 Series, SICAM PTS Protocol Test System and SICAM TOOLBOX II, SICAM Device Manager and SICAM WEB is contained in this manual:

- Typical system configurations
- Secure basic configuration
- Security relevant system settings, parameters and their defaults
- Measures for system hardening
- Traffic matrix (communication interfaces)
- Instructions for security conscious behavior (backup / restore, …)
- Patch management
- Antivirus protection
- Explanation of security specific log and audit messages; possible causes; suitable countermeasures

This information can be used as a starting basis for the secure design and secure operation of a complete system.

Hint

Current SICAM RTUs support a HTTPS-Web server for remote operation with SICAM TOOLBOX II.

Some SICAM RTUs protocols and some SICAM A8000 protocols support a WEB server for diagnostic purposes (access via WEB browser). Authentication for these WEB pages is not provided for.

Therefore, for normal operation this possibility of access should be deactivated via parameterization.

Scope of Validity

This document is valid for SICAM RTUs and the products of the SICAM A8000 Series product line with hardware and firmware versions dated October 2014 or later, SICAM PTS Protocol Test System and for SICAM TOOLBOX II (engineering system for parameterization, diagnostics, simulation) and / or SICAM Device Manager and / or SICAM WEB.

More specifically, this includes:

- SICAM A8000 Series:
  - SICAM CP-8031
  - SICAM CP-8050
  - SICAM CP-8000
  - SICAM CP-8021
  - SICAM CP-8022
- SICAM RTUs
  - SICAM AK 3
  - SICAM BC
- SICAM PTS Protocol Test System
- SICAM TOOLBOX II
  (as application, includes neither hardware, nor an operating system or other standard software such as Microsoft Office or Adobe Acrobat Reader)
- SICAM Device Manager
  (as application, includes neither hardware, nor an operating system or other standard software such as Microsoft Office or Adobe Acrobat Reader)

- SICAM WEB
  (as application, includes neither hardware, nor an operating system or other standard software such as Microsoft Office or Adobe Acrobat Reader)
- This document only describes product characteristics of SICAM A8000 Series, SICAM RTUs, SICAM PTS Protocol Test System and SICAM TOOLBOX II / SICAM Device Manager. It does not describe any system characteristics that result from system-specific networking and parameterizing of the products into a system.

Hint

In this document SICAM RTUs is a collective term for the product line containing SICAM AK 3 and SICAM BC.

Unless otherwise stated, the term SICAM RTUs refers to SICAM AK 3.

Target Group

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

- sales of systems and equipment
- project planning/implementation
- system service
- system operation

Conventions Used

- Manuals that are referenced are written in italics
  e.g. Common Functions, System and Basic System Elements, section Information Objects.
- Menu paths, operator inputs, commands are written in bold letters.
  e.g.: **Authorizations → User/Role Administration → Define User ...**
- SICAM TOOLBOX II parameters are shown with the font Courier in violet.
  e.g.: `Additional parameters | Remote operation`

Notes on Safety

This manual does not constitute a complete catalog of all safety measures required for operating the equipment (module, device) in question because special operating conditions might require additional measures. However, it does contain notes that must be adhered to for your own personal safety and to avoid damage to property. These notes are highlighted with a warning triangle and different keywords indicating different degrees of danger.

Danger

means that death, serious bodily injury or considerable property damage **will** occur, if the appropriate precautionary measures are not carried out.

Warning

means that death, serious bodily injury or considerable property damage **can** occur, if the appropriate precautionary measures are not carried out.

Caution

means that minor bodily injury or property damage could occur, if the appropriate precautionary measures are not carried out.

Hint

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

Qualified Personnel

Commissioning and operation of the equipment (module, device) described in this manual must be performed by qualified personnel only. As used in the safety notes contained in this manual, qualified personnel are those persons who are authorized to commission, release, ground, and tag devices, systems, and electrical circuits in accordance with safety standards.

Use as Prescribed

The equipment (device, module) must not be used for any other purposes than those described in the Catalog and the Technical Description. If it is used together with third-party devices and components, these must be recommended or approved by Siemens.

Correct and safe operation of the product requires adequate transportation, storage, installation, and mounting as well as appropriate use and maintenance.

During operation of electrical equipment, it is unavoidable that certain parts of this equipment will carry dangerous voltages. Severe injury or damage to property can occur if the appropriate measures are not taken:

- Before making any connections at all, ground the equipment at the PE terminal.
- Hazardous voltages can be present on all switching components connected to the power supply.
- Even after the supply voltage has been disconnected, hazardous voltages can still be present in the equipment (capacitor storage).
- Equipment with current transformer circuits must not be operated while open.
- The limit values indicated in the manual or the operating instructions must not be exceeded; that also applies to testing and commissioning.

Consider obligatory the safety rules for the accomplishment of works at electrical plants:

1. Switch off electricity all-pole and on all sides!
2. Ensure that electricity cannot be switched on again!
3. Double check that no electrical current is flowing!
4. Discharge, ground, short circuit!
5. Cover or otherwise isolate components that are still electrically active!

Information about Conformity

The product described conforms to the regulations of the following European Directives:

- 2014/30/EU
  Directive of the European Parliament and of the Council of 26 February 2014 on the harmonization of the laws of the Member States relating to electromagnetic compatibility; Official Journal of the EU L96, 29/03/2014, p. 79–106
- 2014/35/EU
  Directive of the European Parliament and of the Council of 26 February 2014 on the harmonization of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits; Official Journal of the EU L96, 29/03/2014, p. 357–374

The conformity of the product with the regulations of Directive 2014/30/EU is proven through the observance of the harmonized standard

- EN 60870-2-1:1996

The conformity of the product with the regulations of Directive 2014/35/EU is proven through the observance of the harmonized standard

- EN 61010-1:2010

This declaration certifies the conformity with the specified directives, but is not an assurance of characteristics in the sense of the product liability law.

The product is intended exclusively for use in an industrial environment.

Table of Contents

1 Introduction 13

1.1 Objective 13
1.2 Observance of Standards 14
1.3 Security Requirements 14
1.4 Data Privacy Considerations 15

2 Typical Plant Configurations 17

2.1 General 17
2.1.1 Object Protection 17
2.1.2 Network Segmentation / Communication between the Zones 18
2.1.3 Communication within a Zone 18
2.1.4 Communication between the Zones 18
2.2 Network Components 19
2.2.1 Design and Operating Environment 19
2.2.2 Type 19
2.2.3 Management 21
2.3 Typical Network Configurations 22
2.3.1 Control Center Zone and Substation Zone without VPN 23
2.3.2 Control Center Zone and Substation Zone with VPN 25
2.3.3 Substation Zone without Segmentation with external Firewall Rules 27
2.3.4 Substation Zone with Segmentation without internal Firewall Rules 28
2.3.5 Substation Zone with Segmentation with internal Firewall Rules 29
2.3.6 Substation Zone with Segmentation through “Hardware-Based Application-Layer-Firewall” 30
2.3.7 Substation Zone with Engineering Zone 34
2.3.8 Substation Zone with Out Of Band Remote Maintenance 36
2.3.9 Control Center Zone without Segmentation with external Firewall Rules 38
2.3.10 Control Center Zone with Segmentation / Engineering Zone 39
2.3.11 Control Center Zone with Office Firewall 40
2.3.12 Control Center Zone with DMZ 41
2.3.13 Control Center Zone with Internet and Update DMZ 43

3 Measures for System Hardening 45

3.1 General 45
3.2 Supported LAN-Services 46
3.2.1 Services integrated on the Basic System Element 46
3.2.2 Services integrated on the Protocol Element 47
3.3 SICAM A8000 Series / SICAM RTUs 48
3.3.1 Digital signatures 48
3.3.2 Deactivation of Unnecessary System and Communication Services 52

3.3.2.1 One Click to Connect (SICAM A8000 CP-8031/CP-8050) ... 52
3.3.2.2 Remote Operation ... 52
3.3.2.3 Remote Maintenance ... 56
3.3.2.4 Process Reset Command (remote reset) ... 57
3.3.2.5 Time Synchronization – Remote Synchronization ... 58
3.3.2.6 Time Synchronization via (S)NTP ... 59
3.3.2.7 Secure NTP Client (CP-8031/CP-8050 only) ... 59
3.3.2.8 WEB-Server Protocols ... 60
3.3.3 Measures for restricted distribution of system messages ... 62
3.3.3.1 Blocking of messages in topology configuration of SICAM RTUs ... 62
3.3.4 Denial of Service ... 62
3.3.5 Communication to SICAM RTUs via USB ... 63
3.3.6 Enabling for Parameterization/ Diagnostics via Web-Browser ... 63
3.3.7 Secure connection establishment via HTTPS ... 64
3.3.7.1 SICAM A8000 CP-8031/CP-8050 ... 64
3.3.7.2 SICAM A8000 CP-8000/ CP-802x; AK 3 and BC (with SM-2558) ... 66
3.3.8 Connection Password SICAM A8000 CP-8000/ CP-802x/ SICAM RTUs ... 66
3.3.8.1 Assign/Change „Connection Passwords“ ... 68
3.3.8.2 Reset the „Connection Password“ ... 69
3.3.8.3 Device change ... 69
3.3.8.4 Initialize Automation Unit ... 69
3.3.9 Role-Based-Access-Control in SICAM A8000 Series ... 69
3.3.10 PKI Infrastructure/ Certificate Management in SICAM A8000 Series according to IEC 62351-9 ... 72
3.3.10.1 Certificate-based encryption algorithms supported by SICAM A8000 Series ... 72
3.3.10.2 Manual Certificate Management ... 73
3.3.10.3 Automatic Certificate Management according to IEC 62351-9 ... 75
3.3.10.4 Certificate Revocation List (CP-8031/CP-8050) ... 77
3.3.11 AoR ... 78
3.3.12 External Authentication via RADIUS in SICAM A8000 Series ... 78
3.3.13 External Authentication via LDAP in CP-8031/CP-8050 ... 80
3.3.14 IEEE 802.1X ... 81
3.3.14.1 802.1xSupplicant ... 82
3.3.14.2 802.1x Authenticator ... 86
3.3.15 Secure Factory Reset in SICAM A8000 Series, SICAM AK 3 ... 89
3.3.16 Storage of Passwords in SICAM A8000 Series / SICAM RTUs ... 90
3.3.17 Connection of Systems without Security-Functions ... 90
3.4 SICAM PTS Protocol Test System ... 91
3.4.1 Windows System Hardening ... 91
3.5 SICAM Device Manager ... 91
3.5.1 Windows System Hardening ... 91
3.6 SICAM TOOLBOX II ... 92
3.6.1 Windows System Hardening ... 92
3.6.2 Solidification ... 92

3.6.3 Deinstallation or Deactivation of unnecessary Software Components 92
3.6.4 Deactivation of unnecessary System and Communication Services 93
3.6.4.1 Remote Operation 93
3.6.4.2 Remote Maintenance 93
3.6.5 Deactivation of unnecessary Standard Users 93
3.6.6 Limitation of the Rights of Users and Programs.....93
3.7 Security Penetration Testing 94

4 Communication Protocols 95

4.1 Serial Communication Protocols 95
4.1.1 Point-to-Point / Multipoint Traffic 95
4.1.2 Dial-Up Traffic.....95
4.2 Ethernet based Communication Protocols 96
4.2.1 Ethernet based IO Bus (EbIO) 96
4.2.2 IP-based Protocols SICAM A8000 CP-8031/CP-8050.....96
4.2.2.1 IPSec VPN in SICAM A8000 CP-8031/CP-8050 97
4.2.2.2 Service Forwarding 101
4.2.2.3 SNMP Agent & Traps 107
4.2.2.4 SYSLOG Client 108
4.2.2.5 IP Communication Matrix SICAM A8000 CP-8031/CP-8050.....110
4.2.3 IP-based Protocols SICAM AK 3, SICAM BC, SICAM A8000 CP-8000/21/22113
4.2.3.1 IPSec VPN in SICAM A8000 Series / SICAM RTUs.....114
4.2.3.2 SNMP Agent & Traps 118
4.2.3.3 SYSLOG Client 119
4.2.3.4 IEC 62351-3 in SICAM A8000 Series / SICAM RTUs 120
4.2.3.5 EC 60870-5-104 with TLS-Encryption according to IEC 62351-3: Performance and Sizing 123
4.2.3.6 IP Communication Matrix 126
4.2.4 TCP Keep Alive 130
4.2.5 IEC 61850 – GOOSE 130
4.3 Other Layer 2 Communication Protocols 130
4.3.1 Secure Maintenance State 131

5 Patch Management 135

5.1 SICAM A8000 Series / SICAM RTUs 135
5.2 SICAM PTS Protocol Test System 135
5.3 SICAM TOOLBOX II 136
5.3.1 Live Update 136
5.4 SICAM Device Manager 137

6 Virus Protection 139

6.1 General 139

7 Encryption and Authentication processes 141

7.1 SICAM A8000 Series / SICAM RTUs 141
7.1.1 Engineering of SICAM A8000 Series via SICAM WEB 141
7.1.2 Diagnosis of SICAM RTUs Protocols via WEB-Browser 142
7.1.3 Engineering via SICAM TOOLBOX II/SICAM Device Manager 142
7.1.4 IPSec VPN in SICAM RTUs 143
7.2 SICAM TOOLBOX II 144
7.3 SICAM Device Manager 144

8 Backup & Restore 145

8.1 General 145
8.2 Data Backup 146
8.2.1 Automated Backup 147
8.3 Restore 148
8.3.1 Restoration of SICAM A8000 Series / SICAM RTUs 148
8.3.2 Restoration of the SD-Card of SICAM A8000 Series / SICAM RTUs 148
8.3.2.1 Direct Writing of the SD-Card by means of SICAM TOOLBOX II 148
8.3.2.2 Initialization and Loading of the AU by means of SICAM TOOLBOX II 149
8.3.2.3 SD-Card, Direct Writing via SICAM Device Manager 149
8.3.3 Restoration of the SICAM TOOLBOX II Data 149
8.3.4 Restoration of SICAM Device Manager Project Data 150

9 Logging 151

9.1 Security Logging 151
9.1.1 General 151
9.1.2 Supported Systems/Firmwares 152
9.1.3 Logged Security Events 153
9.1.3.1 Structure of Security Events 155
9.1.3.2 Syslog Events SICAM A8000 CP-8031/CP-8050 157
9.1.3.3 Syslog Events SICAM A8000 CP-8000/CP-802x / SICAM RTUs, SICAM Toolbox II 160
9.1.4 Configuration 167
9.1.4.1 SICAM A8000 Series / SICAM RTUs 167
9.1.4.2 SICAM TOOLBOX II 169
9.1.4.3 Viewing Logbook 170
9.2 Diagnostic 170
9.2.1.1 Diagnostic Functions 171
9.2.1.2 Diagnostic Classes 172
9.3 Logbook 173
9.4 Logging with the Windows Event Display 174

10 Remote Maintenance 177

10.1 Remote Maintenance via SICAM TOOLBOX II 177
10.1.1 Configuration of Servers and Clients 179

10.2 Remote Maintenance via SICAM Device Manager 179

11 User Administration 181

11.1 Introduction 181
11.2 SICAM A8000 Series / SICAM RTUs 182
11.2.1 SICAM A8000 Series 182
11.2.1.1 Roles 183
11.3 SICAM TOOLBOX II 184
11.3.1 Defining Users 184
11.3.1.1 Define Domain Users 185
11.3.2 Defining Roles 185
11.3.3 Assignment User <-> Role 186
11.3.4 Changing User Passwords 187
11.4 SICAM Device Manager 187

12 Hardware Interfaces 189

A Security Measure Plan for Oracle Database 191

A.1 Checklist according to “Security Measure Plan for Oracle Database 12c” 192

B Licensing agreement 195

B.1 Open Source Software Used in the SICAM A8000 Series 196

B.2 Open Source Software Used in SICAM RTUs 197

B.2.1 Readout of ReadmOSS.htm 197

B.3 Example of a ReadmOSS.htm: 200

Literature 201

1 Introduction

Contents

1.1 Objective 13
1.2 Observance of Standards 14
1.3 Security Requirements 14
1.4 Data Privacy Considerations 15

1.1 Objective

In the "good old days" as a rule computers were islands of functionality with little interconnectivity, if any at all. Today all computers - servers, Desktop-PCs and automation units are linked with each other. Although this creates new business opportunities, it also means, that these interconnected components can be attacked. Applications that are not designed for use in heavily networked environments are often attacked, because these were not designed for this.

The most important points for a SECURITY Administrator Manual are the increasing use of:

- Routable standard protocols, such as IP and TCP
- Connection of traditionally isolated networks (e.g. remote stations) and
- Standard software components such as OEM operating systems, such as Windows and Linux

This SECURITY Administrator Manual serves as a recommendation for the secure construction and operation of the SICAM RTUs in networked environments. It contains typical examples for the secure networking of telecontrol installations.

It should be taken into account by all those involved during the complete product life cycle:

- Product Management:
  Support for the consideration of the security functions through the understanding of the State-of-the-Art Network Design.
- System Test:
  Execution of test cases in setups as proposed, including security components such as Firewalls.
- Service / Project Personnel:
  Support / Guideline for the installation of IO-products at customer premises; Assurance of a secure network design (including configuration of security components such as Firewall Rules)
- Customer:
  Presentation of a "Security-Best-Practice" configuration as reference, for the documentation of the security awareness at SIEMENS.
- Bodies, that verify the conformity with standards (e.g. BDEW, NERC CIP)

Security must be an integral component of the development process. Security functions must be an integral part of the system design. The security planning at the forefront of the usage offers a more complete and more cost-effective solution. In addition expanded planning ensures that security services can be supported. This means, that the security must be addressed at all levels of the architecture for a cost-effective system solution.

1.2 Observance of Standards

Siemens offers products and technologies, which take into consideration leading Internet-Security-Standards. Major drivers for tested and secure infrastructures are the standards BDEW White Paper and NERC CIP (Critical Infrastructure Protection).

1.3 Security Requirements

What are the most important security requirements in your environment?

- Authentication and authorization of the users.
- Assurance of the integrity of the transmitted data.
- Every user is given only those rights that he needs to fulfill his work.
- Protection against virus infection and trojans.
- Hardening of the system, so that only those services and ports are activated, that are required for working and that the maximum network load is limited to the extent, that embedded systems can continue to work (e.g. limiting the number of broadcasts in the network components).
- Assurance, that in the case of a system crash, a restoration is possible without or only with marginal loss of data.
- Collection and saving of log files within a defined period.
- Operation of the system in a protected environment (physical security).

1.4 Data Privacy Considerations

Siemens considers data privacy aspects related to network operations while designing and developing SICAM A8000 Series. The consideration is reflected in the following technical measures which are realized in the SICAM A8000 Series.

Requirements	SICAM A8000 Compliance	Remarks
Access control to personal data in the products	comply	The device-internal security logbook contains information on security-relevant operations carried out by operating personnel. If RBAC is activated in the device, this logged information also indicates the login name of the person who carried out the operations. Access control in the device ensures that this security logbook can only be accessed by users who are authenticated and authorized as being in the role of a Security Auditor, a Security Administrator or an Administrator.
Compulsory use of passwords	comply	Access to person-identifiable security log information compulsorily requires the user in the role of a Security Auditor, a Security Administrator or an Administrator to log to the device with the correct password.
Encryption (of data at rest and data in motion) where proportionate	comply	Encryption of data is provided by the device in a manner that is the state-of-the-art in the substation automation market.
Automatic log-out functions	comply	The device automatically logs out logged in users after a deterministic time of inactivity.
Deletion possibility	comply	Security log entries can be deleted from the device by resetting the device to factory defaults. The local user cache can be deleted by either deactivating the local user cache feature in the device, by deactivating RBAC in the device, by resetting the security credentials and configuration settings of the device, or by resetting the device to factory defaults..
Two-factor authentication, if necessary	Not necessary	The device is not intended for direct access from a remote location, e.g. over the internet or otherwise unprotected networks. Therefore, two-factor authentication is not necessary, and this is the state-of-the-art substation automation market.

Additional product specific measures	Info	Person-identifiable information is only captured and stored in the device security log if the role-based access control (RBAC) feature is enabled. These log entries can be deleted from the device by resetting the device to factory defaults. Login information (username, password and role) of already logged in users is locally stored in the device only if this option (local user cache) is enabled by the customer while configuring the RBAC option. The local user cache can be deleted by either deactivating the local user cache feature in the device, by deactivating RBAC in the device, by resetting the security credentials and configuration settings of the device, or by resetting the device to factory defaults..

Hint

As the end-user of our products, you are hereby advised to consider your organization’s responsibilities towards fulfilling the GDPR requirements. For more information, please refer to article 25 of the GDPR: https://gdpr-info.eu/art-25-gdpr/

2 Typical Plant Configurations

Contents

2.1 General 17
2.2 Network Components 19
2.3 Typical Network Configurations 22

2.1 General

In this section you are given an overview of secure network configurations. Most systems are not standalone, rather are linked with each other over several network zones with different security requirements.

The following basic considerations for a secure network and communication structure have been included in the listed plant configurations and should be taken into account for the creation of a secure network and communication structure:

- Physical security / building protection
- Network segmentation in zones
- Communication within a zone
- Communication between the zones

Hint

The following chapters

- Building Protection
- Network Segmentation / Communication between the Zones
- Communication within a Zone
- Communication between the Zones

are adopted from the document *Oesterreichs Energie and DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN and VDE; Common Execution Instructions for the application of the BDEW White Paper*. They serve as an introduction for the following network configurations.

2.1.1 Object Protection

With the exception of WAN / long distance routes, technical networks should only be located within the inner security area of the physical object perimeter. Where technical systems are connected beyond these security areas, VPN use should be considered.

In case of insufficient physical or object protection, a manipulation of the SD-card content of the product family SICAM A8000 CP-8000/21/22 cannot be excluded.

However, reading out of sensitive data, such as passwords/preshared keys is not possible.

2.1.2 Network Segmentation / Communication between the Zones

Insofar as applicable and technically possible, the network structure on which the system is based is split up into zones with different functions and different protection requirements. Where technically possible, these networks zones are separated by firewalls, filtering routers or gateways. The communication with other networks must take place exclusively over communication protocols approved by the ordering party under observance of the valid security rules.

A physical separation of functional levels should be preferred over a logical separation. If a physical separation is not possible, the residual risk is to be evaluated. For the separation of networks the use of gateways that perform a protocol conversion and do not allow any direct IP-traffic should be checked.

2.1.3 Communication within a Zone

Security-related communication in the sense of the functional or plant security should only take place within closed network segments structured from dedicated hardware components. Possibilities for the configuration of the parameters of the functional or plant security via network accesses should be avoided in general. If these are absolutely necessary, they should only be accessible over the above mentioned closed network segments.

2.1.4 Communication between the Zones

For data interfaces to third party systems or internal networks and systems that are exposed to an increased extent to external security threats (e.g. an office LAN with Internet utilization, decentralized installations with reduced physical access protection etc.), the function of a DMZ should be provided.

For this the rule should always apply, that DMZ components must not have any access to internal system components in those zones with higher security level. The communication direction should always be directed from the higher security level to the lower.

Process Management / Control Systems and System Operation

Especially at network transitions of system-internal networks (e.g. control system LAN) to other internal networks and to WAN networks (e.g. for process coupling) a DMZ structure and the installation of firewall functionalities should be provided.

Transmission Technology / Voice Communication

Where possible the company’s own infrastructure should be used. With third party providers the observance of security standards should be contractually enforced and, if necessary verified. It should be checked, whether the communication in a third party network must be protected by an internally operated VPN.

Secondary, Automation and Telecontrol Technology

At transitions from local networks (e.g. station or plant LAN) to other networks (e.g. control centers or adjacent stations/plants) the installation of firewall functionalities should be provided.

A separation of different functions is to be generally recommended. Consequently, for process control applications, terminal and plant network should be realized with separate network components. The direct connection of protective devices to the general automation network should be avoided, if direct communication with other automation components is functionally not necessary. If necessary, segmentation with VLANs should be checked.

The direct coupling of different plants, systems and applications over a common plant network should be avoided. A system-overlapping access to components on the plant network should instead be realized over hardened gateway components.

2.2 Network Components

Network components can be roughly classified based on three features:

- Design and operating environment
- Type
- Management

As an example these features are listed here and briefly described.

2.2.1 Design and Operating Environment

In addition to the network components known in the “Office World” there are network components from a variety of manufacturers for use in industrial environments.

Some of these components are designed and approved for special purposes (switchgear, railway, ship …).

- Office
  - suitable for office environments and computer rooms
  - available as desktop devices or for 19” cabinet installation
  - standard temperature range (e.g.: 0 to 40°C)
- Industry
  - more robust designs, suitable for use in rough environments
  - frequently without fan
  - insensitive to dust and spray water
  - power supply with DC or AC voltage, optionally redundant
  - expanded temperature range (e.g.: -40 to 85°C)
  - available for rail assembly or for 19” cabinet installation
  - conform to industry standards e.g.: IEEE 1613, IEC 61850-3 for station automation
  - special functions, e.g.: support of IEC 61850 - GOOSE

2.2.2 Type

Type and functionality of a network component is derived from the network layers supported by the component, whereby a component working on Layer 2 (Layer-2 Switch) supports all “higher” protocols (layer 3-7), but does not “understand" them.

Example:

A switch operating on Layer 2 (Layer-2 Switch) can transmit an IEC 60870-5-104 data message over TCP/IP. However it can neither interpret the content nor can it transmit the corresponding packet beyond the IP network boundary.

For this it requires a network component located on a higher network layer. That can be a Layer-3 Switch, a Router, a Firewall but also a SICAM RTUs component (used as “Hardware-Based Application-Layer-Firewall”).

From the perspective of security, for the creation of a secure network and communication structure every network layer is to be considered and protected accordingly.

Hint

For simplification, in the following considerations and typical plant configurations, the protocol family “Ethernet – IP – TCP/UDP” used as standard in the automation technique is assumed, expanded with the IEC 61850-8-1 protocol for the transmission of IEC 61850 - GOOSE messages common in station automation. All exceptions (GPRS/UMTS, WLAN, ISDN, xDSL …) are specified explicitly.

List of the most frequently used transmission protocols:

OSI-Layer	TCP/IP-Layer	Protocol	Network Component
Applications (7)	Applications	IEC 61850, IEC 60870-5-104, DNP(i), NTP, SNMP, HTTP(s), RDP … (see also IP Communication Matrix, 4.2.3.6)	Hardware-Application-Layer-Firewall
Display (6)			
Session (5)			
Transport (4)	Transport	TCP, UDP	Firewall
Communication (3)	Internet	IP	Router Layer-3 Switch
Backup (2)	Network access	Ethernet IEC 61850 - GOOSE	Layer-2 Switch
Bit transmission (1)			Hub, media converter

List of the different types of network components:

- Media converter
  - OSI-Layer 1
  - Signal conversion between media, e.g.: conversion from Ethernet over copper cable to Ethernet over fiber optics cable
  - Enables it to switch between different transmission media (same speed)
- Hub
  - OSI-Layer 1
  - For the star-shaped connection of terminals
  - Used for the electrical signal distribution, no “Intelligence”
  - Enables it to switch between different transmission media (same speed)
  - ALL data packets are sent to ALL connected stations
  - For security reasons, should not be used in new installations
  - Replaced by Layer-2 Switch
- Layer-2 Switch
  - OSI-Layer 2
  - For the star- or ring-shaped connection of terminals over multiple hierarchies
  - First “intelligent” component in the OSI-Layer model
  - Enables it to switch between different transmission media (e.g. copper to fiber optic, also different speed)
  - Redundancy configurations possible
  - Data packets are not sent to all connected stations, rather only to the stations concerned
  - Prioritization of the data traffic is possible (e.g.: IEC 61850-GOOSE)
  - A physical device can be used to structure multiple networks or network segments, so-called virtual networks (VLAN).
- Layer-3 Switch
  - OSI-Layer 2+3
  - Features as Layer-2 Switch
  - IP Routing as additional feature
  - Redundancy configurations possible
  - Data packets are transmitted between IP networks based on their IP-address
- Router
  - OSI-Layer 3
  - Routing of a variety of protocols and media (Serial, Analog, ISDN)

  - Redundancy configurations possible
  - Data packets are transmitted between IP networks based on their IP-address
  - Often also with integrated or integrable Layer-2 Switch module
- Firewall – Basic
  - OSI-Layer 3-4
  - For the secure separation of network segments based on TCP/IP
  - Packet filter and/or Stateful Inspection Firewall
  - For the secure connection of protected network segments via Virtual Private Network (VPN)
- Firewall – Advanced
  - OSI Layer 3-7
  - For the secure separation of network segments based on TCP/IP or higher network level
  - Stateful Inspection Firewall
  - Application Layer Gateways

Hint

The types of network devices listed here and their functional limits are important for the clarification of the particular basic functionality and their use in typical plant configurations.

Frequently there are network components with overlapping functions, which expand one of the basic functionalities described e.g.: router with switchport, media converter with buffer for different rates ...

2.2.3 Management

The management of the network components is important, above all with redundant configurations (power supply, transmission route …), since a singular failure would otherwise remain undetected.

The failure of a redundant transmission route is not detected by terminals (e.g. SICAM RTUs), only with the failure of all communication routes do the terminals detect the failure of a connection.

Managed network components use the Simple Network Management Protocol (SNMP), to be able to be monitored and controlled from a central station.

- Managed
  - SNMP
  - Signaling contact, see note below
- Not managed
  - NO SNMP
  - Signaling contact, see note below

Hint

For simple diagnostic purposes industrial network devices frequently have one or more signaling contacts. These signaling contacts can be acquired and transmitted as sum information by means of SICAM RTUs.

With that, in many cases the acquisition of a “failure” or a “fault” of the network components is possible without expensive SNMP network management systems.

Diagnosis and the parameterization are carried out with tools provided by the manufacturer, not over SNMP.

2.3 Typical Network Configurations

The following examples show various network installations of SICAM RTUs systems. Remote stations can be widely distributed in the country, but are controlled from one central control center. The communication between control center and remote station often takes place over Wide Area Networks. The networks of the remote stations can be split up into various zones (e.g. process zone, automation zone), but only one individual zone is possible.

Hint

The specified example configurations serve as “building blocks” and can be used as a basis for a secure system design. They can support experienced network designers, but not replaced them!

List of the typical network configurations

- Overview
  - Control Center Zone and Substation Zone without VPN
  - Control Center Zone and Substation Zone with VPN
- Substation Zone
  - Substation Zone without segmentation with external firewall rules
  - Substation Zone with segmentation without internal firewall rules
  - Substation Zone with segmentation with internal firewall rules
  - Substation Zone with segmentation through “Hardware-Based Application-Layer-Firewall”
  - Substation Zone with Engineering Zone
  - Substation Zone with Out Of Band remote maintenance
- Control Center Zone
  - Control Center Zone without segmentation with external firewall rules
  - Control Center Zone with segmentation / Engineering Zone
  - Control Center Zone with Office Firewall
  - Control Center Zone with DMZ
  - Control Center Zone with Internet and Update DMZ

Legend of the network components used

	Router		Router with Firewall
	Layer-2 Switch		Layer-3 Switch
	Firewall		

2.3.1 Control Center Zone and Substation Zone without VPN

In this configuration the process network (Control Center Zone and Substation Zone) is only separated from the entire network by a router, the wide area network (WAN) is regarded as “secure”.

The entire process network is regarded as “secure”, between the process network and other networks (e.g.: Office-LAN, Internet) there are firewalls for network separation.

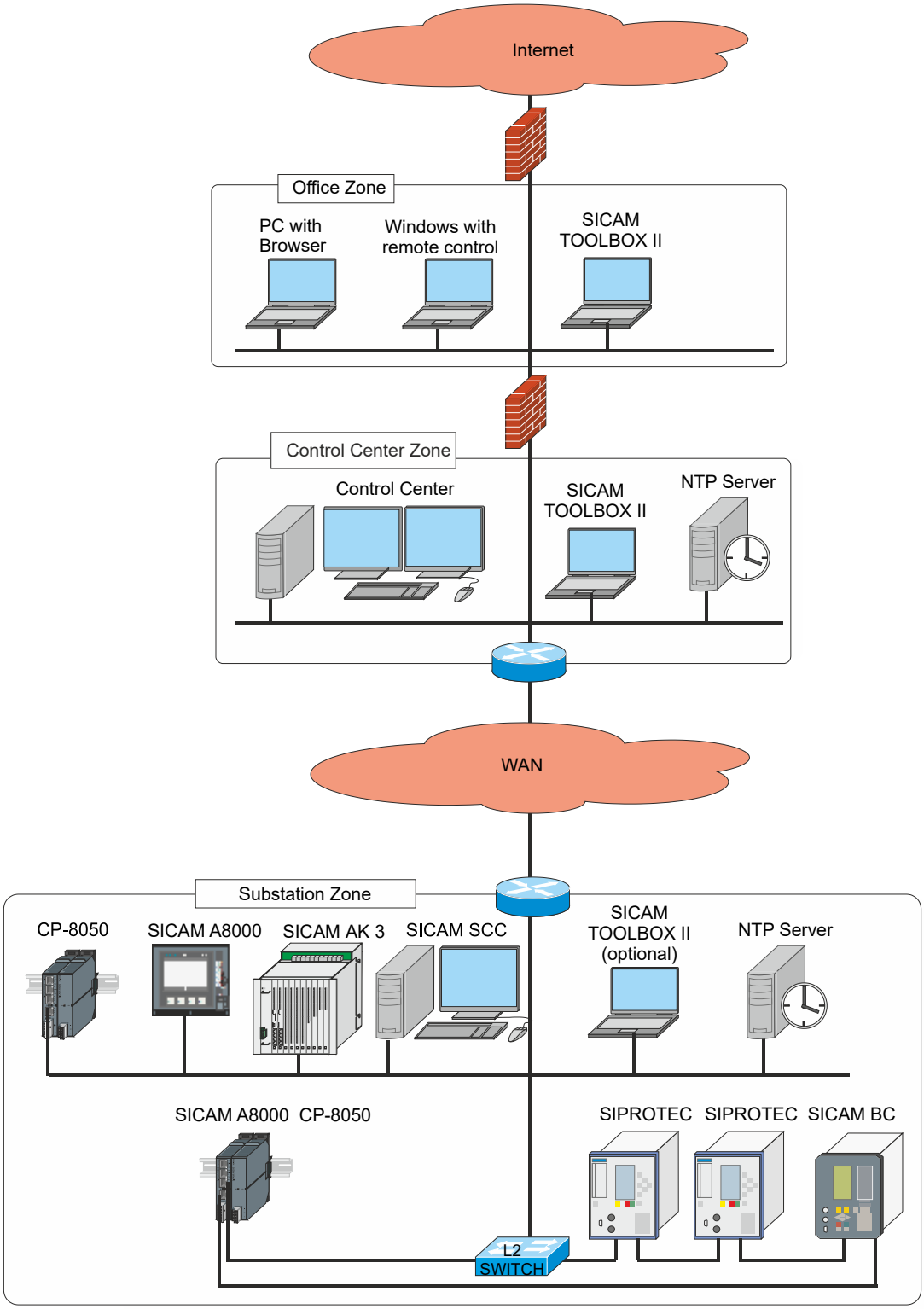
This configuration contains only one network segmentation into different IP network segments, every device in the WAN can communicate with every device in the Control Center or Substation Zone over the IP-Protocol.

Advantages:

- inexpensive
- simple

Disadvantages:

- no security measures at network level
- there are only security measures at the process network boundaries


Internet
Office Zone
PC with Browser
Windows with remote control
SICAM TOOLBOX II
Control Center Zone
Control Center
SICAM TOOLBOX II
NTP Server
WAN
Substation Zone
CP-8050
SICAM A8000
SICAM AK 3
SICAM SCC
SICAM TOOLBOX II (optional)
NTP Server
SICAM A8000
CP-8050
SIPROTEC
SIPROTEC
SICAM BC
L2 SWITCH

2.3.2 Control Center Zone and Substation Zone with VPN

In this configuration the process networks of the Control Center Zone and the Substation Zone are linked through a secure communication tunnel (VPN), security threats over the wide area network (WAN) are blocked by a firewall at the transitions to the Control Center Zone or the Substation Zone.

Control Center Zone and Substation Zone are regarded as “secure”. Within the zones there are no other security measures at network level.

All devices in the WAN can no longer communicate with all devices of the process network, however at network level there is no limitation of the communication possibilities between Control Center Zone and Substation Zone.

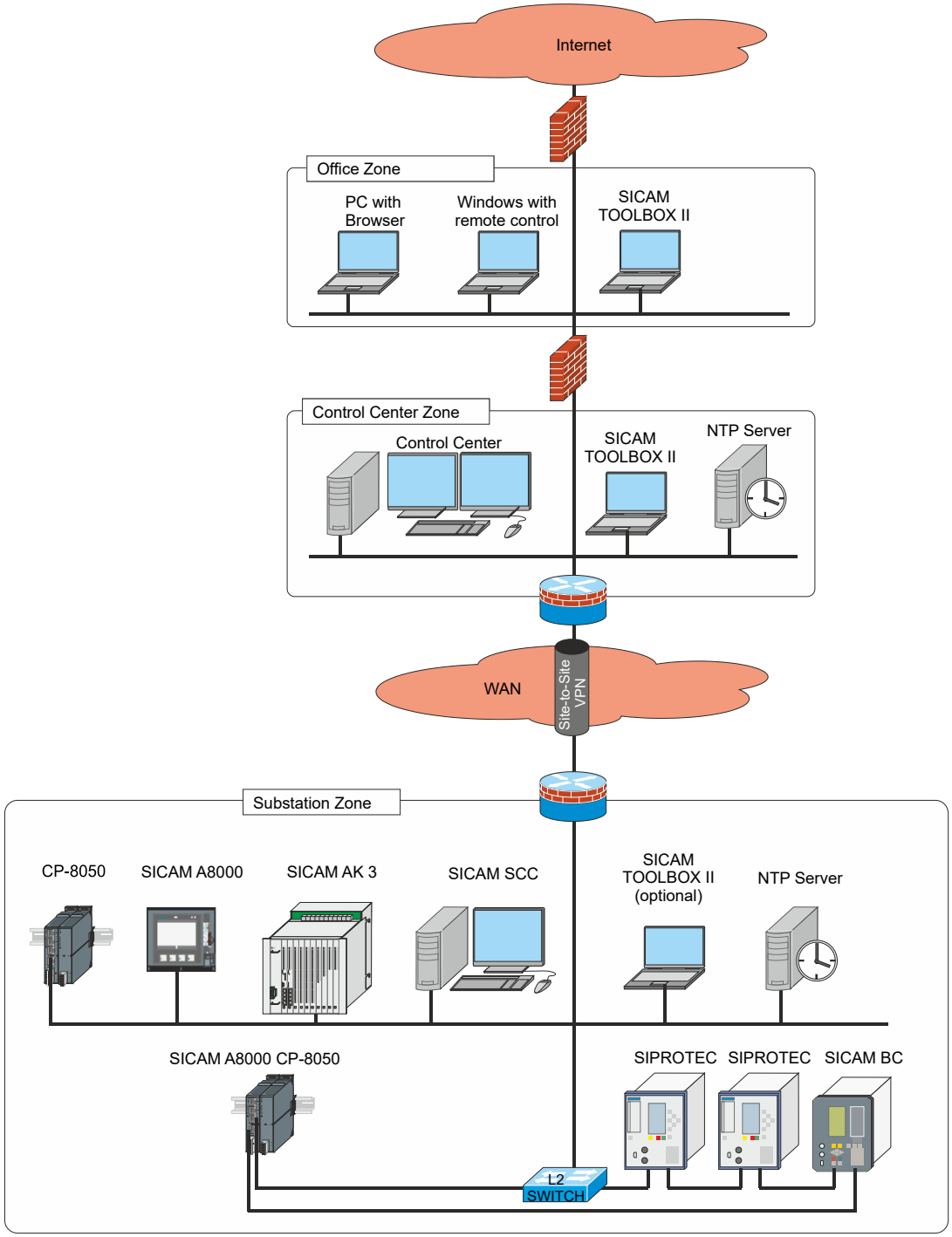
A further advantage of this configuration is the independence of the IP address space of the process network from the IP address space of the “wide area transport network” (WAN). Consequently the process network can be transmitted over other, possibly unsecure networks without coordination of the IP addresses. This technology is therefore also suitable for the transmission over public UMTS or Internet. (e.g.: also for secondary or standby transmission lines).

Advantages:

- “external” or ”unsecure” WAN is protected
- IP addresses must only be coordinated within the zones linked by means of VPN but not in the entire WAN
- simple
- only slightly more expensive
- possible cost saving for WAN-Provider, as only one IP address / one network connection is required

Disadvantages:

- little security within the Control Center and Substation Zone


Internet
Office Zone
PC with Browser
Windows with remote control
SICAM TOOLBOX II
Control Center Zone
Control Center
SICAM TOOLBOX II
NTP Server
WAN
Site-to-Site VPN
Substation Zone
CP-8050
SICAM A8000
SICAM AK 3
SICAM SCC
SICAM TOOLBOX II (optional)
NTP Server
SICAM A8000 CP-8050
SIPROTEC
SIPROTEC
SICAM BC
L2 SWITCH

2.3.3 Substation Zone without Segmentation with external Firewall Rules

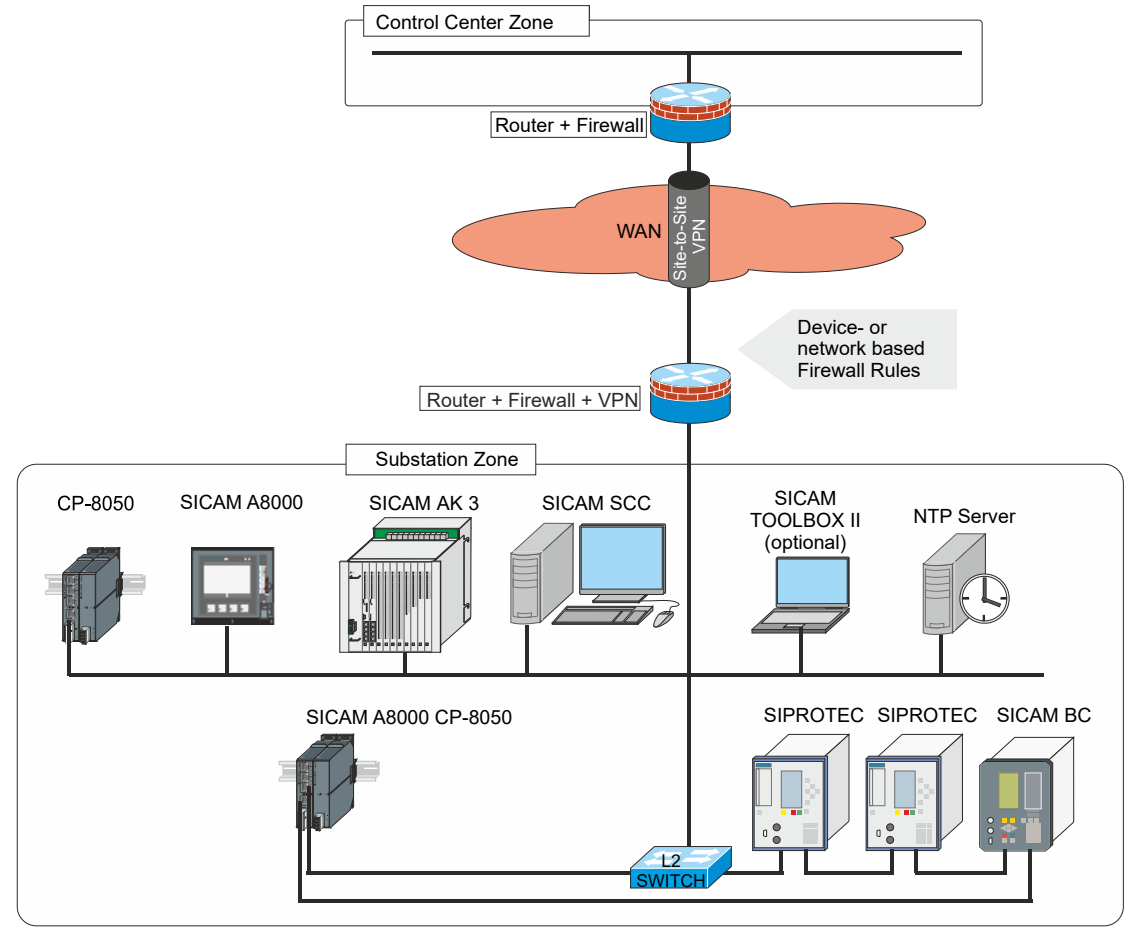
As an improvement to the preceding configuration the data traffic between Control Center Zone and Substation Zone can be restricted by means of device- or network-based Firewall Rules.

Advantages:

- Not every device of the Control Center Zone can communicate with every device of the Substation Zone

Disadvantages:

- Creation, implementation and maintenance of a “Traffic-Matrix” between Control Center Zone and Substation Zone
- More expenditure involved with equipment and changes
- Little security within the Control Center and Substation Zone



2.3.4 Substation Zone with Segmentation without internal Firewall Rules

As an improvement to the preceding configuration the data traffic within the Substation Zone can be split up into different Broadcast Domains.

This functionality can be achieved with VLANs (virtual LANs) or using Layer 3 devices (e.g.: Layer 3 Switch).

Hint

With Layer 2 devices with VLAN functionality the various VLANs cannot communicate with each other, for this they require Layer 3 functionality (Routing) or an external Layer 3 component (e.g.: Router or Firewall).

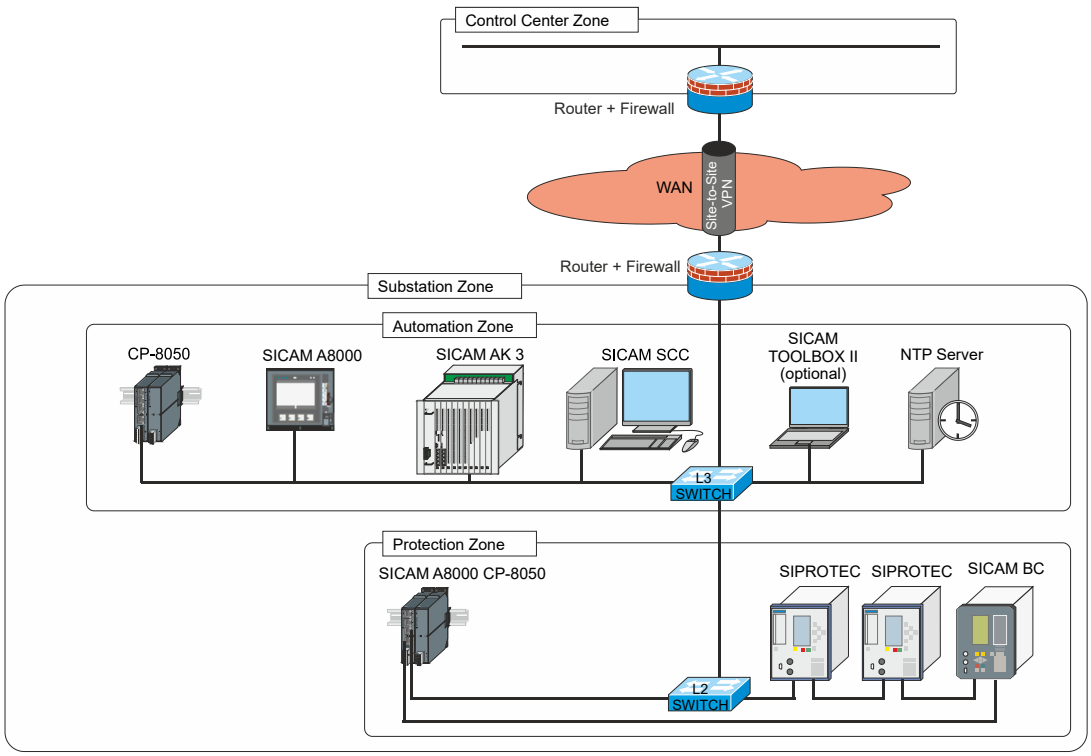
Consequently not every device sees the entire data traffic within the Substation Zone, devices with limited processor capacity are not burdened with data traffic of another Layer 2 segment (e.g.: GOOSE Traffic between protective devices in the Protection Zone does not burden the network segment Automation Zone).

Advantages:

- Different Broadcast Domains

Disadvantages:

- Costs of the Layer 3 devices / Layer 3 functionality



2.3.5 Substation Zone with Segmentation with internal Firewall Rules

In this configuration the data traffic within the Substation Zone is limited.

Consequently e.g. with an increased need for protection (from the perspective of security) it can be prevented, that a computer brought into the Automation Zone over an “easily accessible” network socket can reach a protective device locked in a cabinet over the network.

The network access for the parameterization and diagnostics of some or all protective devices in the Protection Zone could in this case be deliberately restricted to the local service interface.

Hint

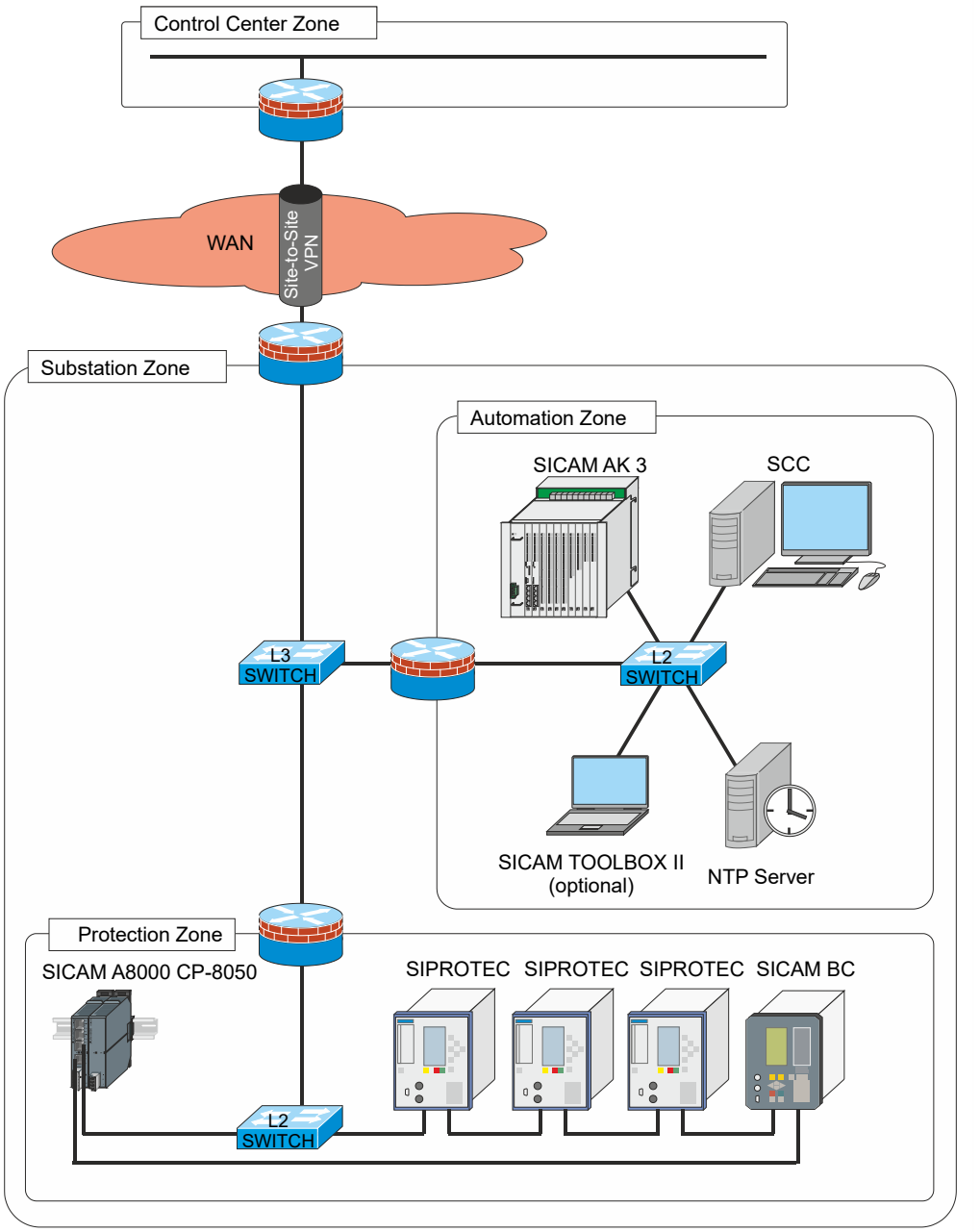
The “individual devices” (3 Firewalls, 1 Layer 3 Switch) specified in the configuration below are used to illustrate functionality.
Depending on the complexity required, this functionality can in most cases also be covered with one device.

Advantages:

- Network security also within the Substation Zone

Disadvantages:

- Costs of the firewall functionality
- Creation, implementation and maintenance of a “Traffic-Matrix” within the Substation Zone
- More expenditure involved with equipment and changes



2.3.6 Substation Zone with Segmentation through “Hardware-Based Application-Layer-Firewall”

If the specification “For the network separation the use of Gateways that perform a protocol conversion and do not allow any direct IP traffic should be examined.” (BDEW White Paper) is to be implemented, then no conventional network firewalls (Layer 3+4) can be used.

In this case SICAM RTUs/SICAM A8000 CP-8031/CP-8050-FWI4 (for mor details refer to *SICAM A8000 CP-8031/CP-8050 Manual*) can be used as a firewall, the data of one network interface are unpacked up to Layer 7 before they are packed again into IP packets at another network interface and forwarded.

Consequently e.g. with the use of a local control panel based on Windows Embedded, which should not be patched, SICAM RTUs could be used as “Hardware-Based Application-Layer-Firewall”.

Hint

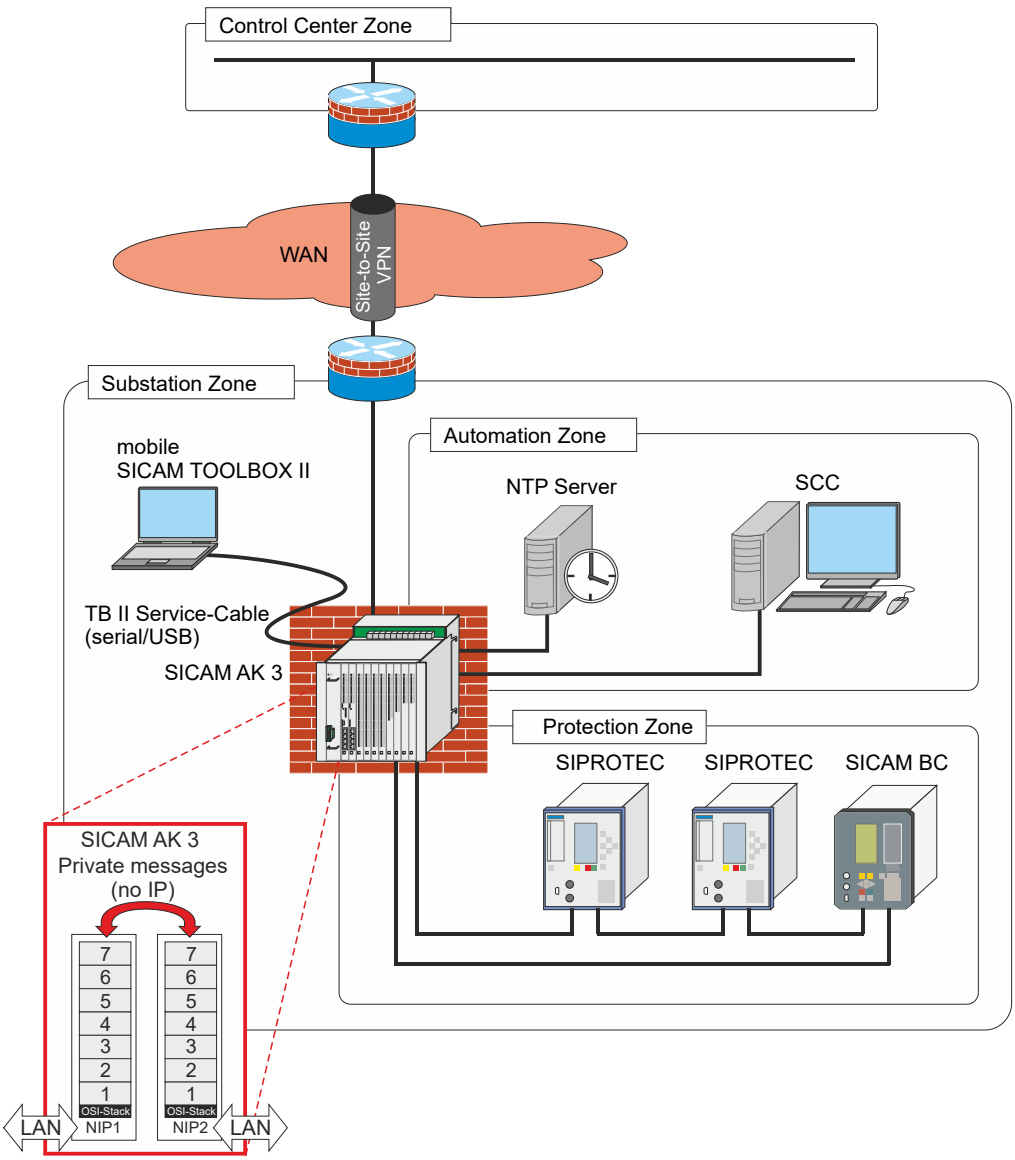
With the use of SICAM RTUs as “Hardware-Based Application-Layer-Firewall” only communication services supported by SICAM RTUs can be transmitted. Since through the “Hardware-Based Application-Layer-Firewall” no IP-Traffic is transmitted, no IP-based communication services function on devices situated behind the “Hardware-Based Application-Layer-Firewall”.

Advantages:

- Network security also within the Substation Zone
- No transparent IP-connection to devices “behind” the “Hardware-Based Application-Layer-Firewall”

Disadvantages:

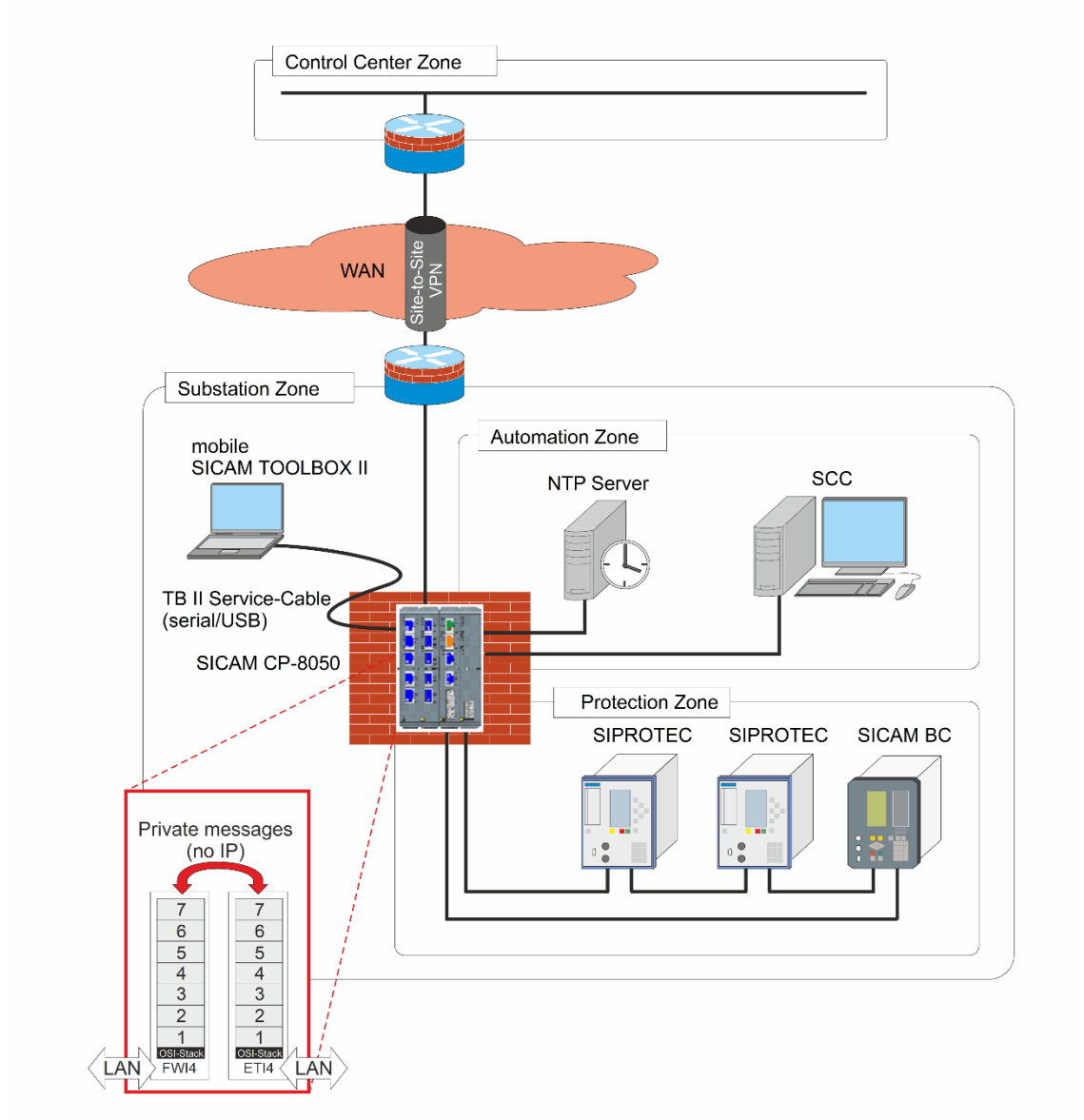
- Costs of the additional network interfaces
- Since no transparent IP-connection exists to devices “behind” the “Hardware-Based Application-Layer-Firewall”, limitations in the functionality can occur, e.g.: in the configuration specified above the local HMI-System cannot be accessed remotely.



Example: SICAM AK 3

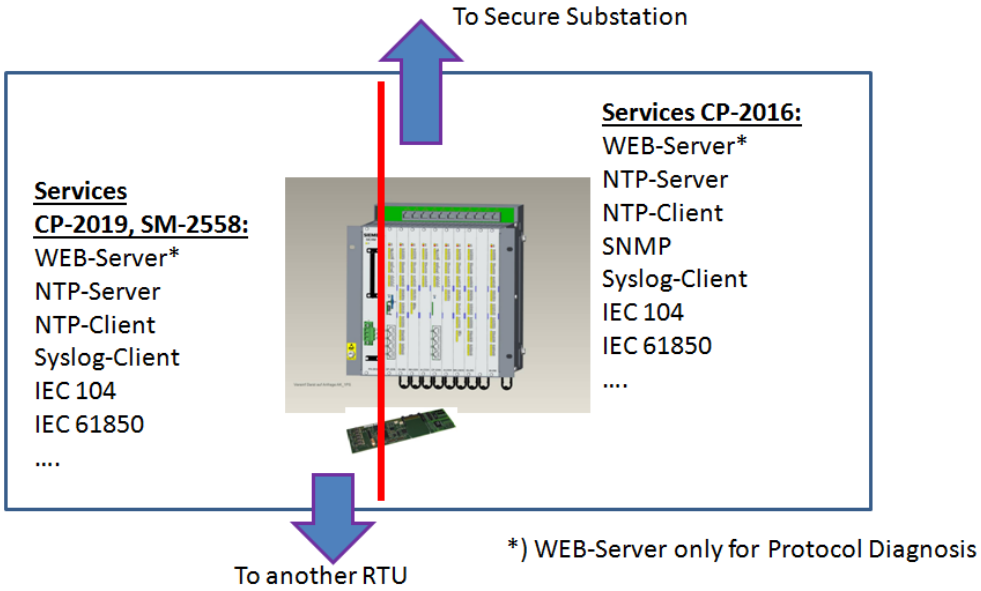
Hint

It is to be ensured when using a DUAL-NIP, that the Switch function does not represent any “Hardware-Based Application-Layer-Firewall”. Only when the data are transported over a further NIP is this an “Hardware-Based Application-Layer-Firewall” again.



Example: SICAM CP-8031/CP-8050-FWI4

Examples for “Hardware-Based Application-Layer-Firewall” in SICAM AK 3, (see also *IP Communication Matrix, 4.2.3.6*):



“Hardware-Based Application-Layer-Firewall” SICAM AK 3 with 1* M-CPU & 1* C-CPU/SM-2558

2.3.7 Substation Zone with Engineering Zone

This configuration introduces a separate zone for engineering devices.

Consequently it can be controlled which devices can reach an Engineering device used in the Substation Zone.

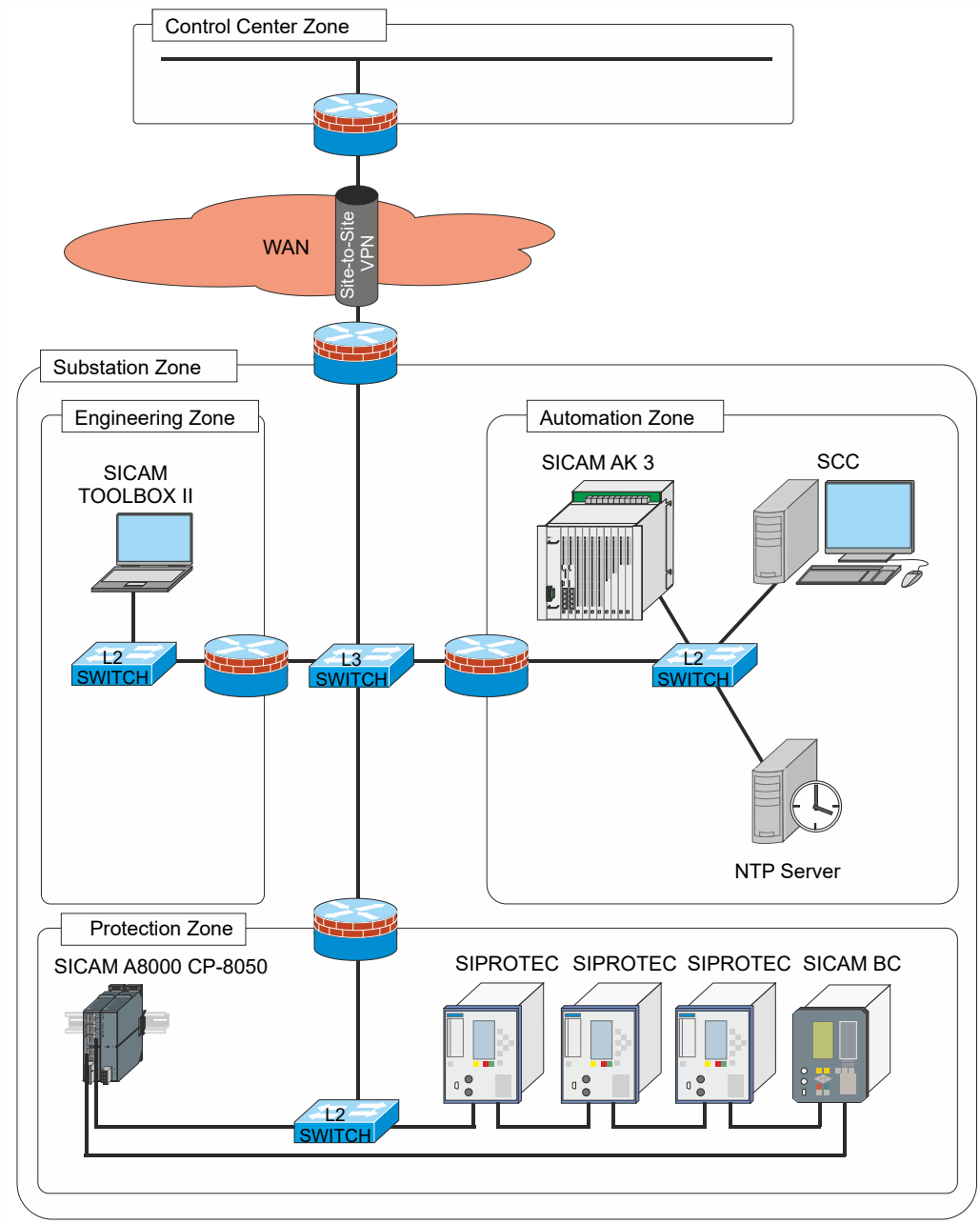
The Layer 2 Switch in the Engineering Zone could also be switched on/off with a key-operated switch; a signaling contact could report local engineering to the operating personnel (and the operating log).

Advantages:

- Control of the parameterization accesses in the Substation LAN
- Network-technical protection against “device accesses not authorized by operating personnel” possible

Disadvantages:

- Costs of the firewall functionality
- More expenditure involved with equipment and changes


Control Center Zone
WAN
Site-to-Site VPN
Substation Zone
Engineering Zone
SICAM TOOLBOX II
L2 SWITCH
L3 SWITCH
Automation Zone
SICAM AK 3
SCC
L2 SWITCH
NTP Server
Protection Zone
SICAM A8000 CP-8050
SIPROTEC
SIPROTEC
SIPROTEC
SICAM BC
L2 SWITCH

2.3.8 Substation Zone with Out Of Band Remote Maintenance

A clear separation between the “Process Data Stream” and the “Engineering Data Stream” should be achieved with the concept of “Out Of Band Remote Maintenance”.

With the interruption of all “Engineering Data Streams”, which is realized in the specified configuration by means of hardware (Switch is switched off, signaling contact indicates switched-on Engineering Data Stream), it can be almost excluded, that an attacker connects to a device in the Substation Zone without being noticed.

Now since the network of the Process Data Stream must not transmit any more Engineering Data (parameterization and diagnostics), the firewalls of the Process Data Stream can be parameterized more restrictive.

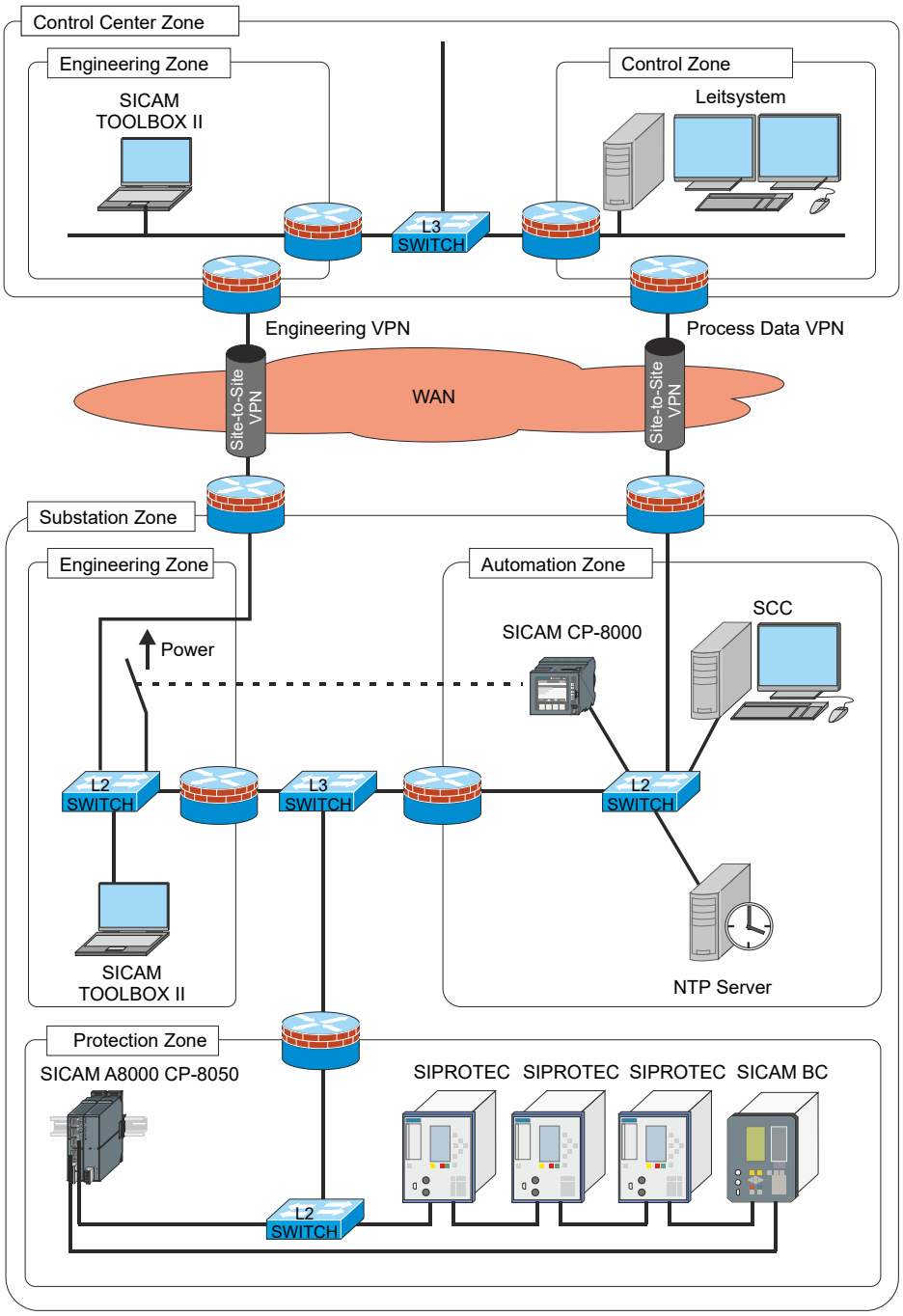
The use of “Hardware-Based Application-Layer-Firewalls” also becomes more practical, since the restriction of direct IP accesses for remote parameterization and remote diagnostics to devices behind the “Hardware-Based Application-Layer-Firewall” is dispensed with.

Advantages:

- Control of the remote parameterization accesses to the Substation LAN
- Network-technical protection against “device accesses not authorized by operating personnel” possible
- Simple, easily monitored solution: In comparison to more complex Firewall parameterization the power of a network component is simply switched off.

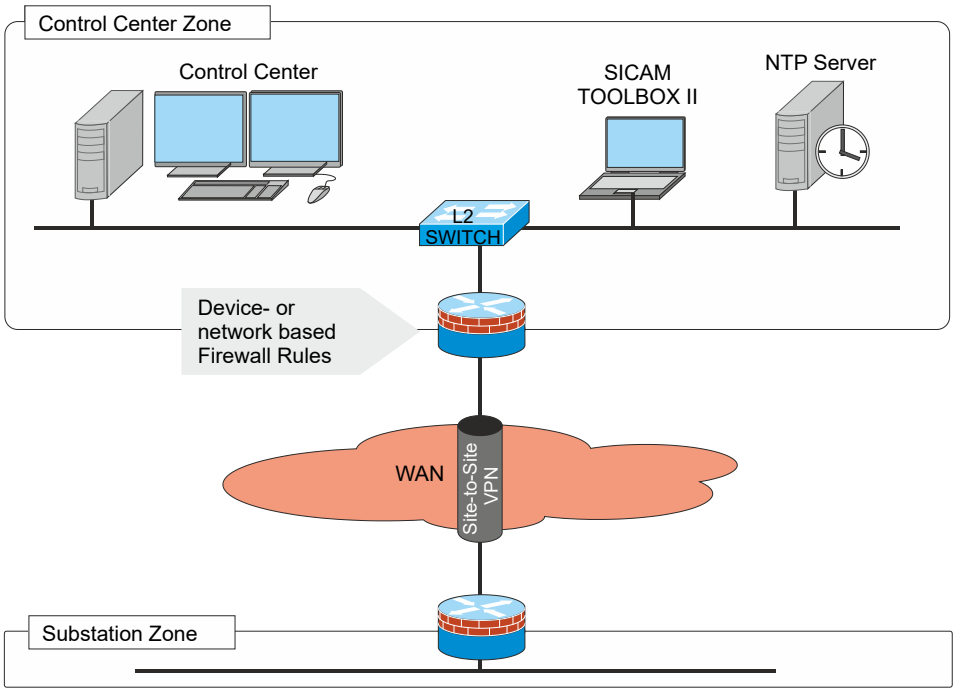
Disadvantages:

- Costs for the Firewall functionality
- Costs for the “Out Of Band” – WAN connection
- More expenditure involved with equipment and changes


Control Center Zone
Engineering Zone
SICAM
TOOLBOX II
Control Zone
Leitsystem
L3
SWITCH
Engineering VPN
Process Data VPN
Site-to-Site
VPN
WAN
Site-to-Site
VPN
Substation Zone
Engineering Zone
Automation Zone
SCC
SICAM CP-8000
Power
L2
SWITCH
L3
SWITCH
L2
SWITCH
SICAM
TOOLBOX II
NTP Server
Protection Zone
SICAM A8000 CP-8050
SIPROTEC
SIPROTEC
SIPROTEC
SICAM BC
L2
SWITCH

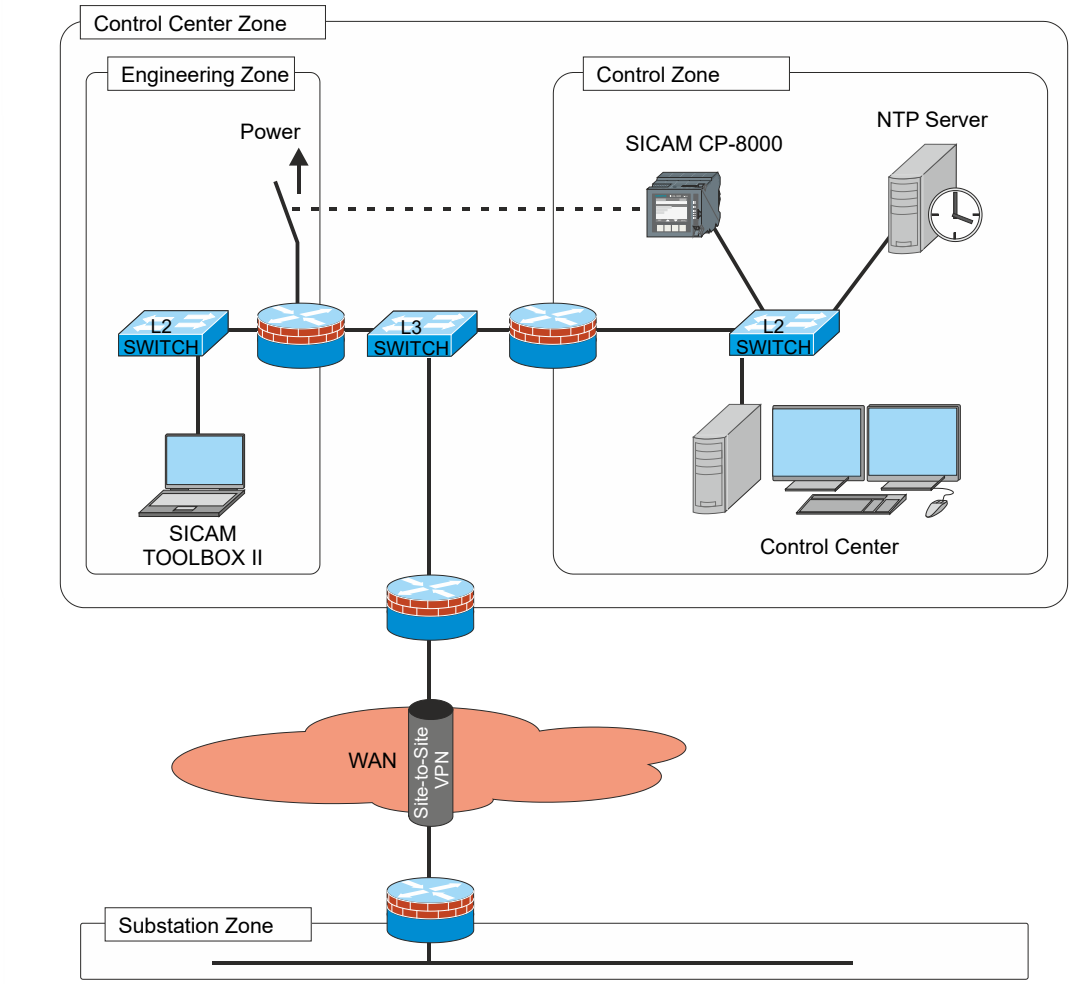
2.3.9 Control Center Zone without Segmentation with external Firewall Rules

Comparable with the solution for the Substation Zone.



2.3.10 Control Center Zone with Segmentation / Engineering Zone

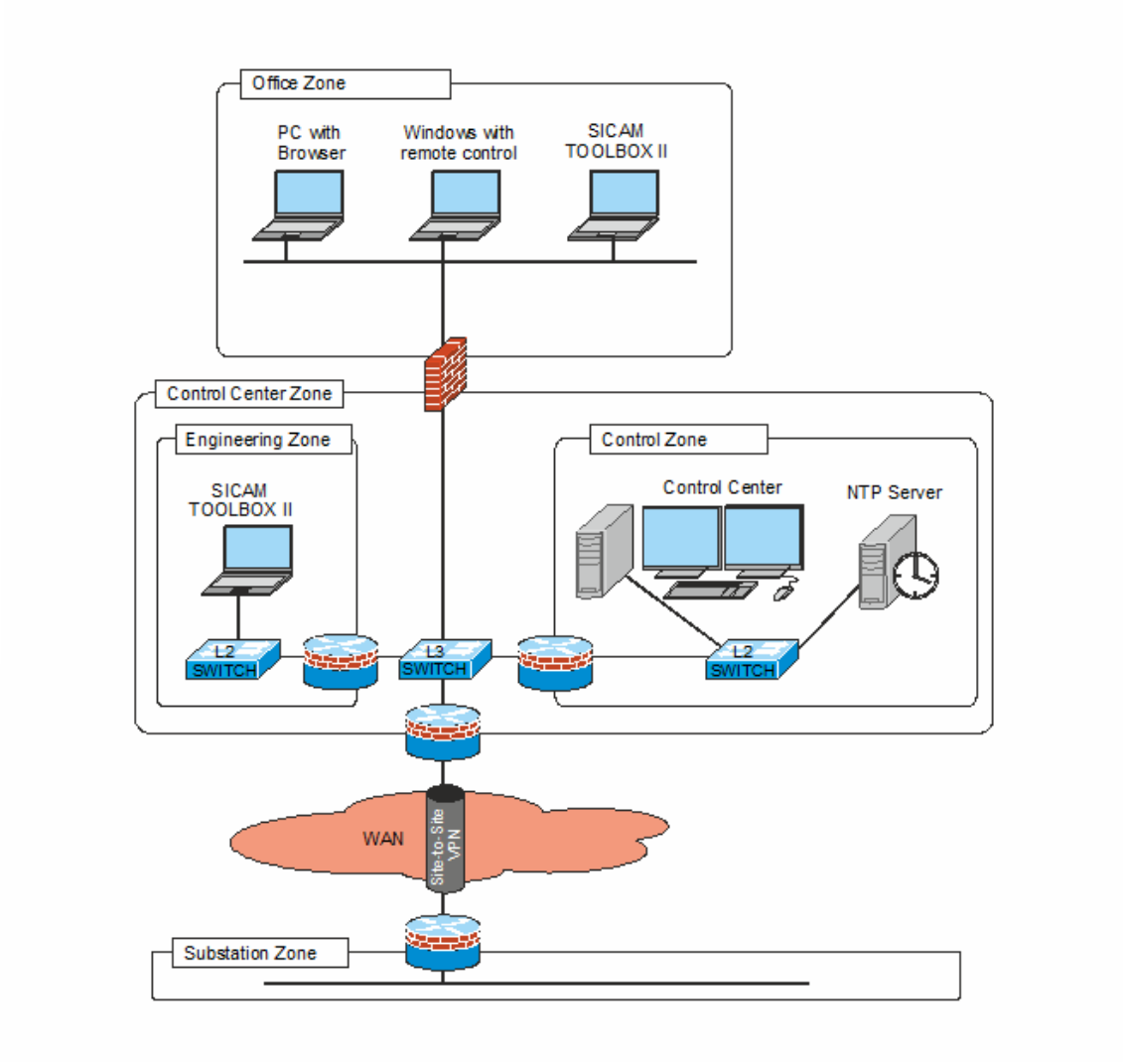
Comparable with the solution for the Substation Zone.



2.3.11 Control Center Zone with Office Firewall

The connection between Process Network and other “unsecure” networks is to be secured with a Firewall in all cases.

Consequently the data traffic between Office Zone and Process Network (Control Center Zone) can be restricted using device- or network-based Firewall Rules.



2.3.12 Control Center Zone with DMZ

As additional security measure a Demilitarized Zone (DMZ) can be inserted between Office Zone and Control Center Zone.

If technically possible, the connection setup must always take place from the secure zone in the DMZ.

Examples:

Data transfer between Control Center Zone and Office Zone via FTP:

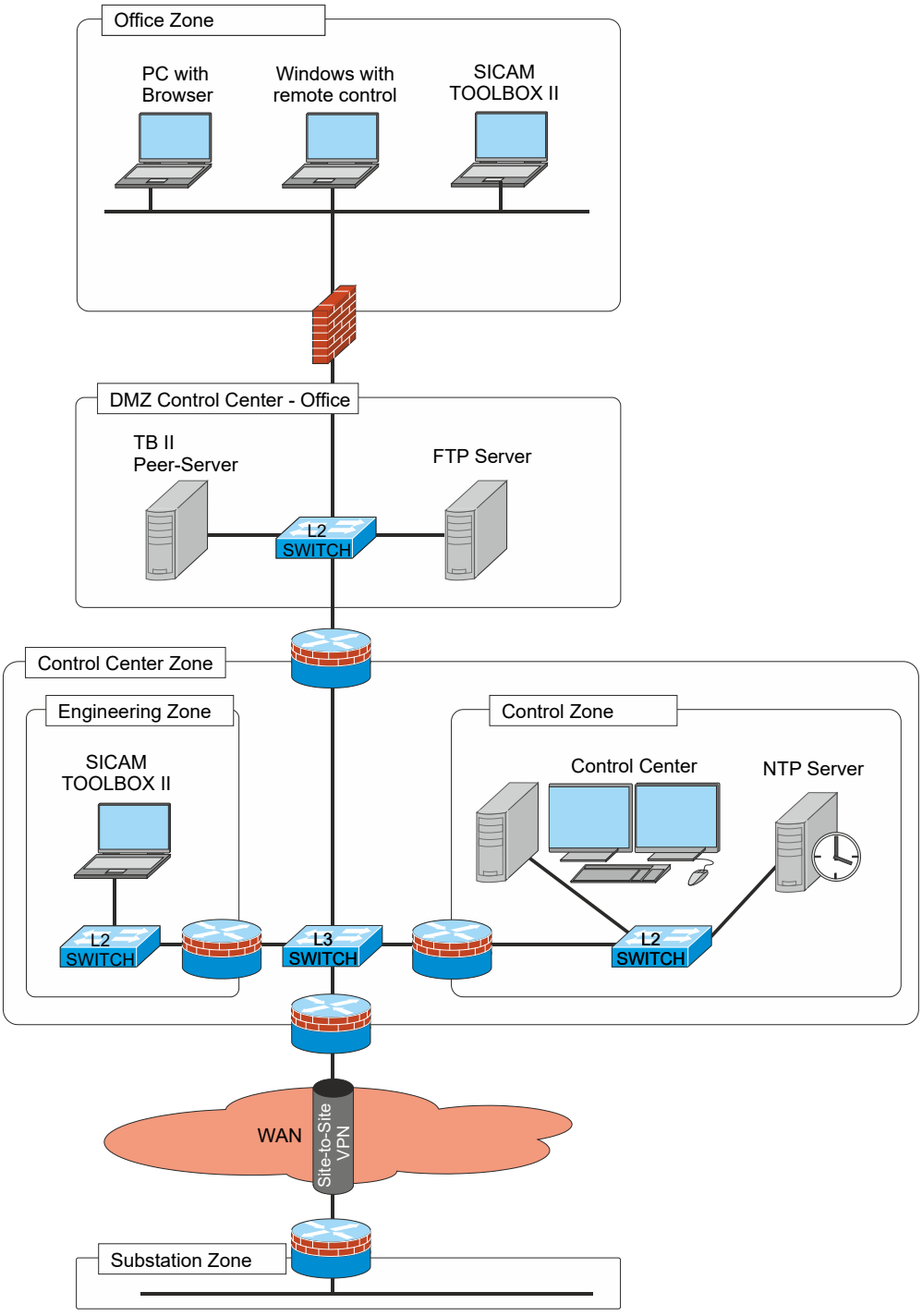
- Computer from the Control Center Zone saves data on FTP Server
- Computer from Office Zone fetches data from FTP Server
- Firewalls permit only passive FTP

Toolbox II Parameterization in Office:

- Toolbox II computer from Office Zone uses Toolbox II Peer Server in the DMZ
- The Toolbox II computer from the Office Zone cannot access the destination systems directly
- Toolbox II computer in the Engineering Zone uses Toolbox II Peer Server in the DMZ and loads the parameters into the destination system
- Firewalls only permit the two computers (IP addresses) access to the Toolbox II Peer Server on the required TCP-Ports (see documentation of the communication ports).

Remote Maintenance of Devices in the Process Network from the Office Zone via Terminal Server:

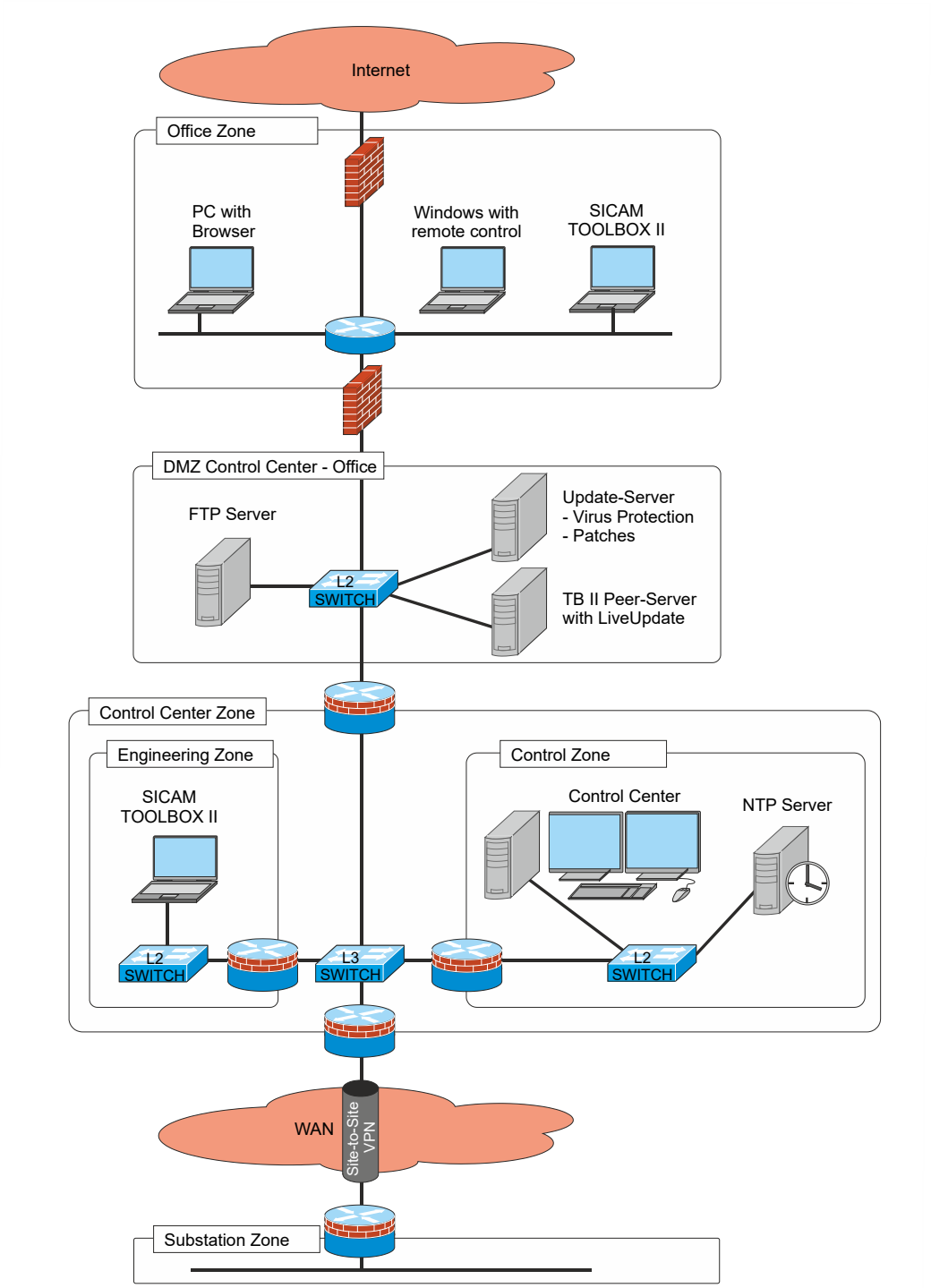
- Computer from the Office Zone establishes connection with Terminal Server in the DMZ via Remote Desktop Protocol (RDP).
- Terminal Server in the DMZ establishes RDP-connection with Toolbox computer in Control Center Zone
- Parameterization and download of the parameters into the destination system takes place from the Toolbox computer in the Control Center Zone


Office Zone
PC with Browser
Windows with remote control
SICAM TOOLBOX II
DMZ Control Center - Office
TB II Peer-Server
FTP Server
L2 SWITCH
Control Center Zone
Engineering Zone
SICAM TOOLBOX II
L2 SWITCH
L3 SWITCH
Control Zone
Control Center
NTP Server
L2 SWITCH
WAN
Site-to-Site VPN
Substation Zone

2.3.13 Control Center Zone with Internet and Update DMZ

In this configuration the DMZ between Office Zone and Control Center Zone is also used for the “distribution servers” for the process network-internal Virus Protection/Patch Management.

Patches and virus signatures are always downloaded by process network devices from these servers, never directly from the Internet (also not via proxies).



3 Measures for System Hardening

Contents

3.1 General 45
3.2 Supported LAN-Services 46
3.3 SICAM A8000 Series / SICAM RTUs 48
3.4 SICAM PTS Protocol Test System 91
3.5 SICAM Device Manager 91
3.6 SICAM TOOLBOX II 92
3.7 Security Penetration Testing 94

3.1 General

Definition of Term *[Source: Wikipedia]*

In computer technology one regards hardening as increasing the security of a system, by which only dedicated software is used, which is necessary for the operation of the system and its correct procedure under security aspects can be guaranteed. As a result the system should be better protected from external attacks.

The Federal Office for Information Security describes hardening in IT security as “[…] the removal of all software components and functions that are not absolutely necessary for the fulfillment of the intended task by the program.”

In practice the following have evolved as objectives of hardening measures:

- the reduction of the possibilities for exploiting vulnerabilities
- the minimization of the possible methods of attack
- the limitation of an attacker, following a successful attack, to available tools
- the minimization of an attacker, following a successful attack, to available privileges
- the increasing of the probability of detection of a successful attack

A possible reduction of the complexity and the maintenance work of the system can also be regarded as a secondary objective of hardening, which can lead to a greater manageability and therefore a minimization of administration errors.

3.2 Supported LAN-Services

3.2.1 Services integrated on the Basic System Element

CP-8031/CPCI85	CP-8050/CPCI85	CP-8000/CPC80 CP-8021/CPC80 CP-8022/CPC80	CP-2016/CPCX26	CP-2019/PCCX26	Services	Protocols
X	X				One Click To Connect (OCTC)	DHCP
		X			Autoconfiguration	DHCP
X	X	X			Autoconfiguration	DNS
X	X	X	X	X	time synchronization	(S)NTP
X	X				time synchronization	NTP(S)
X	X	X			SICAM WEB/SWEB	HTTP(S)
X	X	X			SICAM Device Manager	HTTP(S)
X	X	X	X	X	SICAM TOOLBOX II Remote Operation	HTTP(S)
X	X	X	X		SNMP: as of CPCI85 V1.10	SNMP
X	X	X	X	X	IPsec VPN: as of CPCI85 V3.00	IPSec VPN
X	X	X	X	X	Syslog-Client	Syslog
X	X	X			Radius	Radius
		X			Autoconfiguration	FTP/TFTP
		X			PPP*)	PPP*)
X	X				LDAP User authentication as of V3.00	LDAP
X	X				IEEE1588 ordinary clock	PTP
SICAM A8000			SICAM AK 3			

*) PPP is part of the firmware CPC80, but used in SICAM A8000 CP-8022 only.

3.2.2 Services integrated on the Protocol Element

CP-8031/CPCI85	CP-8050/CPCI85	CP-8000/CPC80 CP-8021/CPC80 CP-8022/CPC80	CP-2016/CPCX26	CP-2019/PCCX26	CP-2017/PCCX25	CP-5014/CPCX55	PRE	Services	Protocols
-	-	-	x	x	-	-	ET24	IEC 60870-104	IEC 60870-104
-	-	-	x	x	-	-	ET25	IEC 61850 Ed.2	IEC 61850 Ed.2
								Web-Server (WEB-page) *)	HTTP(S)
-	-	-	x	x	x	x	SM-2558/ETA3	NTP	(S)NTP
								SICAM TOOLBOX II Remote Operation	HTTP(S)
								Web-Server (WEB-page) *)	HTTP(S)
								IEC 61850 Ed.1	IEC 61850 Ed.1
-	-	-	x	x	-	x	SM-2558/ETA4	NTP	(S)NTP
								SICAM TOOLBOX II Remote Operation	HTTP(S)
								IEC 60870-104	IEC 60870-104
								IPSec VPN	IPSec VPN
								Syslog	Syslog-Client
-	-	-	x	x	x	x	SM-2558/ETA5	NTP	(S)NTP
								SICAM TOOLBOX II Remote Operation	HTTP(S)
								Web-Server (WEB-page) *)	HTTP(S)
								IEC 61850 Ed.2	IEC 61850 Ed.2
-	-	-	x	x	x	x	SM-2558/MBSiA0	MODBUS TCP/IP Slave	MODBUS TCP/IP
								SICAM TOOLBOX II Remote Operation	HTTP(S)
-	-	-	x	x	x	x	SM-2558/MBCiA0	MODBUS TCP/IP Master	MODBUS TCP/IP
-	-	-	x	x	x	x	SM-2558/DNPiA0	DNP3 TCP/IP Slave	DNP3 TCP/IP
								SICAM TOOLBOX II Remote Operation	HTTP(S)
-	-	x	-	-	-	-	ET83	IEC 61850 Ed.1	IEC 61850 Ed.1
								Web-Server (WEB-page) *)	HTTP(S)
-	-	x	-	-	-	-	ET85	IEC 61850 Ed.2	IEC 61850 Ed.2
								Web-Server (WEB-page) *)	HTTP(S)
-	-	x	-	-	-	-	ET84	IEC 60870-104	IEC 60870-104
x	x						ETI4	IEC 60870-104	IEC 60870-104
x	x						ETI5	IEC 61850 Ed.2	IEC 61850 Ed.2
								Web-Server (WEB-page) *)	HTTP(S)
SICAM A8000			SICAM AK 3			SICAM BC			

*) Some SICAM RTUs protocols and some SICAM A8000 protocols support a WEB server for diagnostic purposes (access via WEB browser). Authentication for these WEB pages is not provided for.
Therefore, for normal operation this possibility of access should be deactivated via parameterization.

3.3 SICAM A8000 Series / SICAM RTUs

Included among the hardening measures to be applied with SICAM A8000 Series / SICAM RTUs:

- Deactivation of unnecessary system and communication services (remote operation, remote maintenance, NTP, WEB…)
- Deactivation of unnecessary standard users (WEB)
- Activation of configuration options that increase security
- Measures for restricted distribution of system messages

3.3.1 Digital signatures

SICAM A8000 Series

A digital signature check for all firmwares will be performed if at least the following firmware revisions for the master module are loaded:

Firmware	Digitally signed
CPCi85	from revision 01
CPC80	from revision 12

Hint

After an update of **CPC80** to revision **12** or higher it is not possible any more to load not digitally signed firmware versions.

After an update of **CPC80** to revision **12 or higher** it is not possible to load an earlier firmware version (e.g. CPC80 REV 11 or lower).

CPC80 REV 11 or lower also support digitally signed firmwares of all other modules.

Firmware signatures are implemented in the respective firmware revisions for **SICAM A8000 Serie CP-8000 / CP-802x**, see table below:

Firmware of SICAM A8000 Series CP-8000 / CP-802x	Digitally Signed Revisions
103MT0	05.01
AGPMT0	01.01
BMCUT0	02.01
BPPT0	03.02
COUMT0	03
DIAST0	03.01
DNPiT1	01.01
DNPMT0	01.01
DNPST0	04.01
ET83	02.05
ET84	04.01
ET85	03.04
MODMT0	03.01
MODMT2	03.01
MODST0	02.01
PCBST0	02.01
RP5UT1	02.01
SMST0	03.01
ST1ST0	03.01
TG8ST0	02.01
UMPMT0	02.02
UMPST0	06.01

Hint

It is strictly recommend to update all firmwares during update of CPC80 to revision12 or higher.

An update of the affected firmware is possible at any time using all known possibilities if not yet digitally signed firmwares (due to a not performed or not completed update) exist in the device and if a the respective system element is not in the ready status (RY):

- Loading via SICAM TOOLBOX II
- Loading via SICAM Device Manager
- Generating SD-card via SICAM TOOLBOX II
- Copying of firmware binary files into IN-Directory of SD-card.

SICAM AK 3:

A digital signature check for all firmwares will be performed if at least the following firmware revisions for the M-CPU are loaded:

Firmware	Digitally signed
CPCX26	From revision 04

Hint

After an update of **CPCX26** to revision **04** or higher it is not possible any more to load not digitally signed firmware versions.

After an update of **CPCX26** to revision **04** or higher it is not possible to load an earlier firmware version (e.g. CPCX26 REV 03 or lower).

CPCX26 Revision 03 or lower will continue to support all firmware updates of all other system elements.

CPCX26 revision 04 supports digitally signed firmwares for protocol, basis and periphery system elements only and/or all firmwares listed in the whitelist filter.

The following table contains all firmwares of the whitelist filter of CPCX26 REV 04.

The lowest version of all firmwares compatible with CPCX26 REV 04 is listed in the table. Older versions are not supported!

Whitelist-Filter of SICAM AK 3 (CPCX26 REV 04)							
Firmware	**Revision**	**Firmware**	**Revision**	**Firmware**	**Revision**	**Firmware**	**Revision**
102MA0	02	ENOS00	07	PCCO27	08	TCIO66	02.04
102SA9	01	ERAC00	07	PCCX25	11.02	TEDA01	02.03
103M00	15	ET01	13.01	PCCX26	03.01	TEDAA1	01.01
103MA0	10.01	ET02	15.06	PWSSA0	02	TEMP25	02.02
103S00	04	ET03	07.14	R51201	02.05	TF2551	02
103SA0	06	ET24	02.02	R512A1	02.01	TFTSA0	02
8TKSA0	01	ET25	03.06	RP5U01	06.07	TG8M00	05
AGLiA0	01	ETA2	11.01	RP5UA1	02	TG8MA0	06
AGPMA0	01	ETA3	02.04	RP5Z01	02.10	TG8SA0	06
AX2541	06	ETA4	08.03	RP5ZA1	01	TIPP16	01.16
BDKMA0	04.01	ETA5	03.06	SA8K00	01	TIPS05	03.06 03.07 [1)]
BDKS00	03	ETLS00	02	SA8M00	12.04	TLSM00	02
BDKSA0	03	F537A0	02	SA8MA0	04.02	TLSMA1	04
BISI15	06	G21E00	01	SA8S00	14	TRA00	03
BISI25	06	G74S00	05.02	SA8SA0	01.01	TRET00	23.02
BISI26	04	GACMA0	01	SEAB01	05.01	UMPM00	10.04
BISO25	02.03	HUGM00	02.03	SEAB02	02	UMPM01	07
BISX26	01.03	I21S00	07	SEAB03	09	UMPM02	18.01
BPP00	19	I21U10	03	SEAB04	01.02	UMPM98	01
BPP99	02.05	I21Z10	03	SEAB05	01	UMPMA0	06.01
BPPA0	10	I33SA0	01.01	SEAB06	01	UMPMA1	08
BPPA9	01.01	I35M00	02.04	SEABA3	01	UMPS00	23
CDCM00	01.01	ILSMA0	01	SFBMA1	03	UMPS01	07
COUM00	06.01	JN2M00	02.02	SFBSA1	03	UMPS99	03.01
COUMA0	06.02	LSAMA0	04.02	SIFUA0	01	UMPSA0	05.07
DIAM00	16	M2AS00	05	SKEE11	05	USIO15	07
DIAM99	03.01	M2AS01	08	SKEEA1	02.01	USIO26	05
DIAMA0	05	M3AS00	05.02	SKSZA0	03	USIO27	05

DIAMA1	03	M3AS01	01	SMAMA0	00.50	USIO65	10
DIAMA8	02	MBCiA0	01	SMIM00	04	USIO66	05.05
DIAS00	14.03	MBSiA0	01	SMIMA0	01	VEZA0	01
DIASA0	03.03	MOCZ00	01.01	SMS00	01.01		
DISR00	03	MODi00	02.04 02.05 [1)]	SMSA0	03		
DLTM00	00	MODM00	05.02	SPAM00	09		
DNPi00	02.02	MODMA0	05	SPAMA0	03		
DNPiA1	01	MODS00	04	SPLC01	01, 02, 02.01, 02.02		
DNPM00	08.01	MODS01	02.04	ST1M00	02.01		
DNPMA0	06	MODSA0	04	ST1MA0	02.01		
DNPSA0	06	OMV01	03.02	ST1SA0	02		
DP4S00	04	OX2501	01.03	ST7M00	04.01		
DPM00	08.02	PASI25	08.02	ST7MA0	01		
DPMiA0	02	PCBMA0	05	T20M00	02		
DSFGA0	04.07	PCBSA0	02.02	T29M00	03		
DSFGS0	05.03	PCCE25	21.01	T65MA0	01		
DSFGS1	04.03	PCCO26	08	TCIO65	08.04		

[1)] from CPCX26 REV 04.04

Hint

It is strictly recommend to update all firmwares during update of CPCX26 to revision 04 or higher.

For security reasons, an update of all firmwares to digitally signed firmwares or an update to a version of the whitelist fillter is recommended.

After the update of the M-CPU to a digitally signed firmware version , a downgrade (loading of not digitally signed version) is ruled out.

An update of the affected firmware is possible at any time using all known possibilities if not yet digitally signed firmwares (due to a not performed or not completed update) exist in the device

- Loading via firmware loader of SICAM TOOLBOX II
  or
- Generating SD-card via OPM of SICAM TOOLBOX II

SICAM BC: there is no digital signature check of firmware.

SICAM TOOLBOX II / SICAM Device Manager installer is digitally signed.

3.3.2 Deactivation of Unnecessary System and Communication Services

3.3.2.1 One Click to Connect (SICAM A8000 CP-8031/CP-8050)

Via the Ethernet interfaces the engineering PC (SICAM TOOLBOX II, SICAM WEB) has to be connected to the device SICAM A8000 CP-8031/CP-8050 using a standard patch cable.

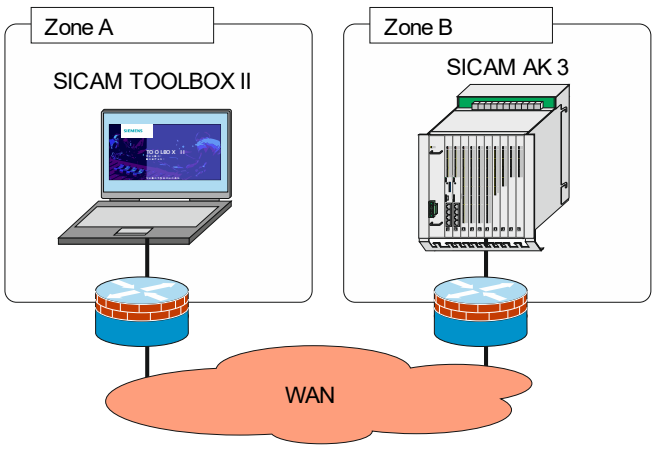
The PC hast to be configured as DHCP Client, and the AU has to be configured as DHCP Server.

The feature "One Click to Connect" of SICAM A8000 CP-8031/CP-8050 supports all SICAM TOOLBOX II functions (incl. AE initialization).

For configuration, enabling of DHCP, assignment of IP-addresses and login to the AU, refer to *SICAM A8000 CP-8031/CP-8050 Manual.*

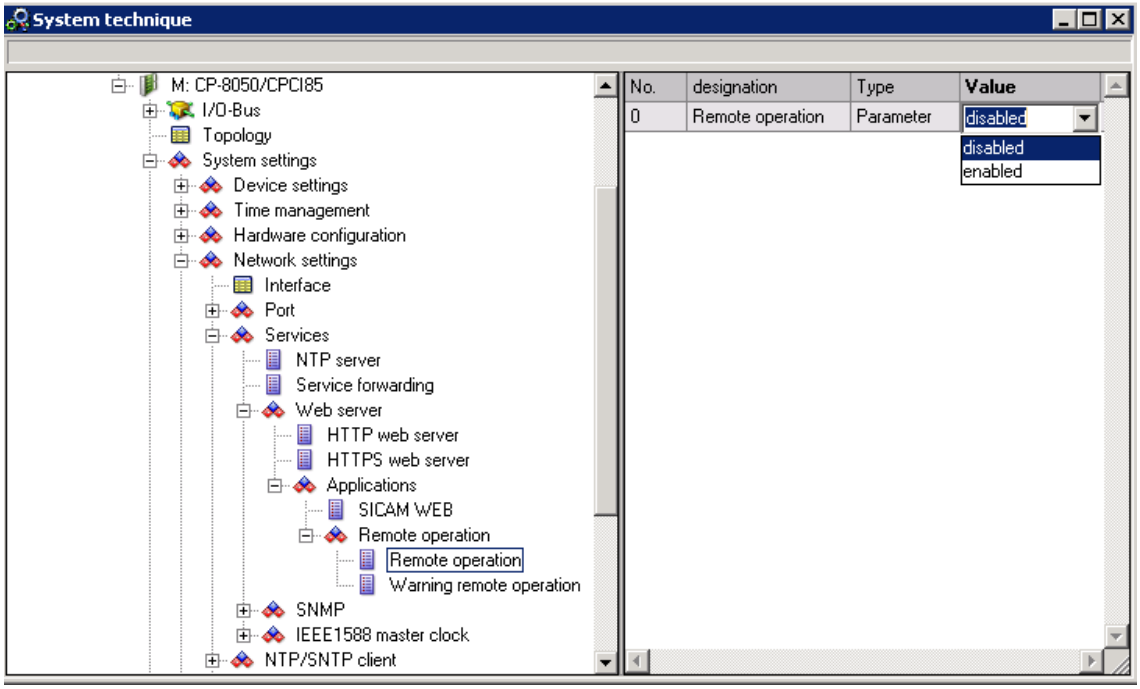
3.3.2.2 Remote Operation

In remote operation, SICAM TOOLBOX II / SICAM Device Manager does not connect with a SICAM RTUs by means of a local parameterization cable, rather over a network interface by means of TCP/IP (with activated Listener Service in SICAM RTUs).

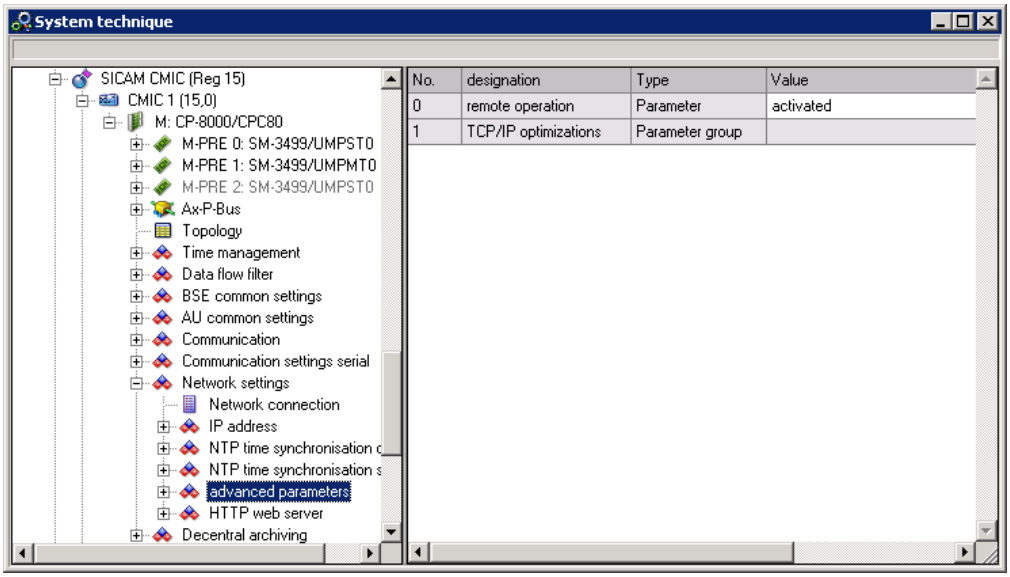


With LAN protocols the remote operation is deactivated by default in SICAM RTUs. If necessary this can be activated individually.
The corresponding parameter `Remote Operation` can be found in the system-technical parameter setting either on the BSE (e.g.: CPC80, CPCX26, PCCX26, CPCI85) or PRE (e.g.: ETA3, ETA4, ETA5).

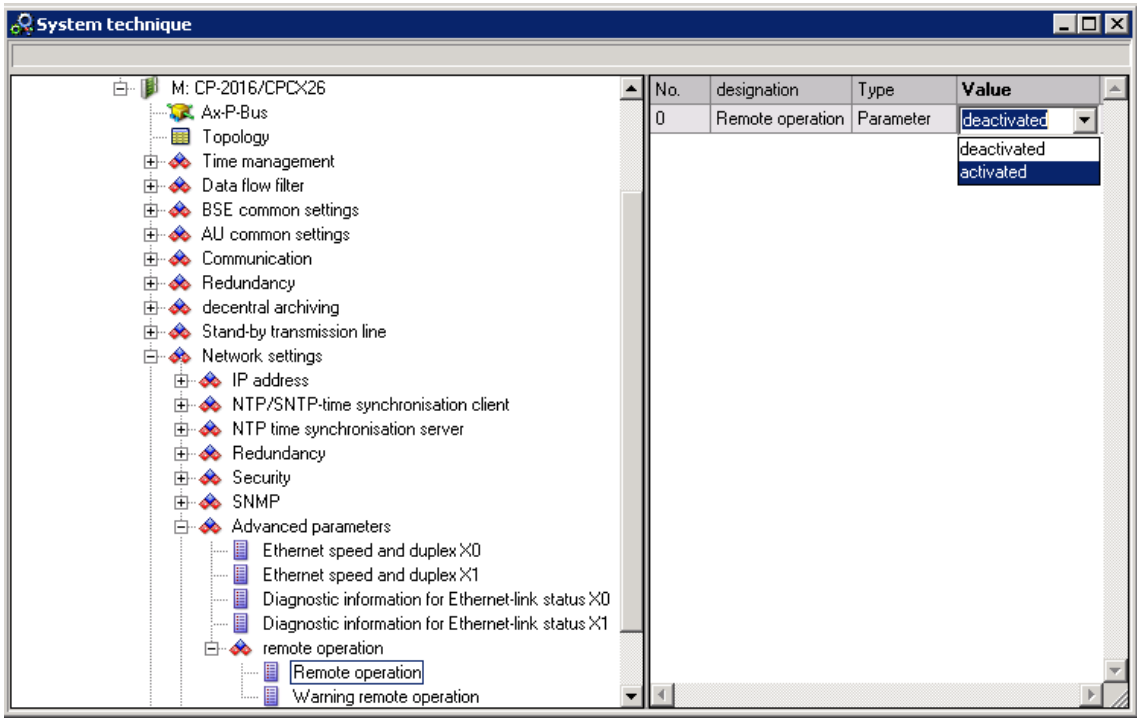
Example: SICAM CP-8050 – CPCI85:



Example: SICAM CP-8000 – CPC80:



Example: SICAM AK 3 - CPCX26:



For the firmwares listed below the remote operation is deactivated by default from the firmware revision specified:

Firmware-Type	Firmware	from Firmware-Revision
	CPCI85	01
BSE	CPC80	01
	CPCX26	01
	PCCX26	01
	ETA3	01
	ETA4	01
PRE	ETA5	01
	MBSiA0	01
	MBCiA0	01
	DNPiA1	01

From Toolbox II V5.10, when connecting via remote operation, a ping-command is sent via TCP with the data field content "SICAM TOOLBOX II" to the IP address selected in remote operation. The target system does not send the same message back, as is usual for the default implementation, but writes the supported connection type into the data field of the response:

Connection type	ping-Request from TBII	ping-answer from target system
Telnet	SICAM TOOLBOX II	SICAM TOOLBOX II
http	SICAM TOOLBOX II / SICAM Device Manager	http:80
HTTPS	SICAM TOOLBOX II / SICAM Device Manager	HTTPS:443

After SICAM TOOLBOX II receives this information it builds up the connection accordingly.

For the protocols listed below the remote operation via HTTPS (secure connection) is possible from the firmware revision specified:

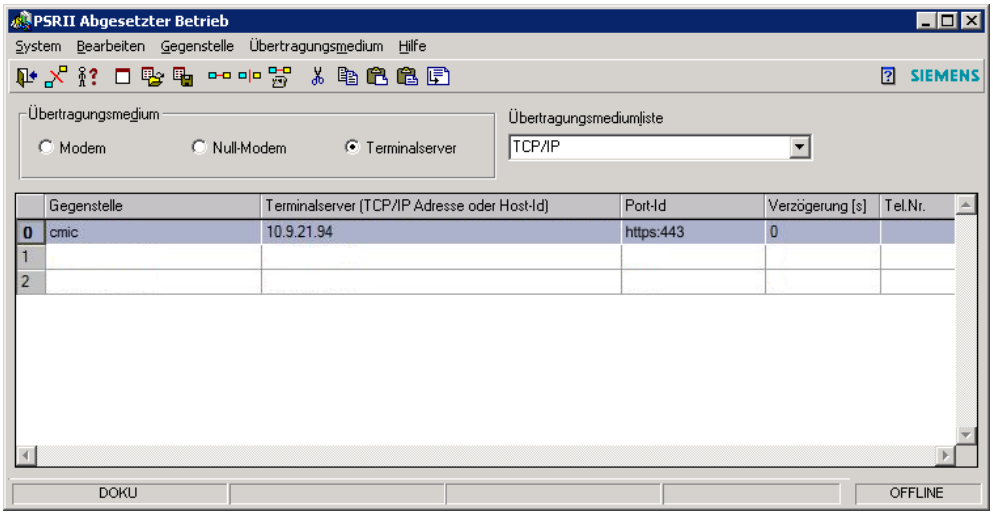
Firmware-Type	Firmware	http	HTTPS
BSE	CPCI85	from Revision 01	from Revision 01 **)
	CPC80	from Revision 01	from Revision 04 *)
	CPCX26	from Revision 01	from Revision 01 *)
	PCCX26	from Revision 01	from Revision 01 *)
PRE	ETA4	from Revision 01	from Revision 02 *)
	ETA3	from Revision 01	from Revision 02 *)
	ETA5	from Revision 01	from Revision 01 *)
	MBSiA0	from Revision 01	from Revision 01 *)
	MBCiA0	from Revision 01	from Revision 01 *)
	DNPiA1	from Revision 01	from Revision 01 *)

*) from SICAM TOOLBOX II V5.11
**) from SICAM TOOLBOX II V6.02

3.3.2.2.1 Establishing a HTTP(S) connection with blocked ICMP-ECHO

In case of a blocked ICMP-ECHO in a firewall between SICAM TOOLBOX II and SICAM RTUs, it is not possible to establish per default an automatic connection. By additional definition of the desired connection type it is possible to bypass this block.

The corresponding parameter – `Port-Id` - can be found in the phone list of the remote operation (System – Remote Operation).



Port-Id	Description
HTTPS:443	Connection to port 443 is established via HTTPS
http:80	Connection to port 80 is established via http
2001	Connection to port 2001 is established

The ports http(80) or HTTPS(443) are available in SICAM RTUs systems/firmwares such as SICAM AK 3, SICAM A8000, ETA4, ETA3 and ETA5. In older systems/firmwares (legacy) such as ET02, ETA2, ..., CPCX25 only port 2001 is available.

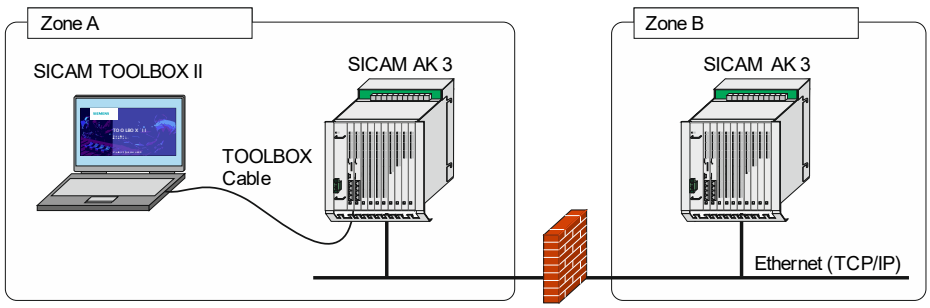
3.3.2.3 Remote Maintenance

For the remote maintenance the SICAM TOOLBOX II establishes a connection to a SICAM RTUs by means of a local parameterization cable or in remote operation over a network interface by means of TPC/IP.

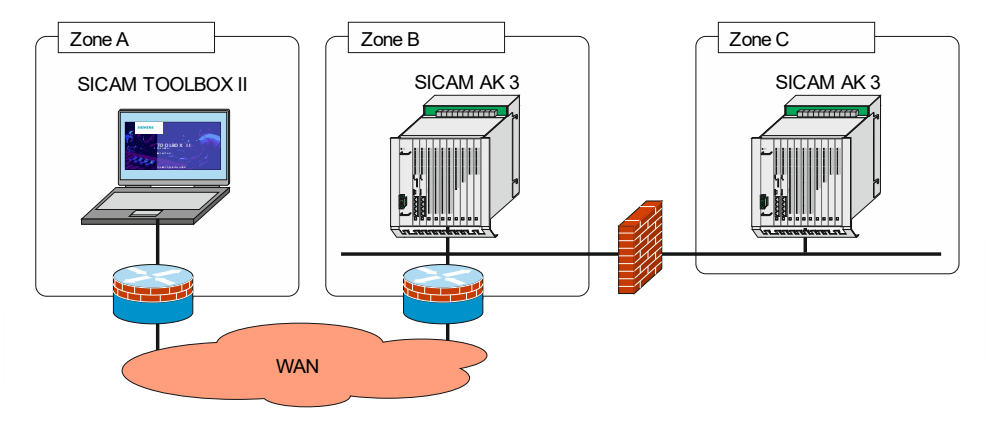
From this moment, with the SICAM TOOLBOX II it is possible to address other components in an automation network by means of remote maintenance. This takes place with internal system messages, which must be routed or blocked in the system-technical parameter setting on the M-CPU in the `Topology`.

The service function messages are applied (see *chapter 3.3.2.3.1; Service Function Messages)*.

Remote maintenance, TOOLBOX II local connection



Remote maintenance, TOOLBOX II remote operation



For remote maintenance by means of SICAM Device Manager a connection is established over the network interface via TCP/IP.

3.3.2.3.1 Service Function Messages

By means of service function messages a variety of system information items are transmitted (e.g. remote maintenance, diagnostics).

The service function messages between SICAM TOOLBOX II and a SICAM RTUs AU are prepared accordingly on LAN protocols (conversion from SICAM RTUs internal format and the format for SICAM TOOLBOX II) and forwarded to the central service function of the SICAM RTUs component for further processing.

For the basic system elements listed below the service function messages are deactivated by default for configuration from the firmware revision specified.

- CPCI85 from Revision 01
- CPC80 from Revision 01
- CPCX26 from Revision 01
- PCCX26 from Revision 01
- CPCX25 from Revision 01
- CPCX55 from Revision 0601
- CPCX65 from Revision 07

If necessary the service function messages can be enabled individually.

The corresponding parameter can be found in the system-technical parameter setting on the M-CPU under `Topology | Service function messages`.

3.3.2.4 Process Reset Command (remote reset)

The remote reset function enables a reset to be executed in a SICAM RTUs by means of system messages, which are received by another SICAM RTUs.

For the basic system elements listed below the process reset command (remoter reset) is deactivated by default for configuration from the firmware revision specified:

- CPCI85 from Revision 01
- CPC80 from Revision 01
- CPCX26 from Revision 01
- PCCX26 from Revision 01
- CPCX25 from Revision 01
- CPCX55 from Revision 0601
- CPCX65 from Revision 07

The corresponding parameter can be found in the system-technical parameter setting on the M-CPU under `Topology | Process reset command` and can be enabled individually as required.

3.3.2.5 Time Synchronization – Remote Synchronization

Time synchronization in a multi-hierarchical network

In the entire network there must be at least one SICAM RTUs synchronized with serial time signal or NTP, i.e. a time master must be present.

The sending of the time synchronization command to other SICAM RTUs takes place automatically in the parameterized control direction from the time master (in the system-technical parameter setting on the M-CPU under `Topology | Clock-Sync` = automatic).

The time synchronization command is only accepted on one communication line, which is defined in the topology parameters as monitor direction.

SICAM RTUs with time master do not accept any time synchronization command.

For special applications the previously described automatic time synchronization can be individually adapted.

The corresponding parameter can be found in the system-technical parameter setting on the M-CPU under `Topology | Clock-Sync`.

Value of the Parameter	Function
Send only	The time synchronization command is sent over this interface, regardless of the parameterized data flow direction
Receive only	The time synchronization command is accepted over this interface for time synchronization
Blocked	Over this interface neither the time synchronization command is sent nor a received time synchronization command accepted

For the basic system elements listed below the time synchronization on the M-CPU is deactivated by default for configuration from the firmware revision specified and can be activated if required:

- CPCI85 from Revision 01
- CPC80 from Revision 01
- CPCX26 from Revision 01
- PCCX26 from Revision 01
- CPCX25 from Revision 01
- CPCX55 from Revision 0601
- CPCX65 from Revision 07

3.3.2.6 Time Synchronization via (S)NTP

The time server of a SICAM RTUs can be synchronized through remote synchronization with the time synchronization command over serial communication or over the LAN (Ethernet TCP/IP – NTP).

Regardless of the remote synchronization a SICAM RTUs, which contains an NTP-Client, can be time synchronized from an NTP-Server.

The corresponding parameters are deactivated by default and can be activated if necessary. They can be found in the system-technical parameter setting on the protocol element under
`Network settings | NTP/SNTP-time synchronisation client`
and
`Network settings | NTP time synchronisation server`
or in case of CP-8031/CP-8050 under
`System settings | Network settings | NTP/SNTP Client | advanced parameters`
and
`System settings | Network settings | Services`.

The following firmwares support NTP-Client:

- CPCI85
- CPC80
- CPCX26
- PCCX26
- ETA3
- ETA4
- ETA5

SICAM RTUs which already have a synchronized system time can be used as NTP-Server.

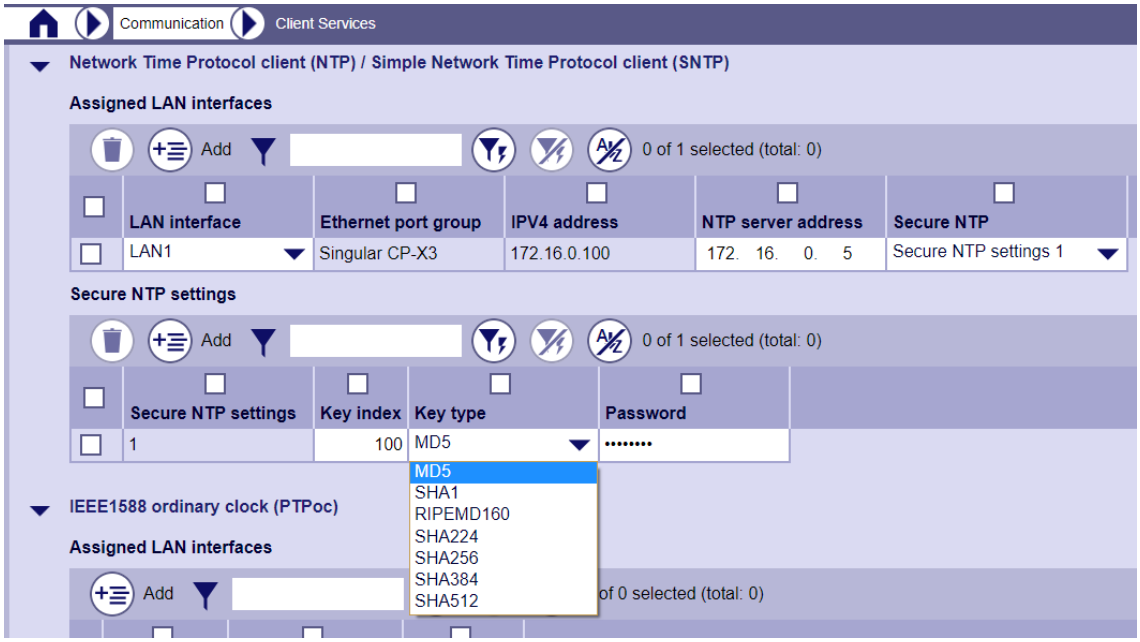
The following firmwares support NTP-Server:

- ETA3
- ETA4
- ETA5

3.3.2.7 Secure NTP Client (CP-8031/CP-8050 only)

NTP has an integral security attribute to put a stop to endeavors to tamper with system time synchronization. NTP may use MD5 encrypted keys to authenticate time stamps provided by a time server. Network time clients and devices can make use of secure keys to authenticate time stamps and ensure their supply of origin.

NTP executes authentication by employing an agreed set of keys between a server and client which are encrypted in time stamps. An NTP time server transmits a timestamp to a client with one of a selection of keys encrypted and appended to the message. When a timestamp is obtained by the client, the security key is un-encrypted and checked against the listing of filed secure keys. In this way the client can be sure that the received time stamp came the expected time source.



Secure NTP settings in SICAM Device Manager

3.3.2.8 WEB-Server Protocols

In SICAM RTUs a WEB-Server (Port 80/443, http(s)) can be activated on the LAN protocols ETA3 and ETA5. With function activated diagnosing is possible.

For the LAN protocols listed below the WEB-Server (http) is deactivated by default for configuration from the firmware revision specified. This can be activated if necessary

Firmware	http
ETA3	from revision 01
ETA5	from revision 01
ET25	from revision 01
ET83	from revision 01
ET85	from revision 01

CP-8031/CP-8050:

Firmware CP-8031/CP-8050
ETi5
DNPiI1
DNPiI2
MBCiI0
MBSiI0
OPUPI0

The corresponding parameter can be found in the system-technical parameter settings under `HTTP-Web server`.

With SICAM A8000 CPC80/CP-802x parameterization can also take place by means of WEB-Browser as an alternative to the SICAM TOOLBOX II / SICAM Device Manager.

Hint

Some SICAM RTUs protocols and some SICAM A8000 protocols support a WEB server for diagnostic purposes (access via WEB browser). Authentication for these WEB pages is not provided for. Therefore, for normal operation this possibility of access should be deactivated via parameterization.

Parameterization of SICAM A8000 Series by means of SICAM TOOLBOX II

If parameterization is carried out by means of SICAM TOOLBOX II, the WEB parameterization option (if available) is deactivated. The WEB-Server is deactivated by default with configuration of the firmware revision specified and can be activated for diagnosing.

In CP-8031/CP-8050. WEB-server is always available

Parameterization of SICAM A8000 Series (CP+8000 and CP-802x, not CP-8031/CP-8050) by means of SICAM WEB (without SICAM TOOLBOX II)

In this case http(s) port 80/443 is activated and cannot be deactivated.

3.3.2.8.1 Deactivation of unnecessary Standard Users (WEB)

ETA3, ETA5, ET25, ET83, ET85: has only 1 USER, WEB only for diagnostics.

3.3.3 Measures for restricted distribution of system messages

You should set following measures on selected interfaces in the telecontrol network (interfaces to other operators) to avoid closed loops messages respectively for restricted distribution of system messages.

3.3.3.1 Blocking of messages in topology configuration of SICAM RTUs

Parameter	Recommended setting	Meaning
Error Message	No transmit	Error message distribution. Automatic means, that error messages are only transmitted if data flow direction is set to "monitor direction" of "both directions".
Clock-sync	Disabled	-
Counter interrogation	No transmit	Counter interrogation command. Automatic means, that the selective interrogation command will be transmitted according the CASDU and the global interrogation command will be transmitted according the parameterized data flow direction.
GI	No transmit	-
Acknowledge network	Disabled	Distribution acknowledge network
Service function messages	Disabled	Distribution service function messages (SICAM TOOLBOX II messages)
systel private range	Disabled	Distribution of the system telegrams within the private range
Reset process command	Receive disabled	Blocking receive reset process command

3.3.4 Denial of Service

SICAM AK 3 and SICAM BC are multiprocessor systems, i.e. in case of a denial-of-service - attack only on NIP is affected.

SICAM A8000 is a single processor system. Here you have to pay attention, that the whole system is affected in case of a DoS-attack.

SICAM A8000 and SM-2558 contain a switch which limits the ports bandwidth and filters broadcast storms.

SICAM A8000 Series and SICAM RTUs (CPCX26, PCCX26, all SM2558 protocols) contain a switch supporting broadcast storm suppression (bandwidth control of the port traffic).

Broadcast storm suppression is the same in all types of devices, but the throughput is depending on the device:

- SICAM A8000 CP-8031/CP-8050: no limitation
- SICAM A8000 CI-8520: 18000 messages per second *)
- SICAM A8000 CP-8000/CP-802x: 4 Mbit per second **)
- SICAM A8000 CI-8522: 18000 messages per second *)
- SICAM AK 3: 10 Mbit per second **)

- SICAM AK 3 SM2558: 50 Mbit per second **)

*) this is the sum for all messages from switch to CPU over all 5 ports from CI-852x in receive direction.

**) In addition to the data given above, SICAM A8000 CP-8000/CP-802x / SICAM AK 3: max. 3300 messages per second

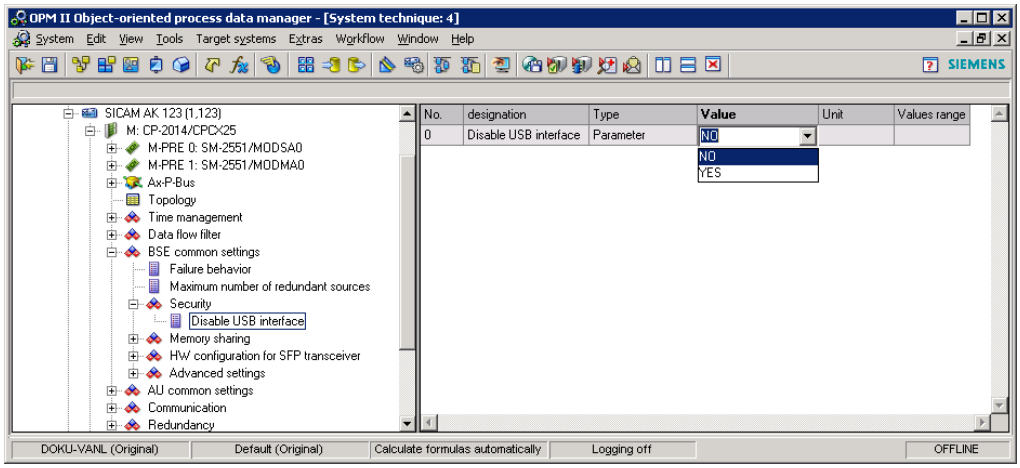
Hint

Mbit per second applies to traffic between internal and external communication ports only, and not to traffic between external ports, these are not limited.

3.3.5 Communication to SICAM RTUs via USB

The local USB-interface for SICAM TOOLBOX II on the master control element of SICAM AK 3 can be disabled if required. This is possible from firmware CPCX25 revision 03.

The corresponding parameter – `Disable USB interface` - can be found in the system technical parameters of the BSE under `BSE common settings - Security`.

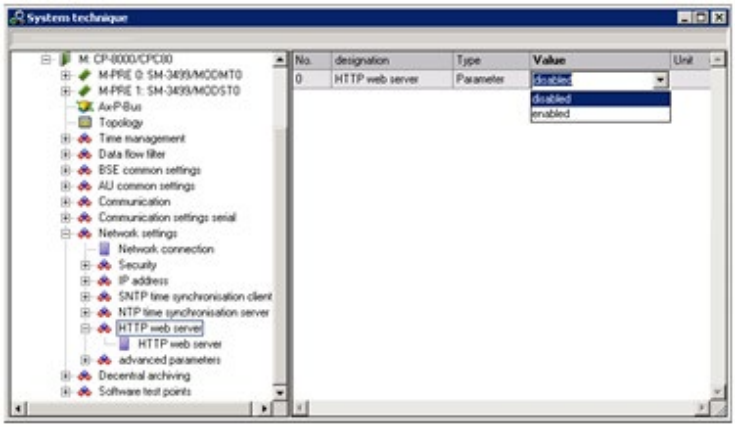


The target system takes over the role of the USB device and the SICAM TOOLBOX II takes the role of the USB host. The target system (USB device) offers no standard services like data access or USB memory. Via USB the same protocol is used as via the serial interface.

3.3.6 Enabling for Parameterization/ Diagnostics via Web-Browser

To parameterize SICAM A8000 Series via a web browser you must enable the HTTP web server in SICAM A8000 CP-8000/CP-802x. Per default the HTTP web server is disabled, but it can be enabled if required.

The corresponding parameter – `HTTP-Webserver` - can be found in the system technical parameter of the BSE under `Network settings | HTTP web server` .



Hint

Depending on the parameterization in SICAM A8000 Series / SICAM RTUs you must enter either http://ip or HTTPS://ip to establish a connection from the browser to SICAM A8000 Series / SICAM RTUs.

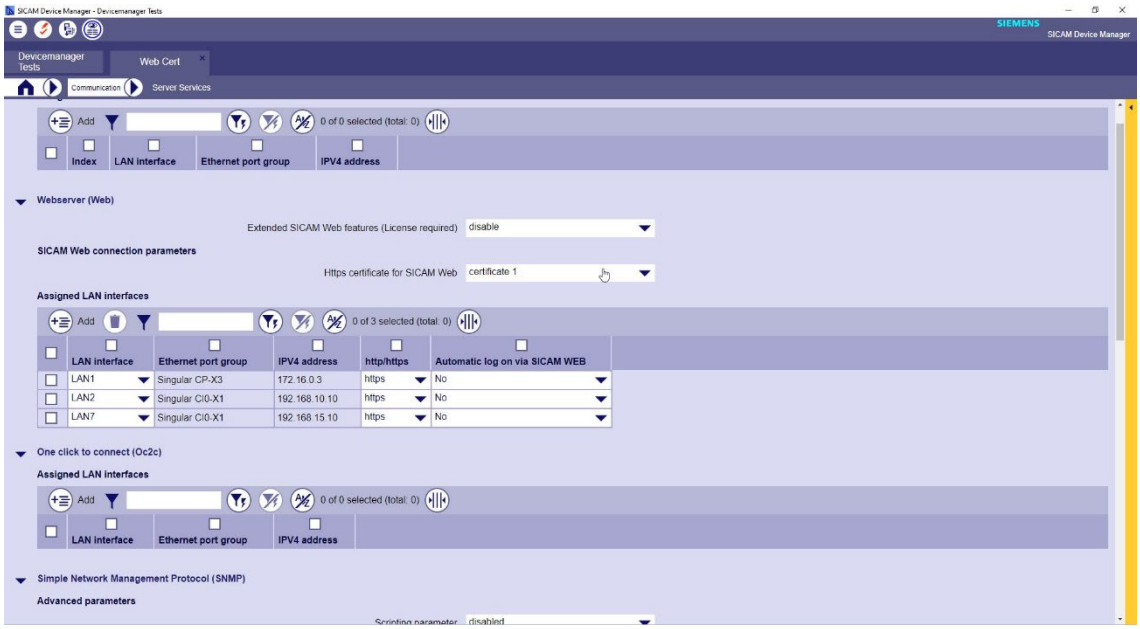
3.3.7 Secure connection establishment via HTTPS

3.3.7.1 SICAM A8000 CP-8031/CP-8050

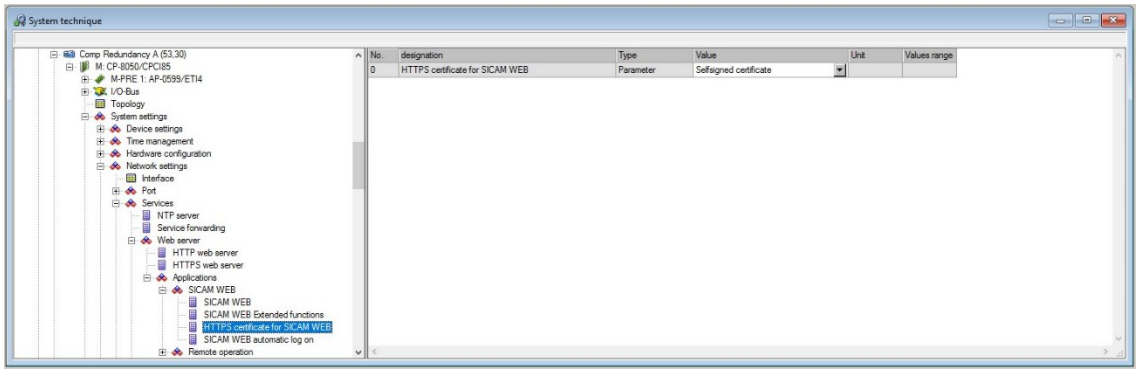
By means of the parameters `HTTP web server` or `HTTPS web server` it is possible in the SICAM A8000 CP-8031/CP-8050 to define the minimal security-level between the engineering tool (SICAM TOOLBOX II or WEB browser) and SICAM A8000 CP-8031/CP-8050.

The corresponding parameter can be found in the system technical parameter of the BSE under `System settings | Network settings | Services| Web server`. By default this parameter is set to “HTTPS web server“.

For the HTTPS web server it is possible to use a user generated certificate instead of the integrated selfsigned certificate. If you import your certificate authority in your web browsers certificate store the connection to your device is shown as secure in your browser.



Settings in SICAM Device Manager



Settings in SICAM TOOLBOX II

Hint

If the connection establishment was not successful, you only see a hint about a "not successful connection establishment" in the SICAM TOOLBOX II. You will get not details about the reason.

3.3.7.2 SICAM A8000 CP-8000/ CP-802x; AK 3 and BC (with SM-2558)

By means of the parameter `HTTP/HTTPS` it is possible to define the minimal security-level between the engineering tool (SICAM TOOLBOX II / SICAM Device Manager or WEB browser) and the devices of SICAM A8000 Series.

The corresponding parameter can be found in the system technical parameter of the BSE or PRE, respectively. By default this parameter is set to „HTTP“.

For SICAM A8000 CP-8000/ CP-802x, AK 3
under `Network settings | Security | HTTP/HTTPS`.

For SICAM AK 3 and SICAM BC with SM-2558:
on PRE (e.g.: SM-2558/ETA4) under `Security | HTTP/HTTPS`

Hint

If the connection establishment was not successful, you only see a hint about a "not successful connection establishment" in the SICAM TOOLBOX II. You will get not details about the reason.

3.3.8 Connection Password SICAM A8000 CP-8000/ CP-802x/ SICAM RTUs

In remote operation (SICAM TOOLBOX II is connected via http or HTTPS with SICAM A8000 CP8000/CP-802x / SICAM RTUs) the user has the possibility to protect the connection establishment with a password. This password is referred to as "Connection Password”.

Per default (delivery status) the “Connection Password” is not set in
SICAM A8000 CP8000/CP-802x / SICAM RTUs. Thus, no inquiry is made.

The “Connection Password” is stored encrypted on the SD-card. It is available for following systems:

System	BSE Firmware	PRE Firmware
SICAM A8000 Series CP-8000/ CP-802x	CPC80 from revision 06	
SICAM AK 3	CPCX26 from revision 01 PCCX26 from Revision 01	ETA4 from revision 03 ETA3 from revision 02 ETA5 from revision 01 MBSiA0 from revision 01 MBCiA0 from revision 01 DNPiA1 from revision 01
SICAM BC	CPCX55 from revision 09	ETA4 from revision 03 ETA3 from revision 02 ETA5 from revision 01 MBSiA0 from revision 01 MBCiA0 from revision 01 DNPiA1 from revision 01

The „Connection Password“ must fulfill following criteria:

- at least 8 to maximum 30 characters long
- a mix of uppercase and lowercase letters, numbers and special characters

The “Connection Password” is only requested, if SICAM TOOLBOX II is connected via http or HTTPS with SICAM A8000 CP8000/CP-802x / SICAM RTUs in remote operation. In case of a direct connection (via a serial or USB cable) or in remote operation via TCP/IP (old process, Port 2001), the “Connection Password” is not requested.

If a wrong „Connection Password“ is entered, you get only the information that the connection could not be established. No details about the reason are given.

Further there is a mechanism which extends the blocking time (1 min) in case of a wrong input. The "Connection Password" itself does not expire!

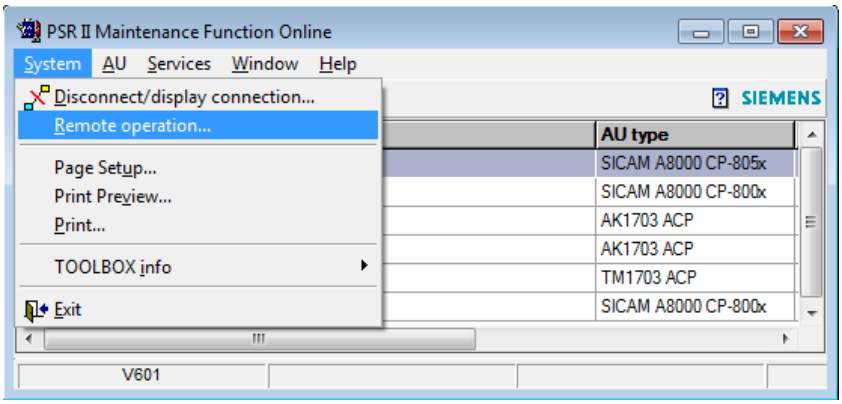
The „Connection Password“ must be set for each LAN-interface of with SICAM A8000 CP8000/CP-802x/SICAM RTUs. Thus, the assignment of an individual „Connection Passwords“ for each interface is possible.

Hint

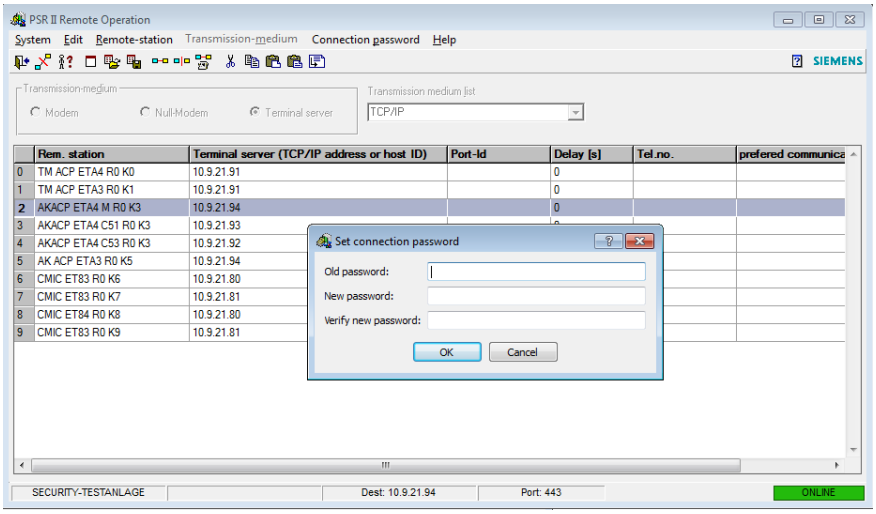
The function „Connection Password“ is not available for SICAM A8000 CP-8031/CP-8050.
The connection to the device is checked by RBAC (role based access), refer to chapter 3.3.9.

3.3.8.1 Assign/Change „Connection Passwords“

The assignment or change of the „Connection Passwords“ is done with the tool „Remote Operation“. (SICAM TOOLBOX II – service programs – special programs – Online Maintenance Function – System (in PSRII Maintenance function Online) – Remote operation)



A dedicated menu item “**Connection password**” is provided for that case. It is only enabled if the connected SICAM A8000 CP8000/CP-802x / SICAM RTUs supports the “Connection Password”, the connection was established via HTTP of HTTPS and no other tools (e.g. diagnosis or parameter loader) communicate with SICAM A8000 CP8000/CP-802x / SICAM RTUs.



For a change the user must at least enter the „old“ „Connection Password“. Per default (delivery status) the „Connection Password“ is not set.

The assignment/change of the „Connection Password“ can only be done with SICAM TOOLBOX II. Only one system can be set at a time.

Hint

The „Connection Password“ can be modified from several places. Especially this is not prohibited in SICAM AK 3!

3.3.8.2 Reset the „Connection Password“

For the case the a user has forgotten his „Connection Password“, there is a possibility to re-establish the default state (what means no „Connection Password“).

This can be done by deleting the corresponding file (SD-card:\TBN\xxxxxx.BIN) from the SD card or by initializing the automation unit.

3.3.8.3 Device change

If a SICAM A8000 CP8000/CP-802x / SICAM RTUs device restarts with different parameters (device change), it automatically reads out the „Connection Password“ of the SD card.

When there is no „Connection Password“ available on the SD card, this will be treated as „no Connection Password“.

3.3.8.4 Initialize Automation Unit

During the initialization of the AU, the „Connection Password“ is reset on the SD card.

During the initialization of the C-CPU, the „Connection Password“ is not reset.

3.3.9 Role-Based-Access-Control in SICAM A8000 Series

SICAM A8000 Series support a role based access control (RBAC). The configuration of RBAC is carried out online at the IED by SICAM WEB.

8 roles according to IEEE 1686, BDEW-Whitepaper and IEC 62351-8 are predefined in devices of SICAM A8000 Series.

A role comprises certain authorizations to execute certain functions. One or more roles and the respective associated rights can be assigned to any user.
The ADMINISTRATOR role has all rights.

A user has to change his password during login if

- a different user (e.g. RBAC-Manager) has changed the password
- a new user account has been created for this user

Necessary firmware:

SICAM WEB/SICAM Device Manager	SICAM TOOLBOX II	CPC80	CPCI85
SWEB revision 05.00 or higher	V06.01 or higher	revision 14 or higher	revision 1.00 or higher

Following functions (more precisely, granted rights to execute certain functions) are assigned to roles predefined in SICAM A8000 Series (acc. to IEEE 1686):

Functions \ Defined Roles	VIEWER	OPERATOR	ENGINEER	INSTALLER	SECURITY ADMIN	SECURITY AUDITOR	ROLE BASED ACCESS MANAGER	ADMIN
General information	X	X	X	X	X	X	X	X
Diagnosis	X	X	X	X	X	X	X	X
Test		X	X	X				X
Operational activities		X	X	X	X			X
Engineering			X	X				X
Install firmware				X				X
Generate/Restore backup					X			X
Security settings [1)]					X			X
Certificate management					X			X
Security logbook					X	X		X
User management					X		X	X

1) Security parameters of CP-8031/CP-8050: RADIUS, LDAP, SNMP, IPSec, Service Forwarding, SysLog, PKI Management (EST, CRL), SD-Card Mode, blocking of engineering/Serial engineering interface (enable/disable)
Security parameters of CP-8000, CP-802X: All network parameters (only if engineered via SICAM TOOLBOX II)

Following functions can be executed via SICAM TOOLBOX II (Engineering System for parameterization, diagnostics, simulation) and / or SICAM Device Manager and / or SICAM WEB:

Engineering System / Functions	SICAM WEB / SICAM Device Manager	SICAM TOOLBOX II
General information	Device information, Installed Firmwares 2), Running Firmwares 2), Download SICAM PAS Configuration 1)	Device address
Diagnosis	Status Diagnosis, Diagnosis Logbook, IP Security Status	Status Diagnosis, History Diagnosis, IDR, IDE, …
View process data	Download process data archive, Alarms & Events, LED State 2)	DEAR, Data flow test *)
Test	Testing Logic 1), Testing I/O Module 1)	Online Test, CAEx Plus, Message simulation
Operational activities	Restart device, Set time, Generate support information 2)	Restart device, Set time, Stop system element
Engineering	Change standard parameter and equip device 1), Upload ICD/IID File 1)	Parameterloader for standard parameter
Install Firmware	Upload Firmware, Upload Language File	Firmware Loader
Generate and Restore Backup	Generate Backup 1), Restore Backup 1)	N.A.
Security settings	Certificate Management	Initialize Parameter, Change security parameter **)
Security Logging	Security Logbook	Security Logbook
Role based access	User Management	N.A.

*) Data flow test during startup is only possible for users with “Restart Device” rights
**) Security parameters are not supported for CP-8000/CP-802x if engineered by SICAM WEB

1) available for CP-8000/CP-802x only
2) available for CP-8031/CP-8050 only

3.3.10 PKI Infrastructure/ Certificate Management in SICAM A8000 Series according to IEC 62351-9

SICAM A8000 CP-8031/CP-8050 supports the usage of key material - both signed via EST (Enrollment over Secure Transport) and manually loaded into the device - and certificate authorities for various services and encrypted communication.

SICAM A8000 CP-8000, CP-802x support the usage of key material - manually loaded into the device - and certificate authorities for various services and encrypted communication.

Necessary parameter setting can be carried out only by users having the appropriate rights (Security Administrator, Administrator).

3.3.10.1 Certificate-based encryption algorithms supported by SICAM A8000 Series

3.3.10.1.1 Encryption Algorithms by means of elliptic curves

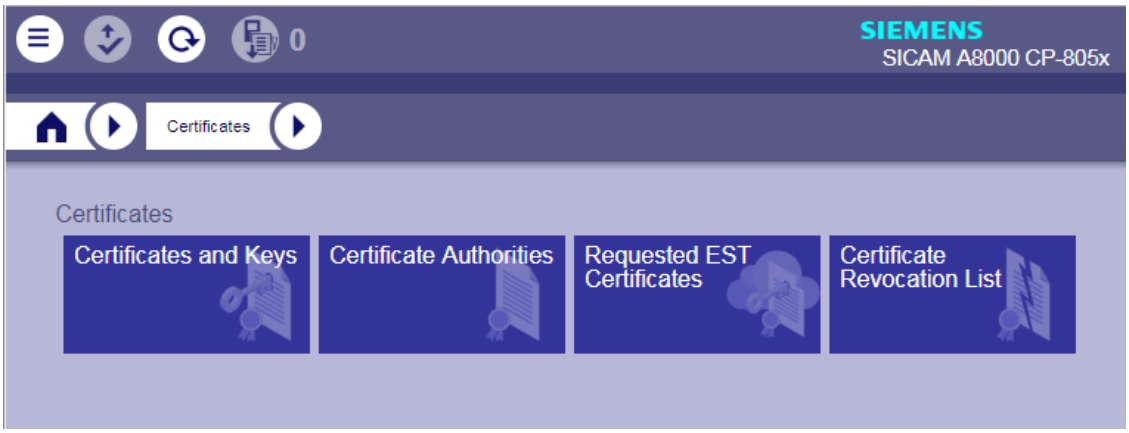
- secp521r1: NIST/SECG curve over a 521 bit prime field
- secp384r1: NIST/SECG curve over a 384 bit prime field
- secp256k1: SECG curve over a 256 bit prime field
- secp224r1: NIST/SECG curve over a 224 bit prime field
- secp224k1: SECG curve over a 224 bit prime field
- secp192k1: SECG curve over a 192 bit prime field (weak – no recommended)
- secp160r2: SECG/WTLS curve over a 160 bit prime field (weak – no recommended)
- secp160r1: SECG curve over a 160 bit prime field (weak – no recommended)
- secp160k1: SECG curve over a 160 bit prime field (weak – no recommended)
- prime256v1: X9.62/SECG curve over a 256 bit prime field
- prime192v1: NIST/X9.62/SECG curve over a 192 bit prime field (weak – no recommended)
- brainpoolP512r1: RFC 5639 curve over a 512 bit prime field
- brainpoolP384r1: RFC 5639 curve over a 384 bit prime field
- brainpoolP256r1: RFC 5639 curve over a 256 bit prime field

3.3.10.1.2 Encryption Algorithms by means of RSA

- Max. cipher strength RSA-2048 for SICAM A8000 CP-8000/21/22, SICAM AK 3
- Max. cipher strength RSA-4096 for SICAM A8000 CP-805x

3.3.10.2 Manual Certificate Management

SICAM WEB enables you to make manually generated certificates with key material available to the device in *.pkcs12 format. This format includes at least a key with a corresponding certificate and, optional, trusted certificate authorities:



SICAM WEB dashboard -> Certificates

Requested EST Certificates and *Certificate Revocation List* tiles are available for SICAM A8000 CP-8031/CP-8050 only.

- Press the Certificates and Keys tile:

Upload certificate/key pair

- Click on Upload certificate/key pair button:

- In the dropdown list, select a *Name*

- Click on *Select a file* to browse your file system where your *. p12 or *. pkcs12 file is stored
  In case of PKCS12 file you have to enter PIN
- Click *OK*

Additional certificates/certificate authorities can be uploaded in *.pem format:

- Press the Certificate Authorities tile

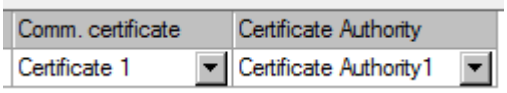
Upload certificate authority

- Click on Upload certificate authority button:

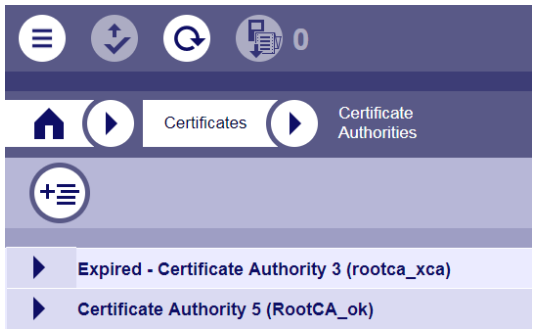
SICAM WEB dashboard -> Certificates -> Certificate Authorities

- In the dropdown list, select a *Name*
- Click on *Select a file* to browse your file system where your *. pem file is stored
- Click *OK*

The assignment of manually generated certificates with key material and certificate authorities to `Upload Certificate -> Name` (certificate 1 to certificate 10 and certificate authority 1 to certificate authority 10) is carried out in the parameter settings of the respective certificate based service by means of SICAM TOOLBOX II, OPM II (system technique):



Examples for certificates and certificate authorities after successful parameterization:



3.3.10.3 Automatic Certificate Management according to IEC 62351-9

There is the possibility to issue new certificates for the device via external certificate request service (EST) in order to avoid certificates manually provided for each service.

The device acting as an EST-client will request new certificates and will autonomously update certificates in due time before the expiry date.

You have to configure IP-address, IP-interface and initial key material to establish a connection to an EST-server (e.g.: SICAM GridPass) by means of TOOLBOX II, OPM II, parameters: `System settings | Security | PKI Management | Remote certificate request (EST)`.

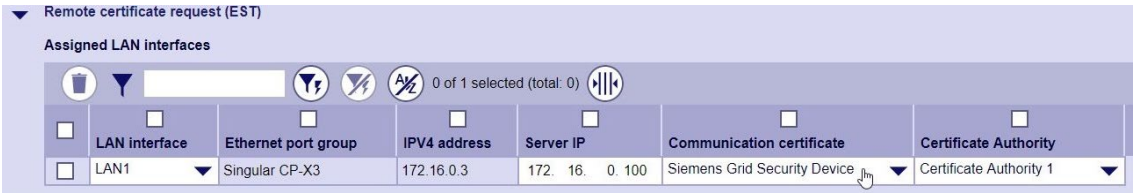
You can use an imported certificate/key (e.g.: certificate1) as initial key material or you can use the basic initial authentication mode. (Siemens Grid Security Device).

In case of using basic initial authentication it is necessary to import the EST-Servers Certificate Authority into the device and the "Siemens Grid Security Root-CA V1.0" certificate (https://support.industry.siemens.com/cs/document/109799728/siemens-grid-security-root-ca-v1-0?dti=0&lc=en-DE) into the EST-server.

Certificate in text format:

-----BEGIN CERTIFICATE-----
MIIFujCCA6KgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBljELMAkGA1UEBhMCREUx
DzANBgNVBAgTBkJlcmxpbjEPMA0GA1UEBxMGQmVybGluMRAwDgYDVQQKEwdTaWVt
ZW5zMSYwJAYDVQQLEx1Db3B5cmlnaHQgKEMpIFNpZW1lbnMgQUcgMjAxNjErMCkG
A1UEAxMiU2llbWVucyBHcmlkIFNlY3VyaXR5IFJvb3QtQ0EgVjEuMDAiGA8yMDE2
MDQxNDEyMzMwNloYDzk5OTkxMjMxMjM1OTU5WjCBljELMAkGA1UEBhMCREUxDzAN
BgNVBAgTBkJlcmxpbjEPMA0GA1UEBxMGQmVybGluMRAwDgYDVQQKEwdTaWVtZW5z
MSYwJAYDVQQLEx1Db3B5cmlnaHQgKEMpIFNpZW1lbnMgQUcgMjAxNjErMCkGA1UE
AxMiU2llbWVucyBHcmlkIFNlY3VyaXR5IFJvb3QtQ0EgVjEuMDCCAiAwCwYJKoZI
hvcNAQEBA4ICDwAwggIKAoICAQC5H02rffikcFMta86n9T/mDb6lXfVSyZTAXa/v
5JlyhUsph9KZaleJWgIOHD8V4aGZzvaGcO0N3ceCJq1VtJMTUzkCxDnS0zmJuiwH
5Grr3DpfFPoxo439a6qQlo4XVCeIIEbWltF9lRvYeKGafkc1EWWNIWuRwRUqVWjN
FWfAydbJRptnzwsfRK+SbfKWSSeEeBp6xyuH4IkorRNuP1dRL5UKi7qNjhnbOt8P
cZV43bfiL0FHJ292hiTmhvWlCS2pGQBhE2SR2HyV6RAUtBxC2u8rqPgduRxw3ulN
O+dQ3KXx8xlSPLKbijcPEIL1jugjTM8H5djt+Ljo/d9kN7je+ioB3GPZzNGkewd0
TO1kjLmsp2EOj25692ENc8gD8aaHWZu/nylJ/Sm6MMUpjr4mYpmVknXS1cMtbVKu
Oovj7nyphe88sFnSQJXxP8Cxuj4s6sIRJzwEzwaEs7z3lIUjErZalGq4ZmPZJ2cB
tfq8deScsC9OogieNh5PH4RyUKqY03CqycfZFWL+/fw95cmj0ON7VUDx1Ba4rUcm
1ZTVbMOeWlL14R1T4Xyo/S1J0gggo6FqmecBLXy821huIn5/jkDoBmxE7biB2ZMQ
VFuMVHTLzrvTmYtvXm6RgtgrA6EBL7VJ2cY68zAz+VS/AeN/Si3Nsn+GDMSNI7wl
iXw4hQIDAQABow8wDTALBgNVHQ8EBAMCAZYwDQYJKoZIhvcNAQELBQADggIBAG7i
YSfbAsa6TrLnO2JDrYZYM59JyM/MYUWqC5Bqcq0yopv4XOV8bZBsPmuOJwx4K70L
1+l/2hTNNiwPz/fJ1BtcvDgpP0wjXtRz/RXGwzuyrcjFu1X1QKeioOoOLrXtH8NN
PENghJXeELuMNDMMCRzPDZ4Ud2qWIksECttCrn3wi45tVZqxjCjGhvhgHK1gWWGU
ntzrddvv6ArY6fbpvTf8Mc73teOUZP/Af5G0QBaBba6g16e+ZNzeEUWn39vg9eZy
Za5AYj+r7IJiqxsVosUVCYUCT4M3J0rGjc9wZodM43oXv9NKmRX95WiVR/Ejp5ux
XL0RQVqJb2B0sbznAgowpEg+6jrl1fGr8ZunkwgaGnSU33RBL4+B7GjO+WN0VYBS
8/+e1jGYZzlcmGg1WL98ufl4X9+3UGiDP18bCeYcBG1T72gxzn0sr6BX2KWmk0Zl
AAA9syqPp/7FXGgUJVdL51FfvBqe3ZzM7AQURlybAAhl0S8hyu4NgCq1d7ThGYF6
ygU+zi1Jev6FnbVeuOlGWgJyWBCML82JrXgI0xBFZPkYQZYht3shBRvL4Hp+OVWv
seXDcAxCjGfmTRhH4v+zPQIC5aXCtw0kflPhUCXIAIMmB+rfFpvwPXUMu7keFfvb
2UOOoa+A1+50zsBCltzKoaUL1JCwAJRMcwQGDOG8
-----END CERTIFICATE-----

Refer also to https://support.industry.siemens.com/cs/document/109799728/siemens-grid-security-root-ca-v1-0?dti=0&lc=en-DE.



Settings in SICAM Device Manager

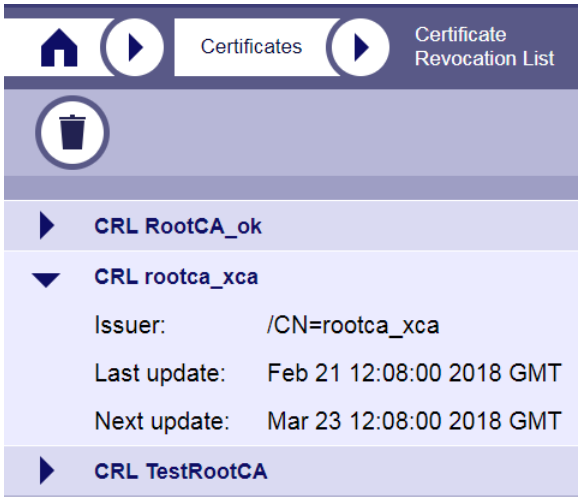
EST Server and configured IP-interface have to be in the same network.

Certificates issued by external sources are listed in the *Certificates -> Requested EST Certificates* tile. You can remove them from the device:

3.3.10.4 Certificate Revocation List (CP-8031/CP-8050)

SICAM A8000 CP-8031/CP-8050 supports administration, validation and automatic (re-) loading of certificate revocation lists provided to the device by trusted certificates and key material.

The *Certificates -> Certificate Revocation List* tile shows an overview of loaded revocation lists:



For enabling this functionality you have to configure the CRL network interface to be used for downloading (over HTTP only) revocation lists by means of TOOLBOX II, OPM II, parameter `CRL Request Interface` under `System settings | Security | PKI Management | Certificate revocation list(CRL)`.

3.3.11 AoR

AoR according to IEC 62351-8 is used for user authentication via RADIUS (refer to chapter 3.3.12.) and LDAP (refer to chapter 3.3.13).

AoR can be defined by the `Area of responsibility (AOR)` parameter under `System settings |Security| Role Based Access Control` (CP-8031/CP-8050) and `Network settings | Authentication` (CP-8000, CP-802x).

Authentication will be successful after verification of the AoR by the client.

If the AoR for a role returned by the authentication server doesn't match with the device AoR, the role will be ignored.

Examples for possible AoR verifications:

Device configured AoR	Server returned AoR	OK = role relevant for login NOT OK = role not relevant for login
"VIENNA.AT"	""	NOK
"VIENNA.AT"	"*.AT"	OK
"VIENNA.AT"	"VIENNA.AT"	OK
"VIENNA.AT"	"AT"	NOK
"VIENNA.AT"	“TEST.VIENNA.AT”	NOK
"SIEMENSSTR.VIENNA.AT"	"*.VIENNA.AT"	OK
"AT"	"AT"	OK
AoR arbitrarily	"*"	OK

3.3.12 External Authentication via RADIUS in SICAM A8000 Series

Authentication and authorization of users can be carried out by an external server via RADIUS-protocol.

You can find the `Radius Authentication` parameter in the system technical parameter of the BSE under
`System settings | Security | Role Based Access Control | Radius`
(CP-8031/CP-8050) and `Network settings | Authentication` (CP-8000, CP-802x).

Parameterization of a primary and secondary Radius server is possible.

According to IEC 62351-8, the respective RADIUS Server must provide the following data:
Radius Vendor ID according IEC 62351-8 must be set to 41912.

Description	Attribute ID	Type	Possible Values
Role-ID	1 + 10*x	Integer	Refer to table below, role definitions
Role Definition	2 + 10*x	String	Refer to table below, role definitions
Area of responsibility (optional)|	3 + 10*x	String	Refer to AOR table below
Revision	4 + 10*x	Integer	0
Valid from	5 + 10*x	String	YYYYMMDDHHMMSSZ
Valid to	6 + 10*x	String	YYYYMMDDHHMMSSZ

The definition of roles is implemented according to IEC 62351-8, in addition, the role ADMINISTRATOR is defined in the private area.

Role–ID	Role-Name	Role Definition
0	VIEWER	IEC-62351-8
1	OPERATOR	IEC-62351-8
2	ENGINEER	IEC-62351-8
3	INSTALLER	IEC-62351-8
4	SECURITY ADMIN	IEC-62351-8
5	SECURITY AUDITOR	IEC-62351-8
6	RBAC MANAGER	IEC-62351-8
-31648 (as INTEGER) 4294935648 (as unsigned INETGER)	ADMINISTRATOR	SiemensGridSecurity

3.3.13 External Authentication via LDAP in CP-8031/CP-8050

CP-8031/CP-8050 supports user authentication via LDAP, which is based on IEC 62351-8 (PULL model with LDAP-profile A).

After authentication with user credentials via LDAP, the device downloads the LDAP attribute inetOrgPerson:userCertificate (cf. RFC 2798) which contains DER encoded X.509 certificate of the user including user roles.

This certificate contains the role of a logged-in user and can be generated and pushed into LDAP by means of e.g. SICAM GridPass.

To manage permission groups between devices, the Area of Responsibility (AoR) configuration of the device can be used as a distinction, refer to chapter 3.3.11.

The communication from the device to the LDAP server is TLS encrypted.

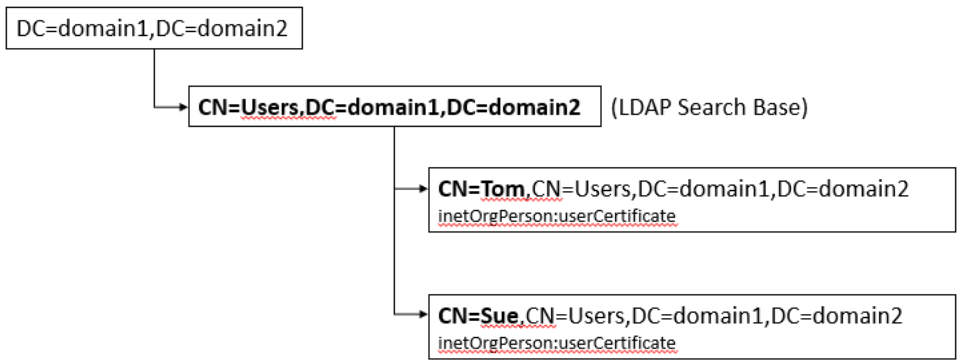
The "LDAP Search String" (LDAP Search Base) is configurable.

Example: „CN=Users,DC=domain1,DC=domain2“

The LDAP filter is not configurable and is derived from the current user name.

Supported Username Format	Example Login User Name	Resulting LDAP Filter
userPrincipalName (UPN)	Tom@somewhere.com	(CN=Tom)
Down-level logon name (sAMAccountName)	domain1\Sue	(CN=Sue)

Example LDAP Database structure:



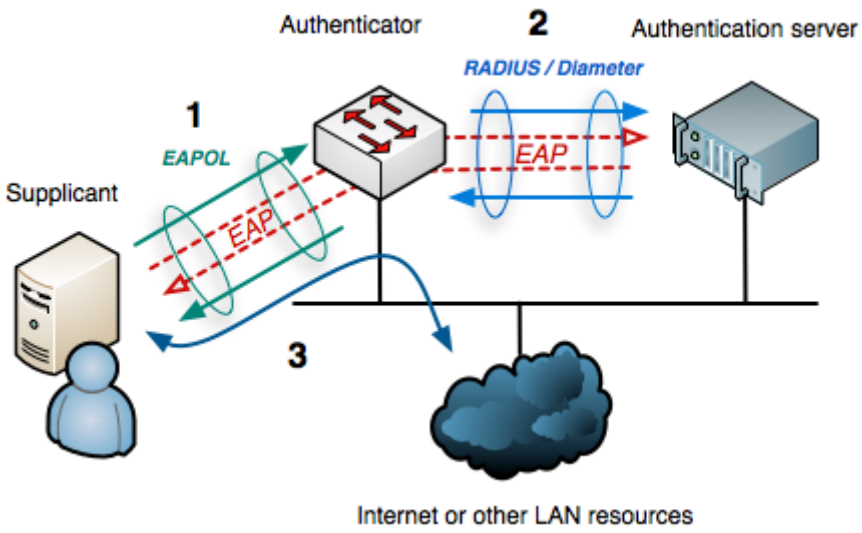
3.3.14 IEEE 802.1X

Valid for: SICAM A8000 CP-8031/CP-8050.

IEEE 802.1X is a standard for port-based network access control. It is an authentication mechanism for devices to connect to a LAN or WLAN.

The parties for 802.1X authentication are:

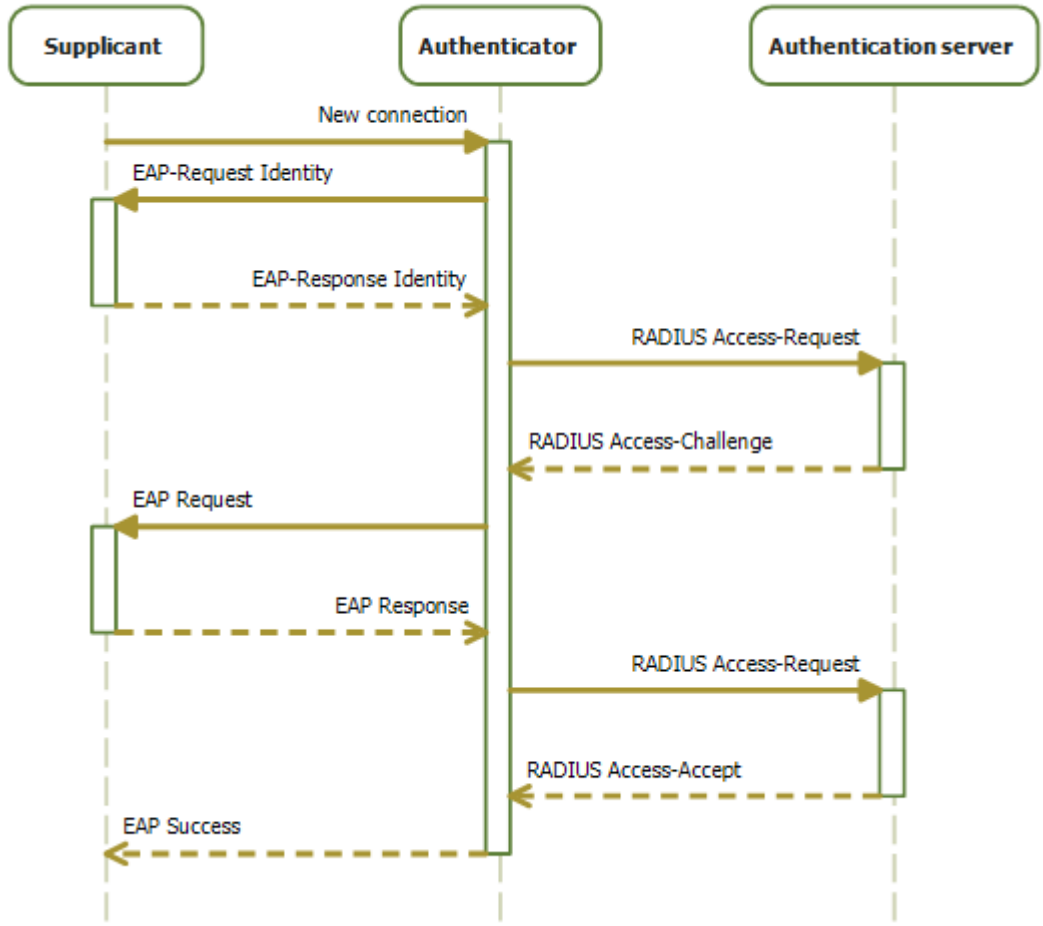
- Supplicant: device requesting a network access
- Authenticator: a switch or another network device
- Authentication server (e.g.: RADIUS server)



Source: https://en.wikipedia.org/wiki/IEEE_802.1X#/media/File:802.1X_wired_protocols.png

Extensible Authentication Protocol (EAP) is used for authentication.

Example for a typical authentication procedure:



Source: https://en.wikipedia.org/wiki/IEEE_802.1X#/media/File:802-1X.png

3.3.14.1 802.1xSupplicant

SICAM A8000 CP-8031/CP-8050 supports IEEE 802.1X as supplicant with EAP_TLS (EAP Modus).

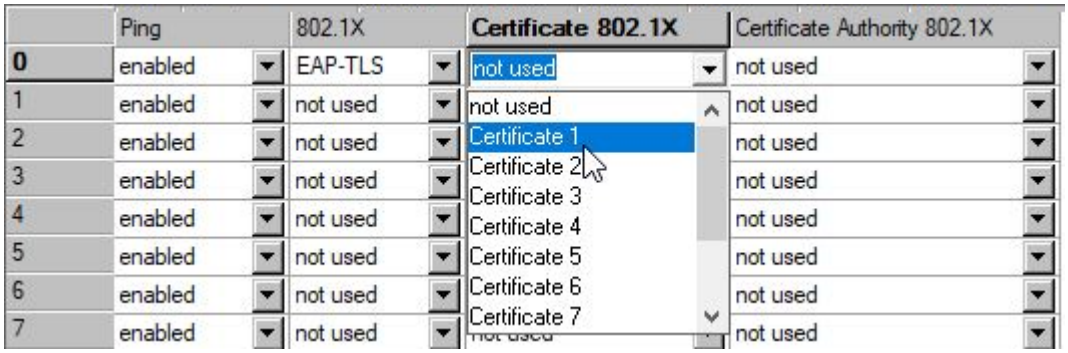
It is not possible to use supplicant and authenticator functionality on the same port.
802.1x functionality supports only RSA certificates.

Settings for CP-8031/CP-8050 via SICAM TOOLBOX II:

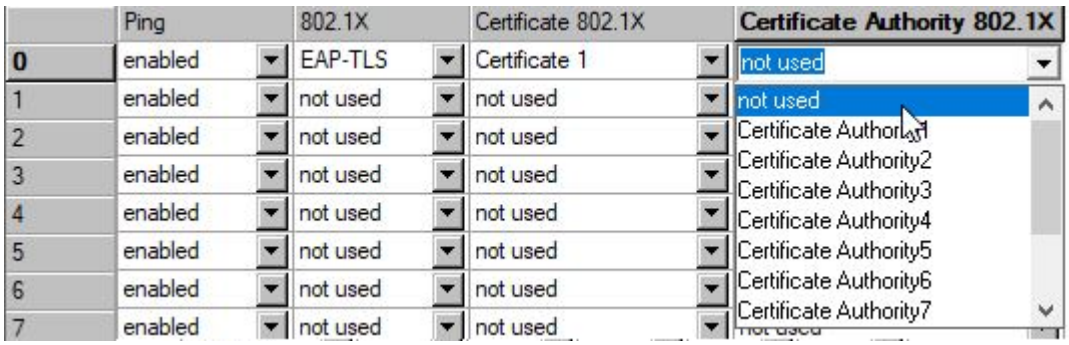
Select `EAP_TLS` (802.1X-mode) under `System settings | Network settings | Interface` :

	IPV4 default gateway	Ping	802.1X	Certificate 802.1X	Certificate Authority 802.1X
0		enabled	not used	not used	not used
1		enabled	not used	not used	not used
2	10.9.126.254	enabled	EAP-TLS	not used	not used
3	10.9.126.254	enabled	not used	not used	not used
4	10.9.126.254	enabled	not used	not used	not used

Select a client certificate for authentication:



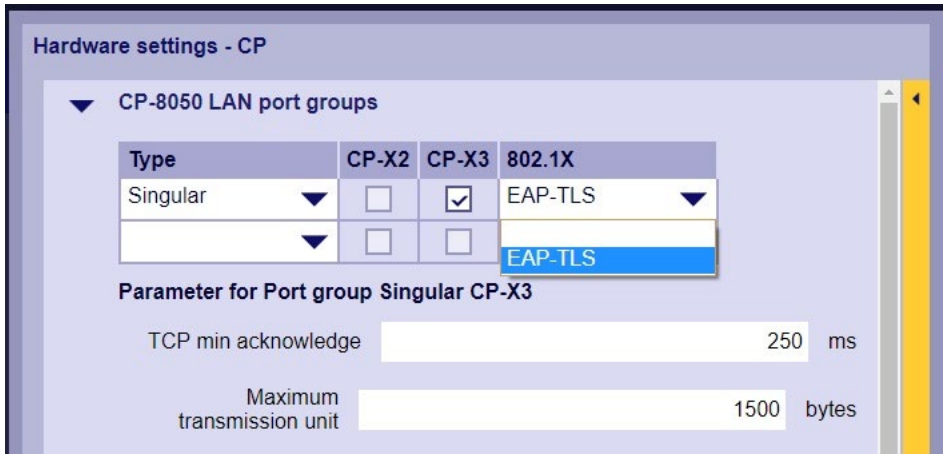
Select the CA-certificate for authentication if it isn't attached to the client certificate. Otherwise select "not used":



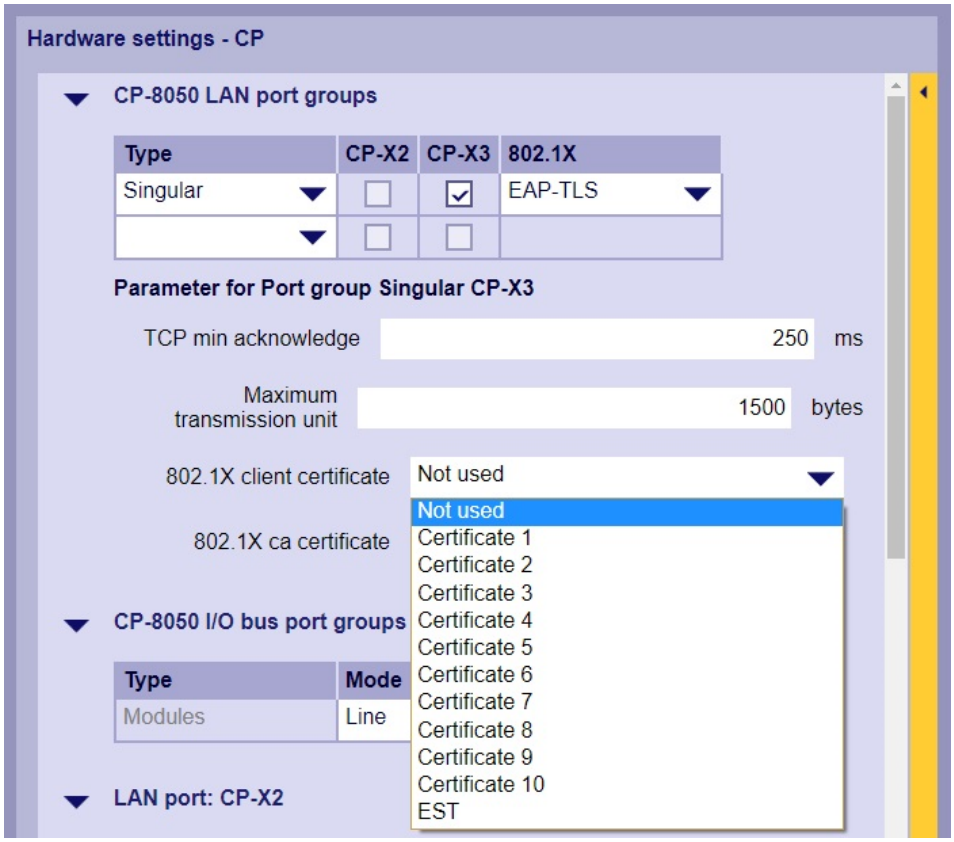
Settings for CP-8031/CP-8050 via SICAM Device Manager:

Open "Properties of module" of the base device under `Configuration | Hardware`

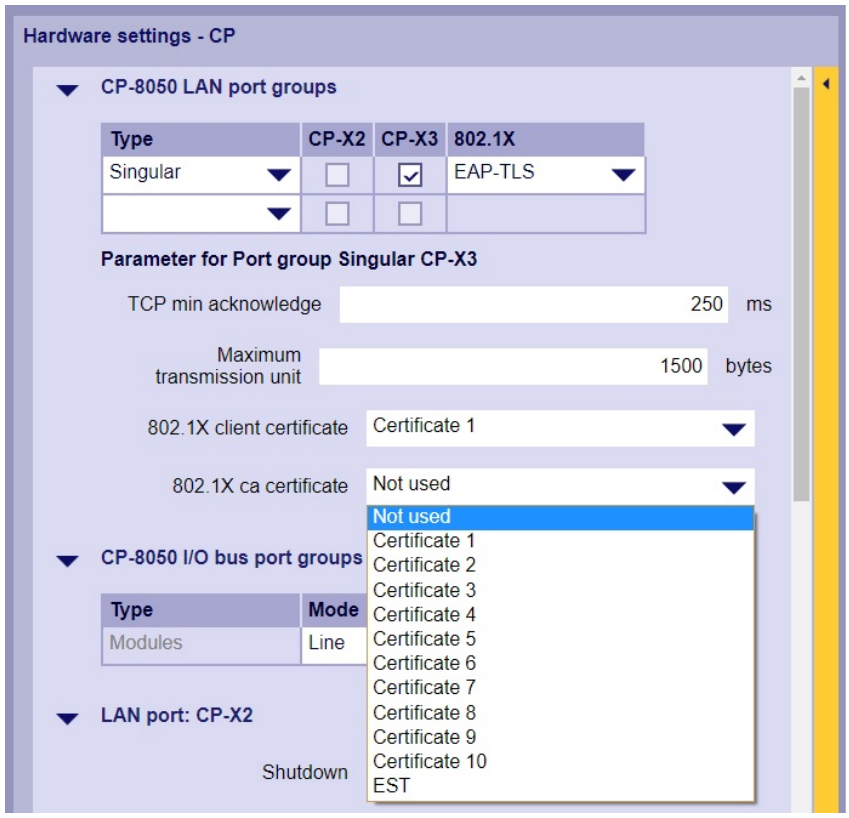
and select `EAP_TLS` (802.1X-Modus) for a hardware port:



Select a client certificate for authentication:


Hardware settings - CP
CP-8050 LAN port groups
Type
CP-X2
CP-X3
802.1X
Singular
EAP-TLS
Parameter for Port group Singular CP-X3
TCP min acknowledge
250
ms
Maximum transmission unit
1500
bytes
802.1X client certificate
Not used
802.1X ca certificate
Not used
Certificate 1
Certificate 2
Certificate 3
Certificate 4
Certificate 5
Certificate 6
Certificate 7
Certificate 8
Certificate 9
Certificate 10
EST
CP-8050 I/O bus port groups
Type
Mode
Modules
Line
LAN port: CP-X2

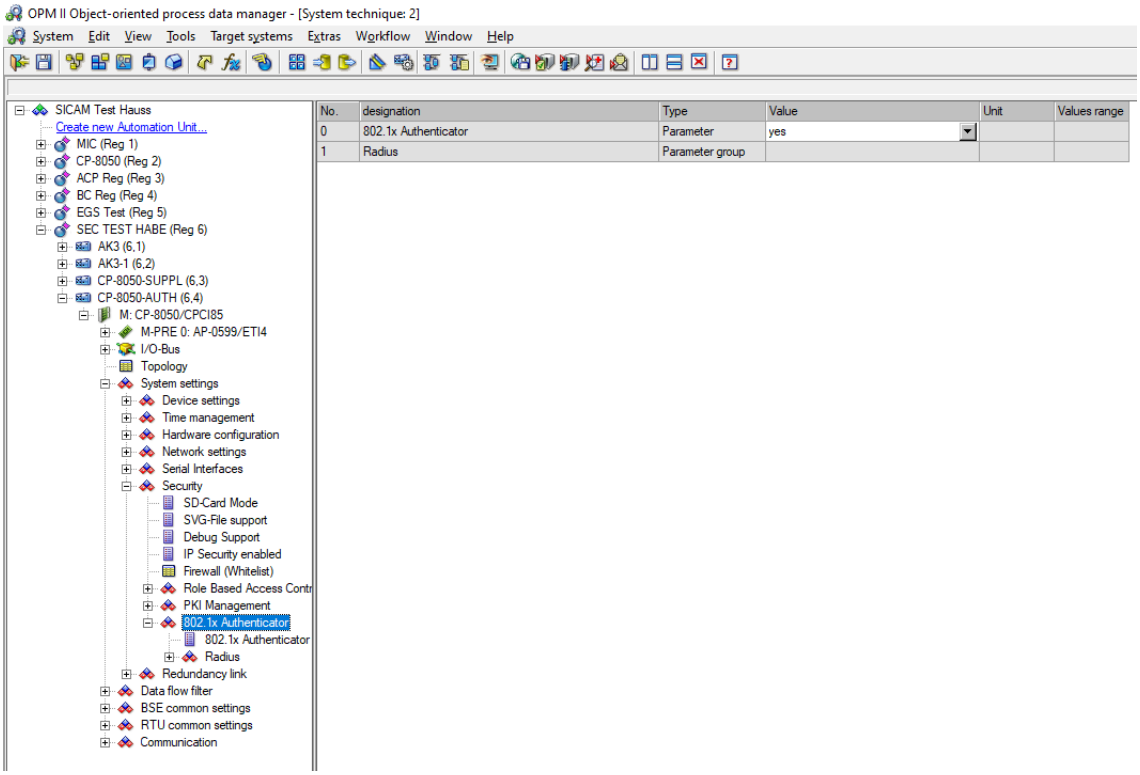
Select the CA-certificate for authentication if it isn't attached to the client certificate. Otherwise select "not used":



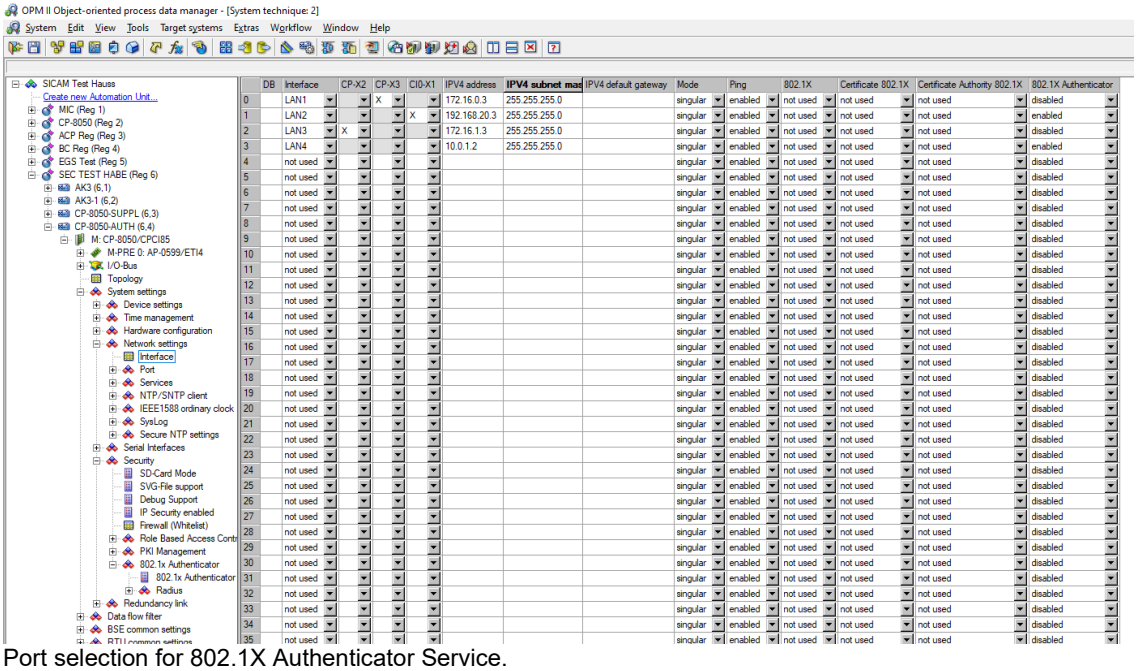
3.3.14.2 802.1x Authenticator

SICAM A8000 CP-8031/CP-8050 supports IEEE 802.1X as authenticator. For authentication purposes, a RADIUS server is necessary.

Settings for CP-8031/CP-8050 via SICAM TOOLBOX II:

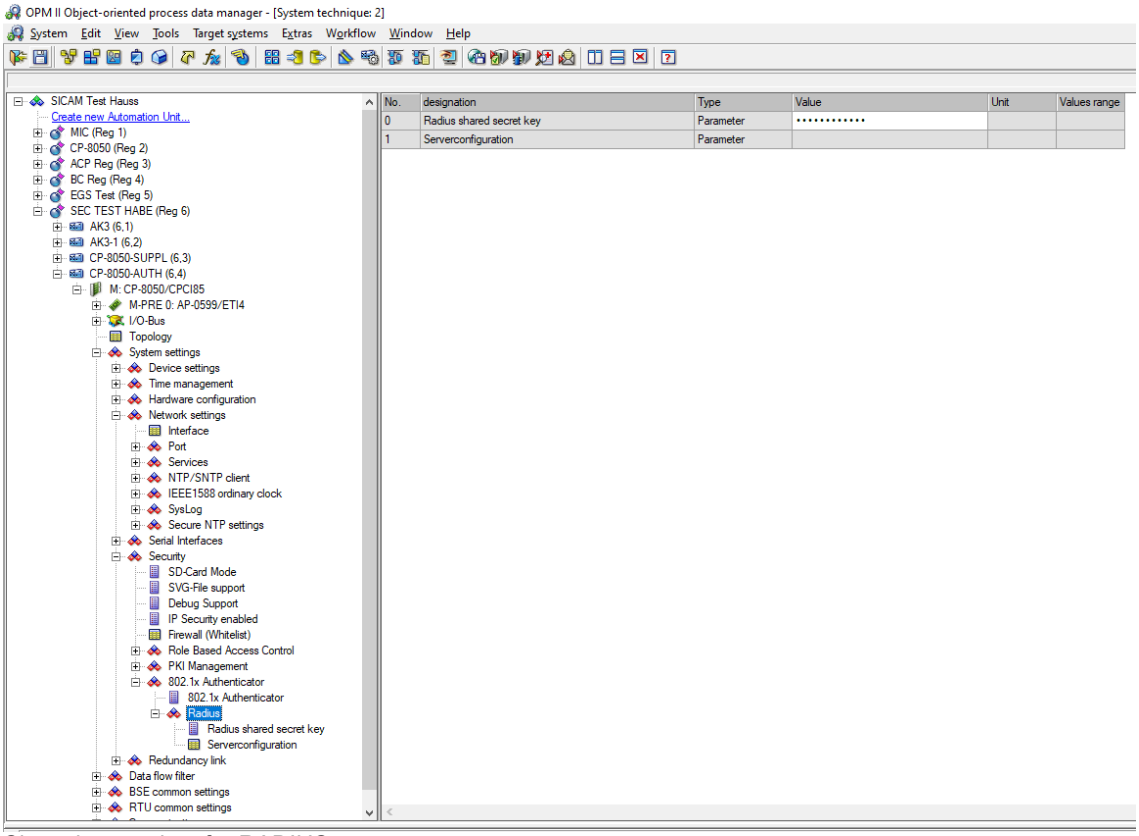


Enabling 802.1X Authenticator Service via SICAM TOOLBOX II

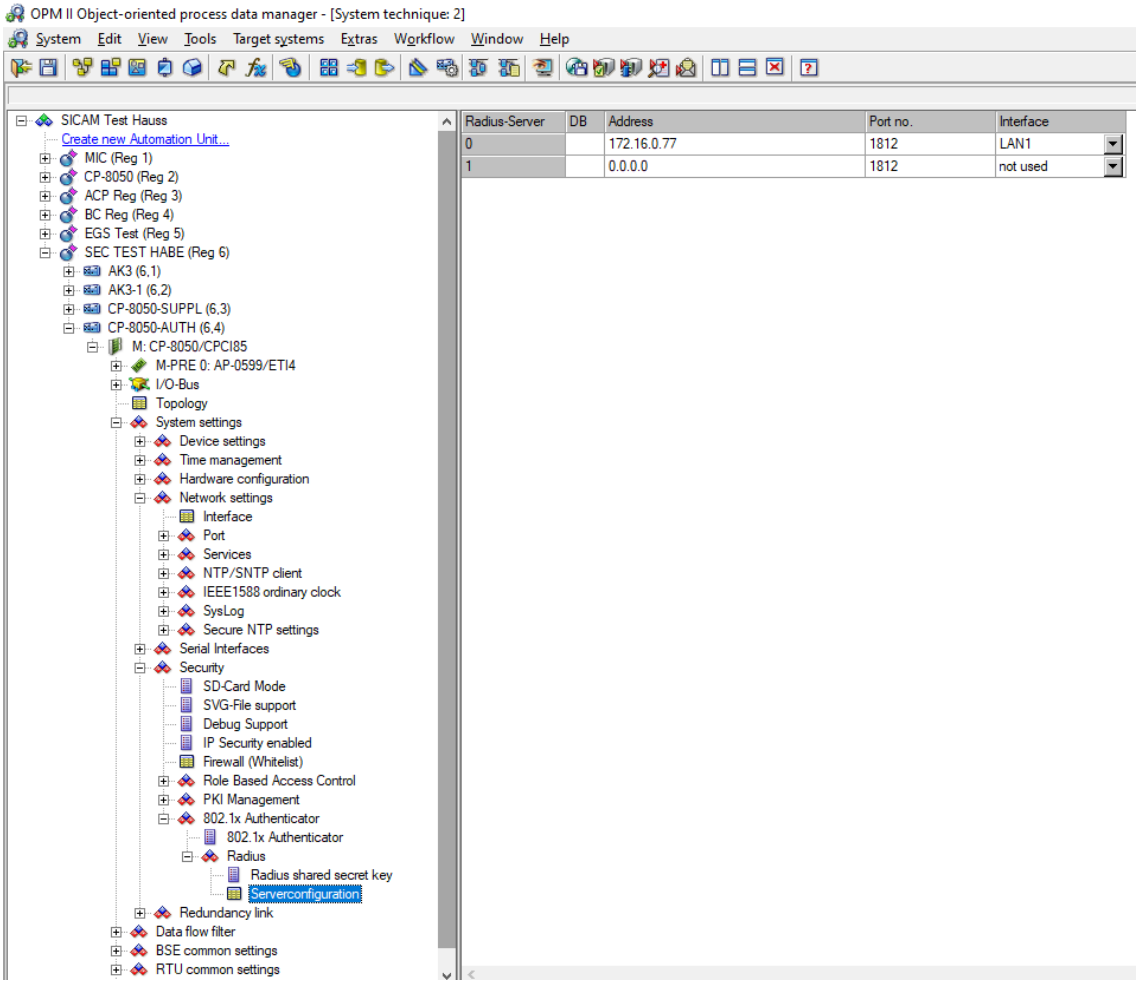


Port selection for 802.1X Authenticator Service.

Ports CP-X2 and CP-X3 do not support this function.

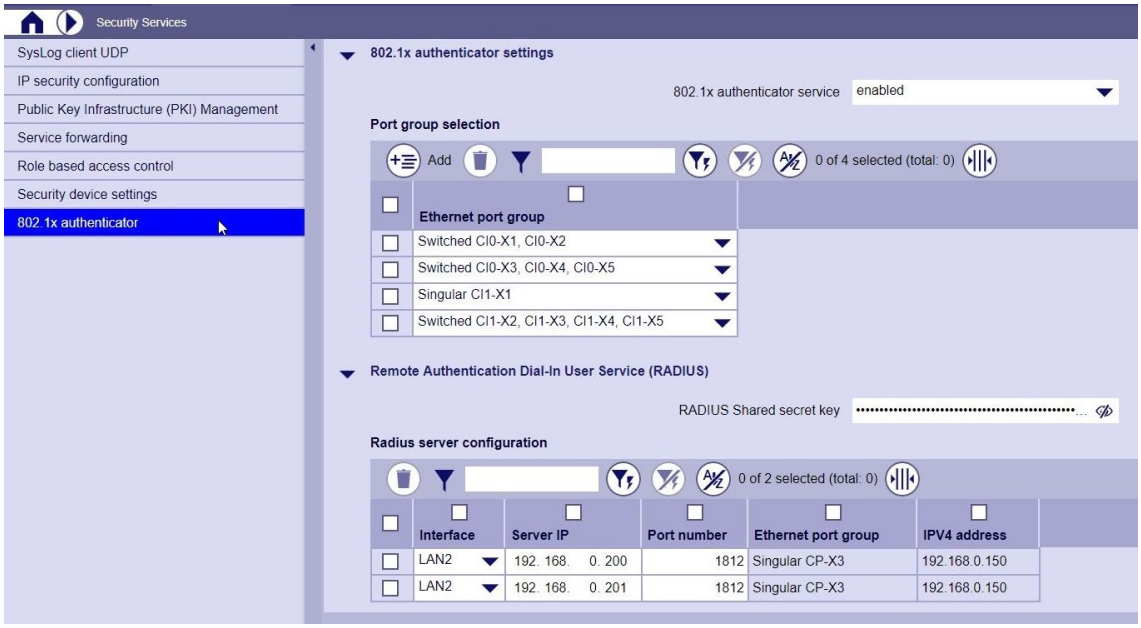


Shared secret key for RADIUS



Configuration of RADIUS server

Settings for CP-8031/CP-8050 via SICAM Device Manager:



Authenticator service will start for each selected port group of CI-modules.

3.3.15 Secure Factory Reset in SICAM A8000 Series, SICAM AK 3

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

That means that following security relevant information will be deleted, or set to delivery status (Factory Settings):

Deletion of

- all applications (firmwares), except CPCI85, CPC80,SWEB00,
  in case of SICAM AK 3: all applications (firmwares), except already loaded firmwares (CPCX26, PCCX26, ETAx,…)
- all configurations (parameter, user management, users, passwords, keys, certificates)
- all logs and diagnosis information (diagnosis logbook, security log)
- all SD-Card data

When is a Secure Factory Reset necessary?

- The device is out of order and shall be sent back to the factory.
- By means of role based access control and secure configuration all interfaces were securely configured (access not possible any more) and the admin password has been forgotten/lost.

Operational actions in case of SICAM A8000:

- In the root directory of the SD-card, store the file **FactoryReset.txt.**
  Content of the file: *FactoryReset*
- Insert SD-card and switch on the device
  Wait until RY LED is lighting (may take up to 15 minutes)

Operational actions in case of SICAM AK 3:

- Format the SD card, or use a new SD card
- Create a new AU with SICAM TOOLBOX II and create with this configuration a SD card
- Plug the SD card into CP-2016 and switch on the device
- Wait until the RY LED lights (can last several minutes)

Comparison between Factory Settings and Default Settings

The difference between a configuration of standard settings and a configuration after a reset of the device to its factory settings is shown in the following table:

Configuration	Factory Settings	Standard Settings 1)
Firmware/applications	CPCI85, CPC80, SWEB00 (current version at the time of production)	CPCI85, CPC80, SWEB00 (current version at the time of production)
Region number	249	Defined during creation of an AU
Component number	254	Defined during creation of an AU
X3 (LAN 1) TCP/IP Addresse	172.16.0.3	172.16.0.3
One Click to Connect (CP-8031/CP-8050)	enabled via X3 (LAN1) DHCP	disabled
Remote operation	enabled via X3 (LAN 1)	disabled
WEB Browser for SICAM WEB (HTTPS)	enabled via X3 (LAN 1)	enabled via X3 (LAN 1)
Connection to SICAM TOOLBOX II via serial interface	enabled via X5	enabled via X5
Standard user	Administrator (Password not set)	Administrator (Password not set)

1) State after configuration of CP-8031/CP-8050 via SICAM TOOLBOX II

3.3.16 Storage of Passwords in SICAM A8000 Series / SICAM RTUs

Preshared keys and passwords, which are used for authentication, are stored securely in SICAM A8000 Series / SICAM RTUs.

SICAM A8000 Series:
User passwords are stored in the form of salted HASH. SWEB00 05.00 or higher is required for user management in SWEB.

SICAM A8000 Series/SICAM RTUs:
Preshared keys (for, e.g., IPSec, SNMP, Radius, …) are stored in an encrypted form.

3.3.17 Connection of Systems without Security-Functions

Automation systems without security functions can be connected by using a SICAM AK 3, using 2 processor modules, e.g., CP-2016 and SM-2558, as “Hardware-Based Application-Layer-Firewall”.

See also: Substation Zone with Segmentation through “Hardware-Based Application-Layer-Firewall“

3.4 SICAM PTS Protocol Test System

Included among the hardening measures to be applied with **SICAM PTS Protocol Test System**:

- Windows System Hardening

Hint

A collection of best practice hardening guides for various operating systems, server services and standard applications can be found e.g. at the Center for Internet Security (HTTPS://www.cisecurity.org/)

3.4.1 Windows System Hardening

Windows system hardening has to be performed according to the manual Secure Substation, refer to:

https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&mandator=ic_sg&id1=DLA20_114

3.5 SICAM Device Manager

Included among the hardening measures to be applied with **SICAM Device Manager**:

- Windows System Hardening

Hint

A collection of Best-Practice hardening guides for various operating systems, server services and standard applications can be found e.g. at the Center for Internet Security (http://www.cisecurity.org)

3.5.1 Windows System Hardening

Windows system hardening has to be performed according to the manual Secure Substation, refer to:

https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&mandator=ic_sg&id1=DLA20_114

3.6 SICAM TOOLBOX II

Included among the hardening measures to be applied with **SICAM TOOLBOX II**:

- Windows System Hardening
- Deinstallation or deactivation of unnecessary software components (ST-Emulation, message simulation, data flow test, …)
- Deactivation of unnecessary system and communication services (remote operation, remote maintenance)
- Deactivation of unnecessary standard users
- Activation of configuration options that increase security
- Limitation of the rights of users and programs

Hint

A collection of Best-Practice hardening guides for various operating systems, server services and standard applications can be found e.g. at the Center for Internet Security (http://www.cisecurity.org)

3.6.1 Windows System Hardening

Windows system hardening has to be performed according to the manual Secure Substation, refer to:

https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&mandator=ic_sg&id1=DLA20_114

3.6.2 Solidification

If solidification software is installed, you must at least enter following exceptions for SICAM TOOLBOX II:

Configuration of the application-exceptions:

Example for „TBII 6.00“:

```
sadmin updaters C:\Siemens_EA\TBII\EMII\BIN\wait4db_tbii.exe
sadmin updaters C:\Siemens_EA\TBII\EMII\BIN\vtb.exe
```

3.6.3 Deinstallation or Deactivation of unnecessary Software Components

The security-critical software components such as ST-Emulation, message simulation, data flow test, service function online as well as the debugging function must be restricted accordingly with rights, so that only the Administrator can use these tools.

The SICAM TOOLBOX II consists of several Toolsets (EMII, PSRII, OPMII, CAEx plus, ...). Every Toolset (with the exception of EMII) can be installed or uninstalled separately.

Consequently through the deinstallation of the Toolset PSRII the customer can remove all security-critical components (ST-Emulation, message simulation, ...) from his computer.

In addition, by means of User/Role Administration, the customer has the possibility to allow access to the individual tools only for limited users.

3.6.4 Deactivation of unnecessary System and Communication Services

3.6.4.1 Remote Operation

With the remote operation tool the service interface between SICAM TOOLBOX II and SICAM RTUs can be activated for remote maintenance purposes.

The following transmission media are supported:

- SICAM TOOLBOX II Modem (dial-up modem) - Modem (dial-up modem)
- SICAM TOOLBOX II Network (TCP/IP) - Terminal Server (TCP/IP to serial)
- SICAM TOOLBOX II Network (TCP/IP) - TCP/IP (over Process LAN)
- SICAM TOOLBOX II Network (TCP/IP) - (Router – dial-up modem) - SICAM RTUs (dial-up modem)
- SICAM TOOLBOX II Null Modem - Null Modem

The start of the remote operation can take place from all online tools and the OPM II.

3.6.4.2 Remote Maintenance

See Chapter 12; User Administration

3.6.5 Deactivation of unnecessary Standard Users

During the installation following users are created:

User	Hint
PROFI	Standard user. These can be deleted by the users SAT_ROOT, SAT250, SAT_ADM and SAT_INT.
STANDARD	
ADMIN	
SAT_ROOT	These users can be disabled or removed from SICAM TOOLBOX II
SAT250	
SAT_ADM	
SAT_INT	

See also *Chapter* 12, User Administration

3.6.6 Limitation of the Rights of Users and Programs

These limitations are controlled by the Windows operating system.

With the Windows Firewall it is possible on the server only to enable selected users for the port over which the ORACLE database can be reached (e.g. by means of a specific USER-group). Other Windows users cannot reach the ORACLE database.

See also Chapter *12, User Administration*

3.7 Security Penetration Testing

All SICAM A8000 Series/SICAM RTUs LAN-Interfaces are subjected to extensive security tests. These tests are documented in detail in the document *SICAM A8000 Series RTUs Security Penetration Testing (DC0-134-2)*.

See also: Supported LAN-Services

4 Communication Protocols

Contents

4.1 Serial Communication Protocols 95
4.2 Ethernet based Communication Protocols 96
4.3 Other Layer 2 Communication Protocols 130

4.1 Serial Communication Protocols

4.1.1 Point-to-Point / Multipoint Traffic

Serial communication protocols are used in own communication networks. The data are transmitted uncoded. This is also the case when the data are transmitted over radio (e.g. relay operation).

4.1.2 Dial-Up Traffic

For the transmission of data in dial-up traffic a serial transmission protocol is used based on IEC 60870-5-101 with proprietary expansions:

- Connection setup according to AT-Hayes (Industry standard for the control of modems)
- Authentication (access control) in the private range of the IEC 60870-5-101
- Transmission of data with established connection according to IEC60870-5-101 (unbalanced)
- Control information for tripping a connection in the private range of the IEC60870-5-101

→ No verification of the telephone number of the calling participant!
→ No encoding of the data during the transmission!

For the transmission of telecontrol data in dial-up traffic, in most cases the communication takes place over public communication networks (PSTN, GSM, ISDN), which enables global access of systems to the stations. So that the stations in dial-up traffic are protected against unauthorized access, appropriate measures are required.

To protect the central station and remote stations against unauthorized access and manipulation, the following measures can be used in the transmission protocol for the transmission of telecontrol data in dial-up traffic:

- Phone number concept
- Transmission protocol
- Identification of the calling station
- Authentication (with password and access code)

For details about these measures, refer to document *SICAM RTUs – Common Functions – Protocol Elements; Chapter Security in Dial-Up Traffic.*

4.2 Ethernet based Communication Protocols

4.2.1 Ethernet based IO Bus (EbIO)

Ethernet interfaces of CP-8031/CP-8050 can be used as EbIO.

EbIO is based on a proprietary protocol on Ethernet-level (no IP, no TCP/UDP).
Data on EbIO are encrypted and authenticated.

4.2.2 IP-based Protocols SICAM A8000 CP-8031/CP-8050

SICAM A8000 CP-8031/CP-8050 supports optional encryption by means of IPSec VPN.

All IP-based protocols in SICAM A8000 Series verify the IP-address of the remote station, i.e. messages are only accepted from certain IP-addresses.

Protocols can be encrypted via TLS 1.2, or, alternatively, unencrypted protocols are transmitted through an encrypted IPSec tunnel. Both methods cannot be used in parallel (simultaneously). CP-8031/CP-8050 support TLS and IPSec simultaneously.

The maximum amount of encrypted IPSec communication channels is limited to no more than 8 per AU.

The maximum amount of encrypted TLS communication channels is limited to no more than 25 per PRE.

Hint

Encoding must take place at the lower network levels (e.g. through SSL/TLS-encoding or with VPN-technology).

For a central user management the external authentication by means of RADIUS via UDP or TLS-based LDAP is provided. Further details are described in the *SICAM A8000* CP-8031/CP-8050 Manual.

One Click To Connect:

- DHCP-Server is used in case to provide dynamic IP addresses
- DNS-Server is used in case to resolve the FQDN of the devices

Refer also to 3.3.2.1.

4.2.2.1 IPSec VPN in SICAM A8000 CP-8031/CP-8050

IPSec VPN (Internet Protocol Security – Virtual Private Network) is an extension of the Internet Protocol (IP) for encryption and authentication mechanisms. IPSec VPN actively establishes a VPN tunnel (initiator), which guarantees the required confidentiality, authenticity and integrity of data transmission in IP networks. The termination of the IPSec VPN tunnel takes place in a network router (tested systems: Cisco IOS, Cisco ASA, Scalance). SICAM A8000 CP-8031/CP-8050 (from CPCI85 Rev.01.10) support up to 8 parallel IPSec VPN tunnels.

Thus, it is possible, to completely secure the IEC 60870-5-104 communication between a SICAM RTUs and a higher-level control center, even if the connection is running over a public network.

SICAM A8000 CP-8031/CP-8050 uses the IKE-protocol (internet key exchange) and the PSK-authentication process (pre-shared key). The used key (preshared key) can be set by means of an engineering tool (e.g. SICAM TOOLBOX II) and it is securely stored both in SICAM TOOLBOX II and SICAM A8000 CP-8031/CP-8050.

Preconditions:

System	Firmware	PRE	SICAM TOOLBOX II	SICAM WEB
SICAM A8000 CP-8031/CP-8050	CPCI85 Rev. 01.10		V6.01	n.a.

Supported ciphers, refer to IPSec Parameter.

Hint

For configuration examples for IPSec VPN see manual: *SICAM A8000 CP-8031/CP-8050*, chapter "*Use Cases*".

4.2.2.1.1 Activation of IPSec VPN

In order to activate IPSec VPN for the Ethernet interface you need to set following parameter/value in the system-technical parameter of the BSE:

`Security | IP Security enabled` : **YES**

Afterwards you have access to the configuration parameter of the IPSec VPN connection under `Security | IP security` .

Hint

IPSec VPN tunnel can be established via following Ethernet interfaces:
CP-8031/CP-8050, CI-8520: LAN1-LAN50

4.2.2.1.2 IPSec Parameter

Parameter	Value or Format	Default value
IP security		
ICMP ping reply		
IPSec VPN tunnel 1 enabled		
IPSec VPN tunnel 2 enabled		
Local site		
Identifier (Local ID)	IP-address or FQDN or User-FQDN; recommended: FQDN	*)
VPN client IP-address	IP V4 address	-
VPN client default gateway	IP V4 address	-
VPN client subnet mask	IP V4 address	
Remote site 1		
Identifier (Remote ID)	IP V4-address or FQDN or User-FQDN; recommended: FQDN	*)
IP-Address	IP V4 address, (for routing in tunnel 1)	-
Subnet IP-Address	IP V4 address, (for routing in tunnel 1) **)	-
Subnet mask	IP V4 address, (for routing in tunnel 1)	-
IKE security associations 1		
Internet key exchange (IKE) Version	Version 1 Version 2 (recommended)	Version 2
SA lifetime (timeout)	120 – 2 147 483 647 Sek.	1720800 sec.
Auto-selection of authentication & encryption	No Yes (recommended)	Yes
If Auto-selection of authentication & encryption = No, then Encryption algorithm	AES-128 AES-192 AES-256	AES-128
If Auto-selection of authentication & encryption = No, then Authentication algorithm	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	HMAC-SHA1
If Auto-selection of authentication & encryption = No, then Diffie Hellman Group	1024-bit (group 2) 1536-bit (group 5) 2048-bit (group 14)	group 2

IPSec authentication		
Pre-shared Key	Maximum 128 characters (PSK can only be set, old PSK cannot be read!)	-
IPSec security associations 1		
SA lifetime (timeout)	300 to 2 147 483 647 sec.	172 800 sec.
SA lifetime (data size limit)	20 Kbyte to 128 MByte	-
Auto-selection of authentication & encryption	No Yes (recommended)	Yes
If Auto-selection of authentication & encryption = No, then Encryption algorithm	AES-128 AES-192 AES-256	AES-128
If Auto-selection of authentication & encryption = No, then Authentication algorithm	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	HMAC-SHA1
If Auto-selection of authentication & encryption = No, then Diffie Hellman Group	1024-bit group (group 2) 1536-bit group (group 5) 2048-bit group (group 14)	group 2

***) Hint**

It the IKEV1- ID is empty, then only the IP-address is used (ID-type is: IP-address).
If a IKEV1- ID is set, then the ID-type is FQDN.

For IKEV2 the ID of type FQDN must be set. A missing ID causes a network IPSec error message.

PFS (Perfect forward Secrecy) is enabled in all IPSec implementations.

****) Hint**

The wildcard IP address is allowed. However, .network planning should be done with great caution.

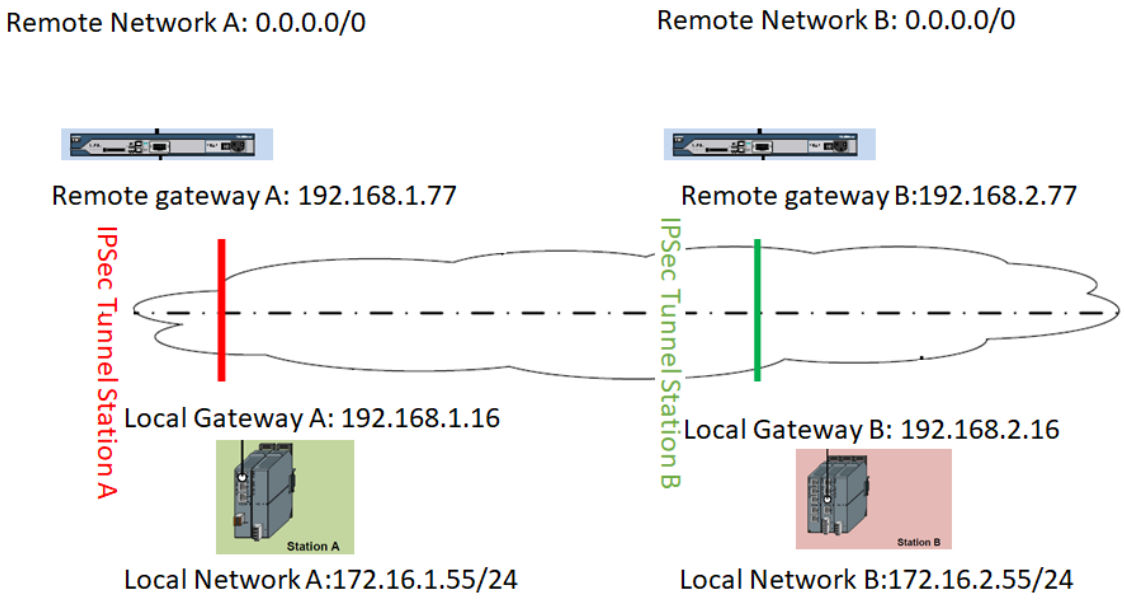
IT security: by setting the remote IP address to 0.0.0 all network components can access the device through the IPSec tunnel !

Routing should be planned with great caution, especially when using remote IP address in combination with Multiple IPSec tunnel configuration or Service Forwarding.

Hinweis

The configuration of a LAN interface (without IPSec) must not use an IP address from the IPSec Remote Subnet.

Example for a configuration with wildcard IP address 0.0.0.0 as remote IP address:



Remote IP address for IPSec tunnel is set to 0.0.0.0 in both CP-8031/CP-8050. Each CP-8031/CP-8050 is connected to the control center via an own IPSec tunnel.

Through this tunnel, a CP-8031/CP-8050 can be connected via IEC 60870-5-104 protocol with another CP-8031/CP-8050.

The IP-network of the control center and of the respective CP-8031/CP-8050 can then be freely selected. Due to the wildcard remote IP address, control center and both CP-8031/CP-8050 can be in the same subnet.

4.2.2.1.3 Changing the Pre-shared key

See *SICAM TOOLBOX II Online-Help, Chapter "OPM II", section "Security for SICAM RTUs | Pre-shared key"*.

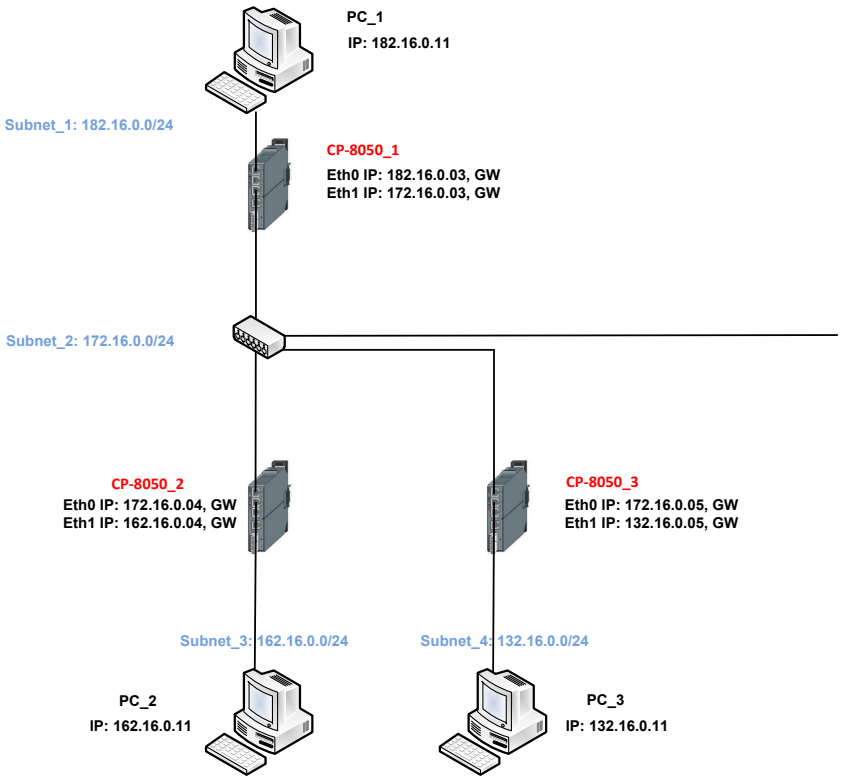
4.2.2.2 Service Forwarding

SICAM A8000 CP-8031/CP-8050 supports forwarding of TCP and UDP packets (e.g.: in a network hierarchy, SNMP requests can be forwarded through SICAM A8000 CP-8031/CP-8050 over different device network interfaces to multiple remote destinations / other devices (CP-8031/CP-8050) in different networks.

Service Forwarding: supported services:

Service	Port	Type	without IPSec	with IPSec
SNMP	161	UDP	x	x
SNMP Traps	162	UDP	x	x
HTTP	80	TCP	x	x
HTTPS	443	TCP	x	x
Syslog	514	UDP	x	x
Radius	1812	UDP	x	x
NTP	123	UDP	x	x
LDAP	389	TCP	x	x
IEC 60870-104	2404	TCP	x	x
EST	8085	TCP	x	x
CRL Client	80	TCP	x	x
IEC 61850	102	TCP	x	x

After configuring the respective routing and firewall tables for service forwarding an engineer can now access a PC_2 in Subnet_3 and/or PC_3 in Subnet_4 from PC_1 in Subnet_1 via Subnet_2 as shown in the picture below:



Respective parameters can be found under
`System settings | Network settings | Services | Service forwarding`:

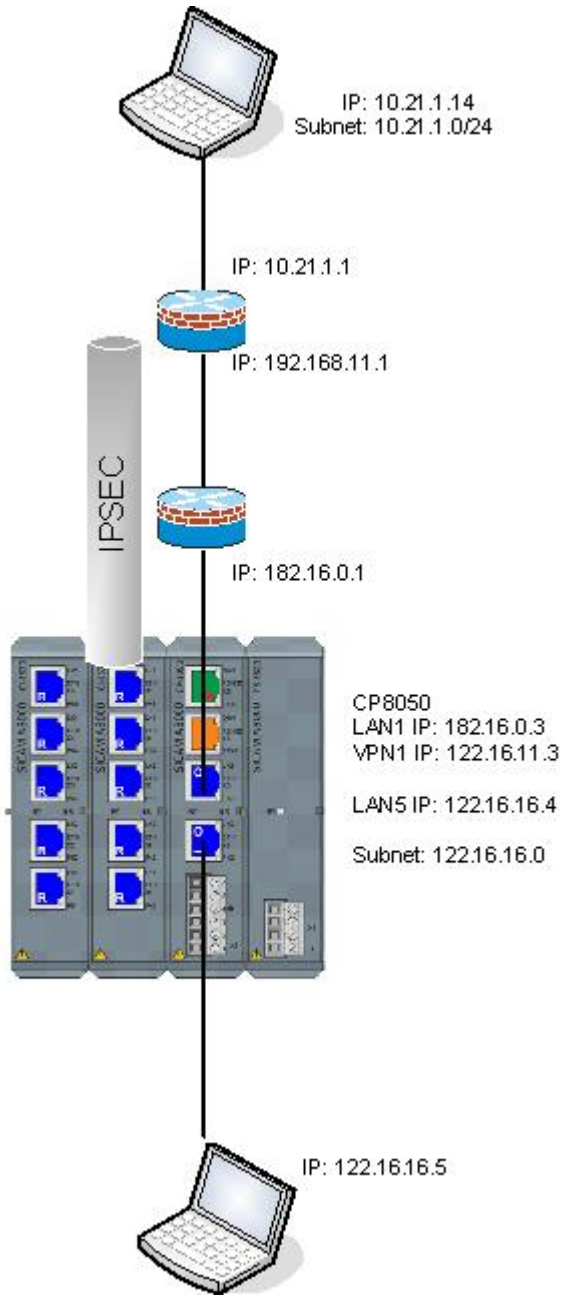
CP-8031/CP-8050_1									
input interface	**output interface**	**source IP address**	**source subnet mask**	**source IP gateway**	**destination IP address**	**destination subnet mask**	**destination IP gateway**	**protocol**	**port**
LAN1	LAN2	182.16.0.0	255.255.255.0		162.16.0.0	255.255.255.0	172.16.0.4	TCP	443
LAN1	LAN2	182.16.0.0	255.255.255.0		132.16.0.0	255.255.255.0	172.16.0.5	TCP	443
LAN1	LAN2	0.0.0.0			162.16.0.0	255.255.255.0	172.16.0.4	UDP	161
LAN1	LAN2	0.0.0.0			132.16.0.0	255.255.255.0	172.16.0.5	UDP	161

CP-8031/CP-8050_2									
input interface	**output interface**	**source IP address**	**source subnet mask**	**source IP gateway**	**destination IP address**	**destination subnet mask**	**destination IP gateway**	**protocol**	**port**
LAN1	LAN2	182.16.0.0	255.255.255.0	172.16.0.3	162.16.0.0	255.255.255.0		TCP	443
LAN1	LAN2	0.0.0.0			162.16.0.0	255.255.255.0		UDP	161

CP-8031/CP-8050_3									
input interface	**output interface**	**source IP address**	**source subnet mask**	**source IP gateway**	**destination IP address**	**destination subnet mask**	**destination IP gateway**	**protocol**	**port**
LAN1	LAN2	182.16.0.0	255.255.255.0	172.16.0.3	132.16.0.0	255.255.255.0		TCP	443
LAN1	LAN2	0.0.0.0			132.16.0.0	255.255.255.0		UDP	161

Port „0“ for Global Forwarding, see below.

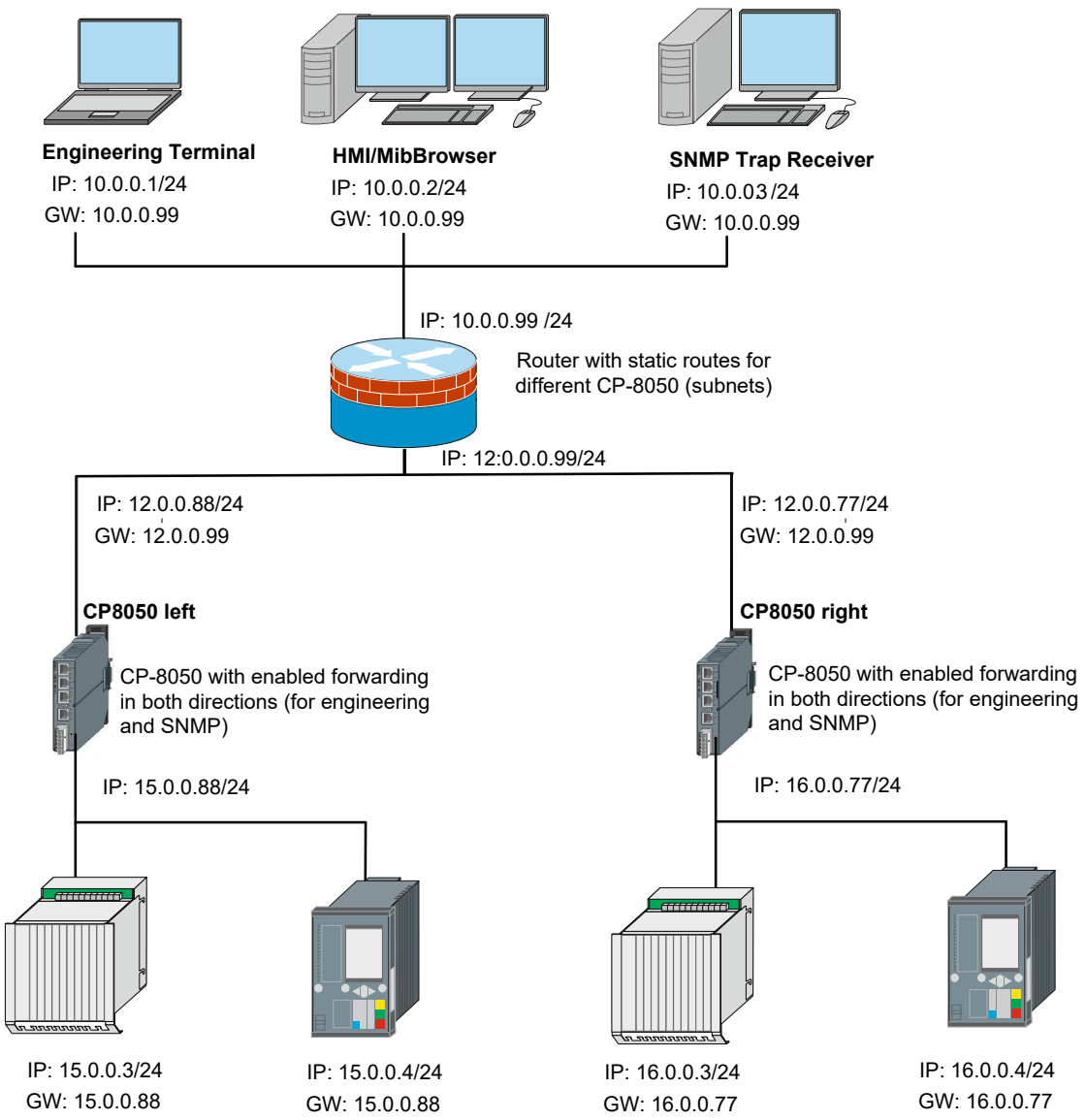
Example: Service Forwarding with IPSec-tunnel:



Input interface	Output interface	Source IP address	Source subnet mask	Source IP gateway	Destination IP address	Destination subnet ma	Destination IP gatewa	Protocol	Port
LAN5	VPN1	122.16.16.0	255.255.255.0	0.0.0.0	10.21.1.0	255.255.255.0	182.16.0.1	UDP	123
LAN5	VPN1	122.16.16.0	255.255.255.0	0.0.0.0	10.21.1.0	255.255.255.0	182.16.0.1	UDP	162
LAN5	VPN1	122.16.16.0	255.255.255.0	0.0.0.0	10.21.1.0	255.255.255.0	182.16.0.1	UDP	514
LAN5	VPN1	122.16.16.0	255.255.255.0	0.0.0.0	10.21.1.0	255.255.255.0	182.16.0.1	UDP	1812
VPN1	LAN5	10.21.1.0	255.255.255.0	182.16.0.1	122.16.16.0	255.255.255.0	0.0.0.0	TCP	80
VPN1	LAN5	10.21.1.0	255.255.255.0	182.16.0.1	122.16.16.0	255.255.255.0	0.0.0.0	UDP	161
VPN1	LAN5	10.21.1.0	255.255.255.0	182.16.0.1	122.16.16.0	255.255.255.0	0.0.0.0	TCP	443
VPN1	LAN5	10.21.1.0	255.255.255.0	182.16.0.1	122.16.16.0	255.255.255.0	0.0.0.0	TCP	2404

Every device needs a unique IP Address, to allow a control center terminal to connect to each network device via its IP address.

Example for SNMP management in a network (four different subnets) with control center via two CP-8031/CP-8050:



Respective parameters can be found under `System settings | Network settings | Services | Service forwarding:`

CP8050 left										
	input interface	**output interface**	**source IP address**	**source subnet mask**	**source IP gateway**	**destination IP address**	**destination subnet mask**	**destination IP gateway**	**protocol**	**port**
For, e.g.: SNMP Traps	LAN2: 15.0.0.88	LAN1: 12.0.0.88	0.0.0.0			10.0.0.0	255.255.255.0	12.0.0.99	UDP	162
For, e.g.: SNMP MibBrowser	LAN1: 12.0.0.88	LAN2: 15.0.0.88	0.0.0.0			15.0.0.0	255.255.255.0		UDP	161
For Engineering	LAN1: 12.0.0.88	LAN2: 15.0.0.88	10.0.0.0	255.255.255.0	12.0.0.99	15.0.0.0	255.255.255.0		TCP	443

CP8050 right										
	input interface	**output interface**	**source IP address**	**source subnet mask**	**source IP gateway**	**destination IP address**	**destination subnet mask**	**destination IP gateway**	**protocol**	**port**
For, e.g.: SNMP Traps	LAN2: 16.0.0.77	LAN1: 12.0.0.77	0.0.0.0			10.0.0.0	255.255.255.0	12.0.0.99	UDP	162
For, e.g.: SNMP MibBrowser	LAN1: 12.0.0.77	LAN2: 16.0.0.77	0.0.0.0			16.0.0.0	255.255.255.0		UDP	161
For Engineering	LAN1: 12.0.0.77	LAN2: 16.0.0.77	10.0.0.0	255.255.255.0	12.0.0.99	16.0.0.0	255.255.255.0		TCP	443

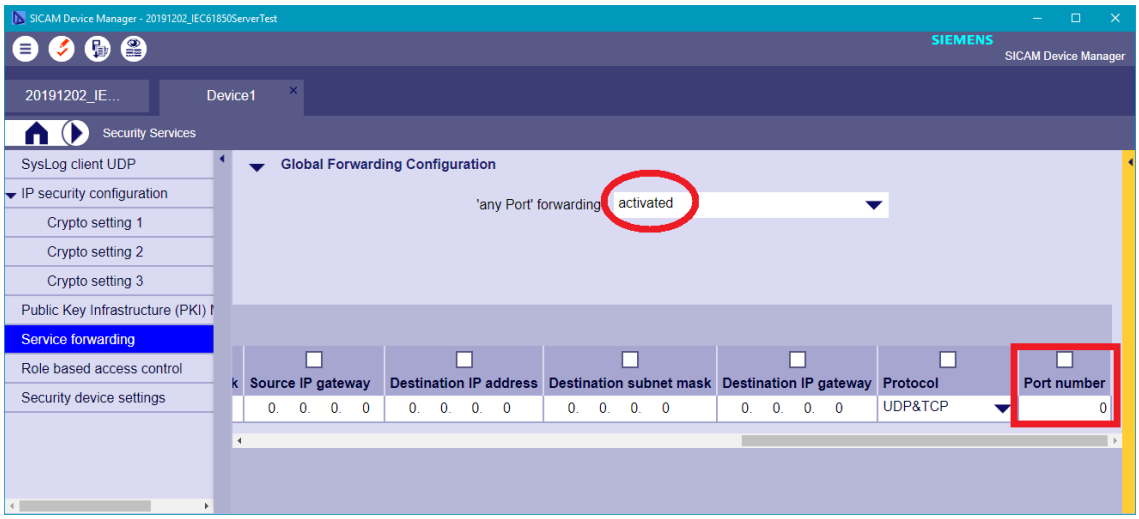
Port „0“ for Global Forwarding, see below.

CP-8031/CP-8050 supports **Global Forwarding**,

All port numbers can be forwarded depending on the defined IP-addresses.

In SICAM Device Manager, set the „any Port" forwarding parameter to *activated*.

Set Portnumber to „0":



Settings for **Global Forwarding** in SICAM Device Manager.

4.2.2.3 SNMP Agent & Traps

SICAM A8000 CP-8031/CP-8050 supports SNMP (firmware version CPCI85 Rev. 1.20 or higher).

Only the secure version SNMPv3 (according to RFC 2574) is supported (in contrast to SICAM A8000 Serie CP-8000/CP-802x and SICAM AK) using the following cipher suites (according to RFC 7630 and RFC 3414):

- MD5
- SHA1
- SHA2 (SHA-224, SHA-256, SHA-384, SHA-512)
- CBC-DES
- AES-128
- AES-256

The User Based Security Model (USM) according to RFC 3414 is supported, but dynamic User Management (this is part of the engineering data) is not supported.

Hint

SNMP is not designed for device configuration.

4.2.2.3.1 Changing SNMP-Passwords

SICAM TOOLBOX II:

Passwords for SNMPv3 users are defined in the system-technical parameters of the basic system element under:

```
System settings | Network settings |.Services | SNMP | Crypto settings |
Settings 1-5 | PSK Authentication
```

and under:

```
System settings | Network settings |.Services | SNMP | Crypto settings |
Settings 1-5 | PSK encryption
```

Passwords are assigned to a certain SNMPv3 user:

```
System settings | Network settings | Services | SNMP | User | User
configuration | User 0-3 | Crypto settings
```

SICAM Device Manager:

Defining passwords for SNMPv3 users under:

```
System | Communication | Server services | SNMP | Crypto settings |
Settings 1-5 | PSK Authentication
```

and under:

```
System | Communication | Server services | SNMP | Crypto settings |
Settings 1-5 | PSK encryption
```

Hint

There are no default passwords. . When activating SNMP for the first time, passwords must be defined.

4.2.2.4 SYSLOG Client

SICAM A8000 Series CP-8031/CP-8050 provides a security logbook (syslog-client). The syslog-client captures relevant events related to security and transmits them to an external syslog server.

For more details, see 9.1 Security Logging.

4.2.2.5 IP Communication Matrix SICAM A8000 CP-8031/CP-8050

In this table, “SICAM A8000 Series” always refers to SICAM A8000 CP-8031/CP-8050.

Service	Layer 4 Prot.	Layer 7 Protocol	From Host (Client)	From Port (Client)	To Host (Server)	To Port (Server)	Process control	System monitoring	System diagnostics	System parameter setting
DNS Server	UDP	DNS	PC	>1024	SICAM A8000 Series	67/UDP (Server or Relay-Agent)				x
DHCP Client	UDP	DHCP	SICAM A8000 Series	68/UDP (Client)	PC	67/UDP (Server or Relay-Agent)				x
DHCP Server / Relay Agent	UDP	DHCP	PC	67/UDP (Server or Relay-Agent)	SICAM A8000 Series	68/UDP (Client)				x
NTP Time Setting	UDP	NTP	SICAM A8000 Series	123	NTP Server	123 (symmetric mode)	x			
NTP Time Setting	UDP	NTP	SICAM A8000 Series	123	SICAM AK 3, SICAM BC	123 (symmetric mode)	x			
SNMP	UDP	SNMP	PC	>1024	SICAM AK 3 SICAM A8000 Series	161		x	x	
SNMP Trap	UDP	SNMP	SICAM A8000 Series	>1024		162		x	x	
IPsec VPN	UDP	-	SICAM A8000 Series	500, 4500	CISCO Router	500, 4500	x	x	x	x
Syslog Client	UDP	-	SICAM A8000 Series	514	Syslog Server	514 *)		x		
RADIUS authentication protocol	UDP	-	SICAM A8000 Series	>1024	RADIUS AAA Server	1812 *)	x	x	x	x
Toolbox, remote Operation - Start	ICMP	ECHO	Toolbox-PC		SICAM A8000 Series				x	x
LDAP Authentication protocol CP-8031/CP-8050 only)	TCP			>1024	389		x	x	x	x
Web	TCP	HTTP	PC with browser		SICAM A8000 Series	80			x	x
Web	TCP	HTTPS	PC with browser		SICAM A8000 Series	443			x	x

Service	Layer 4 Prot.	Layer 7 Protocol	From Host (Client)	From Port (Client)	To Host (Server)	To Port (Server)	Process control	System monitoring	System diagnostics	System parameter setting
Remote Operation TBII	TCP	HTTP	Toolbox PC		SICAM A8000 Series	80			x	x
Remote Operation TBII	TCP	HTTPS	Toolbox PC		SICAM A8000 Series	443			x	x
Process Communication	TCP	IEC 60870-5-104	SICAM A8000 Series SICAM PTS	>1024	SICAM PAS SICAM SCC SICAM AK 3 SICAM BC SICAM A8000 Series SICAM PTS	2404	x	x	x	x
Process Communication	TCP	DNP(i)	other DNP(i)-System SICAM A8000 Series	>1024	other DNP(i)-System SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC	20000	x	x		
Process Communication	TCP	IEC 61850	SICAM A8000 Series SICAM PTS	>1024	SICAM PAS SICAM SCC SIPROTEC SICAM AK 3 SICAM BC SICAM PTS	102	x	x	x	x
Process Communication	TCP	MODBUS TCP/IP Slave	SICAM A8000 Series	>1024	SICAM AK 3, AK SICAM TM SICAM BC	502	x	x		
Process Communication	TCP	MODBUS TCP/IP Master	SICAM A8000 Series	>1024	SICAM AK 3 SICAM BC	502	x	x		
SICAM PTS Protocol Test System Licence Protection	TCP	-	PC	>1024	LICENCE	22350 22351 **)				
Debug ***)	TCP	SSH	PC		SICAM A8000 Series	22			x	
Ping	ICMP	PING	SICAM A8000 Series		SICAM A8000 Series					x
EST,…) external certificate requests	TCP	EST	SICAM CP-8031/ CP-8050	>1024	EST Server/ SICAM GridPass	8085	x			

Service	Layer 4 Prot.	Layer 7 Protocol	From Host (Client)	From Port (Client)	To Host (Server)	To Port (Server)	Process control	System monitoring	System diagnostics	System parameter setting
CRL Client	TCP	HTTP	SICAM CP-8031/ CP-8050	>1024	CRL Webserver/ SICAM GridPass	80	x			

*) The RADIUS UDP Port is freely adjustable. The syslog server port id freely adjustable.

**) SICAM PTS Protocol Test System - Licence Protection

The dongle driver (via USB) opens TCP ports 2235 and 22351. These ports are not used by SICAM PTS Protocol Test System.
It is not possible to deactivate this function within the dongle driver.

***) The given port is used exclusively for debugging. The service „Secure Shell (SSH)“ can be enabled by the parameter „Debug“.However, the access to the device is protected by a password.

The protocols or devices listed are common/typical clients or servers, it can also be third party devices. However this is to be taken from the respective project-specific design documentation

.

4.2.3 IP-based Protocols SICAM AK 3, SICAM BC, SICAM A8000 CP-8000/21/22

All IP-based protocols in SICAM A8000 Series / SICAM RTUs verify the IP-address of the remote station i.e. messages are only accepted from certain IP-addresses.

With the communication protocol IEC 60870-5-104 the transmission of data can be either uncoded or encrypted (using TLS 1.2 encryption or IPSec VPN).

SICAM A8000 Series and SICAM AK 3 with SM-2558/ETA4 support optional encryption by means of IPSec VPN.

Protocols can be encrypted via TLS 1.2, or, alternatively, unencrypted protocols are transmitted through an encrypted IPSec tunnel. Both variants cannot be used in parallel. A parameterization error will occur if TLS and IPSec are enabled.

The maximum amount of encrypted IPSec communication channels is limited to:

System	Firmware	PRE	amount of encrypted IPSec communication channels
SICAM A8000 Series CP-8000/CP-802x	CPC80 from Rev. 10		2
SICAM AK 3	CPCX26 from Rev. 03		2
SICAM AK 3	PCCX26 from Rev. 03		4
SICAM AK 3, SICAM BC		SM-2558/ETA4 from Revision 05	1

The maximum amount of encrypted TLS communication channels is limited to:

System	PRE-Firmware	amount of encrypted TLS communication channels
SICAM A8000 Series CP-8000/CP-802x	ET84 from Rev. 05 ET84 from Rev. 05.10	4 8 *) **)
SICAM A8000 Series CP-8000/CP-802x	ET85 from Rev. 03.11 Client ET85 from Rev. 03.11 Server	25 ***) 6
SICAM AK 3	ET24 from Revision 03 ET24 from Revision 04.10	4 25 *)
SICAM AK 3	ET25 from Revision 03.11 Client ET25 from Revision 03.11 Server	100 6
SICAM AK 3	SM-2558/ETA4 from Revision 09 SM-2558/ETA4 from Revision 10.10	8 25 *)
SICAM AK 3	SM-2558/ETA5 from Revision 03.11 Client SM-2558/ETA5 from Revision 03.11 Server	100 6

*) Tested with following cipher suites: TLS_RSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. Amount of TLS connections and performance can be negatively influenced by using different cipher suites

**) max. amount of encrypted TLS connections of the device

***) amount of connections can be increased if server function on firmware is disabled

For TLS encryption a crypto-chip must be integrated both in master module and in PRE-firmware. There is no crypto-chip integrated in SICAM BC, therefore SICAM BC does not support TLS encryption.

Hint

Encoding must take place at the lower network levels (e.g. through SSL/TLS-encoding or with VPN-technology).

Authentication:

For the external authentication of users (from CPC80 version 09) an access to an external server is provided by means of RADIUS.

AutoConfig:

For a customer specific function (download of SICAM WEB Backup-Files) the protocols DHCP, DNS and TFTP are used.

- DHCP Client is used in this case to obtain a dynamic IP address.
- DNS Client is used in this case to resolve the FQDN of the TFTP servers
- TFTP Client is used in this case to load the SICAM WEB Backup-File from the server

Further details are described in the corresponding *SICAM A8000 Series* Manual.

4.2.3.1 IPSec VPN in SICAM A8000 Series / SICAM RTUs

IPSec VPN (Internet Protocol Security – Virtual Private Network) is an extension of the Internet Protocol (IP) for encryption and authentication mechanisms. IPSec VPN actively establishes a VPN tunnel (initiator), which guarantees the required confidentiality, authenticity and integrity of data transmission in IP networks. The termination of the IPSec VPN tunnel takes place in a network router (tested systems: Cisco IOS, Cisco ASA, Scalance). SICAM AK 3 and the SICAM A8000 Series (from CPC80 Rev.10) support two parallel IPSec VPN tunnel.

Thus, it is e.g. possible, to completely secure the IEC 60870-5-104 communication between a SICAM RTUs and a higher-level control center, even if the connection is running over a public network .

SICAM A8000 Series and SICAM RTUs use the IKE-protocol (internet key exchange) and the PSK-authentication process (pre-shared key). The used key (preshared key) can be set by means of an engineering tool (e.g. SICAM TOOLBOX II). It is securely stored both in SICAM TOOLBOX II and SICAM RTUs.

Preconditions:

System	Firmware	PRE	SICAM TOOLBOX II	SICAM WEB
SICAM A8000 CP-8000/ CP-802x	CPC80 from rev. 10		V5.11 HF3	SWEB00 from rev. 02.01
SICAM AK 3	CPCX26 from rev. 03		V5.11 HF3	-
	PCCX26 from rev. 03		V5.11 HF3	-
SICAM AK 3, SICAM BC		SM-2558/ETA4 from revision 05 *)	V5.11 HF3	-

*) ETA4 supports only one IPSec Tunnel

Hint
For configuration examples see manual: *SICAM A8000 Series*, chapter "*Use Cases*".

Supported ciphers, refer to IPSec Parameter.

4.2.3.1.1 Activation of IPSec VPN

In order to activate IPSec VPN for the Ethernet interface you need to set following parameter/value in the system-technical parameter of the BSE:

`Network settings | Security | IP Security enabled` : **YES**

Afterwards you have access to the configuration parameter of the IPSec VPN connection under `Network settings | Security | IP security`.

Hint
IPSec VPN tunnel can be established via following ethernet interfaces:
- SICAM A8000 Series..... X1
- SICAM AK 3..... X0

4.2.3.1.2 IPSec Parameter

Parameter	Value or Format	Default value
IP security		
`ICMP ping reply`		
`IPSec VPN tunnel 1 enabled`		
`IPSec VPN tunnel 2 enabled`		
Local site		
`Identifier (Local ID)`	IP-address or FQDN or User-FQDN; recommended: FQDN	*)
`VPN client IP-address`	IP V4 address	-
`VPN client default gateway`	IP V4 address	-
`VPN client subnet mask`	IP V4 address	

Remote site 1		
Identifier (Remote ID)	IP-address or FQDN or User-FQDN; recommended: FQDN	*)
IP-Address	IP V4 address, (for routing in tunnel 1)	-
Subnet IP-Address	IP V4 address, (for routing in tunnel 1)	-
Subnet mask	IP V4 address, (for routing in tunnel 1)	-
IKE security associations 1		
Internet key exchange (IKE) Version	Version 1 Version 2 (recommended)	Version 2
SA lifetime (timeout)	120 – 2 147 483 647 Sec.	86400 sec.
Auto-selection of authentication & encryption	No Yes (recommended)	Yes
If Auto-selection of authentication & encryption = No, then Encryption algorithm	DES 3DES AES-128 AES-192 AES-256	AES-128
If Auto-selection of authentication & encryption = No, then Authentication algorithm	HMAC-SHA1 HMAC-MD5 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	HMAC-SHA1
If Auto-selection of authentication & encryption = No, then Diffie Hellman Group	768-bit group (group 1) 1024-bit group (group 2) 1536-bit group (group 5) 2048-bit group (group 14)	group 2
IPSec authentication		
Pre-shared Key	Maximum 128 characters (PSK can only be set, old PSK cannot be read!)	-
IPSec security associations 1		
SA lifetime (timeout)	300 to 2 147 483 647 sec.	3600 sec.
SA lifetime (data size limit)	20 Kbyte to 128 MByte	12000
Auto-selection of authentication & encryption	No Yes (recommended)	Yes

If Auto-selection of authentication & encryption = No, then Encryption algorithm	3DES AES-128 AES-192 AES-256	AES-128
If Auto-selection of authentication & encryption = No, then Authentication algorithm	HMAC-SHA1 HMAC-MD5 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	HMAC-SHA1
If Auto-selection of authentication & encryption = No, then Diffie Hellman Group	768-bit group (group 1) 1024-bit group (group 2) 1536-bit group (group 5) 2048-bit group (group 14)	group 2
IPSec tunnel supervision by ping 1		
Ping enabled	No Yes (recommended) **)	No
Ping cycle time	180 … 3600 s	180 s
Ping peer IP-address	Peer Host behind the tunnel	-

***) Hint**

It the IKEV1- ID is empty, then only the IP-address is used (ID-type is: IP-address).
If a IKEV1- ID is set, then the ID-type is FQDN.

For IKEV2 the ID of type FQDN must be set. A missing ID causes a network IPSec error message.

PFS (Perfect forward Secrecy) is enabled in all IPSec implementations.

****) Hint**

Ping enabling for IKEV1 recommended..

Ping enabling for IKEV2 NOT recommended.

A restart of the tunnel will be triggered if there is no data transfer (IPSec over GPRS) for about 15 minutes.
A restart of the device can be triggered via configuration (software-testpoint) if there is no data transfer for about 60 minutes.

4.2.3.1.3 Changing the Pre-shared key

See *SICAM TOOLBOX II Online-Help, Chapter "OPM II", section "Security for SICAM RTUs | Pre-shared key"*.

4.2.3.2 SNMP Agent & Traps

SICAM A8000 Series/SICAM RTUs support SNMPv2 and SNMPv3 according to RFC 2574, more details can be found *in SICAM RTUs, Ax 1703, Common Functions Protocol Elements, chapter 10*.

SNMPv2 and SNMPv3, overview

System (SNMP-Agent)	Firmware (Central processing/communication supports advanced cipher suites with SHA2)
SICAM A8000 CP-8000/CP-802x (SNMP v2 and SNMP v3)	CPC80 from Rev. 12
SICAM AK 3 (SNMP v2 and SNMP v3)	CPCX26 from Rev. 4.0

Supported cipher suites according to RFC7630 and RFC3414:

- MD5
- SHA1
- SHA2 (SHA-224, SHA-256, SHA-384, SHA-512)
- CBC-DES
- AES-128
- AES-256

User based security model (USM) according to RFC 3414 is supported, but not dynamic user management (this is part of engineering data).

HMAC-SHA-2 is supported in the USM model (according to RFC 7630), as of firmware version 12 of CPC80 and as of firmware version 4 of CPCX26 (see table above).

Hint

SNMP cannot be used for configuring the device

4.2.3.2.1 Changing SNMP-Passwords

Prerequisites:

`Secure Password storage` parameter must be activated under

`Network settings | Security` before password can be defined.

Passwords for SNMPv3 users are defined by means of SICAM TOOLBOX II or SICAM Device Manager in the system-technical parameters of the basic system element under:

`Network settings | SNMP | SNMPv3 | User | User 1-4 | Password for authentication PSK`

and under:

`Network settings | SNMP | SNMPv3 | User | User 1-4 | Password for encryption PSK`

Protocols for authentication and encryption of passwords for SNMPv3 under:

`Network settings | SNMP | SNMPv3 | Authentication Protocol`

and under

`Network settings | SNMP | SNMPv3 | Privacy Protocol`

4.2.3.3 SYSLOG Client

SICAM A8000 Series/SICAM RTUs provides a security logbook (syslog-client). The syslog-client captures relevant events related to security and transmits them to an external syslog server.

For more details, refer to chapter 9.1 Security Logging.

4.2.3.4 IEC 62351-3 in SICAM A8000 Series / SICAM RTUs

4.2.3.4.1 IEC 62351-3 for IEC 60870-5-104

Optionally, an encryption according to IEC 62351-3 can be deployed for the communication connection via IEC60870-5-104.

Prerequisites:

System	Firmware	PRE
SICAM A8000 CP-8000/CP-802x	CPC80 as of Rev. 12	ET84 as of Rev. 05
SICAM A8000 CP-8031/CP-8050	CPCI85 as of Rev 02	ETI4 as of Rev 02
SICAM AK 3	CPCX26 as of Rev. 04	ET24 as of Rev. 03
	PCCX26 as of Rev. 04	ET24 as of Rev. 03
SICAM AK 3		SM-2558/ETA4 as of Rev. 09

Connection Definition

In the *Connection Definition* you can define an encrypted connection entering the name of the related certificate and private key (without file extension):

Example for CP-8000/CP-802x:

	DB	Stationsnummer (intern)	Connection	Controlling/Controlled	IP-Adresse	Verschlüsselung TLS	Dateiname TLS
0		0	aktiviert	controlled	172.16.0.4	Verschlüsselt	TESTCERT

General statements:

Uploading certificates for CP-8000/CP-802x works in the same way as for CP-8031/CP-8050, refer to chapter 3.3.10.2

Example: *file name* for connection definition: “CERT_1” for “Certficate 1”, “CERT_2” for “Certficate 2” and so on.

Already imported certifcates on SD card are displayed in SICAM WEB certificate management, refer to chapter 3.3.10.2

The name of the certificate has to be: <name>.PEM

The name of the private key has to be: <name>.key

The certificate must contain the total certificate chain including CA (Certification Authority).

TLS 1.2 as of revision 15.20 is supported.

Supported Cipher Suites TLS 1.2

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256

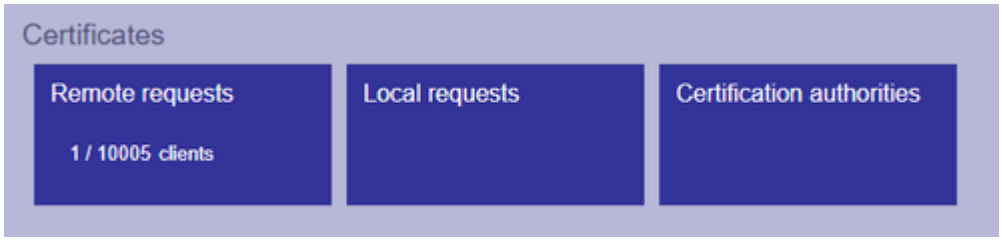
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_NULL_SHA256 *)
- TLS_ECDHE_RSA_WITH_NULL_SHA *)
- TLS_ECDHE_ECDSA_WITH_NULL_SHA *)

*) is used only if the parameter `Encryption TLS` is set to Null-Cipher

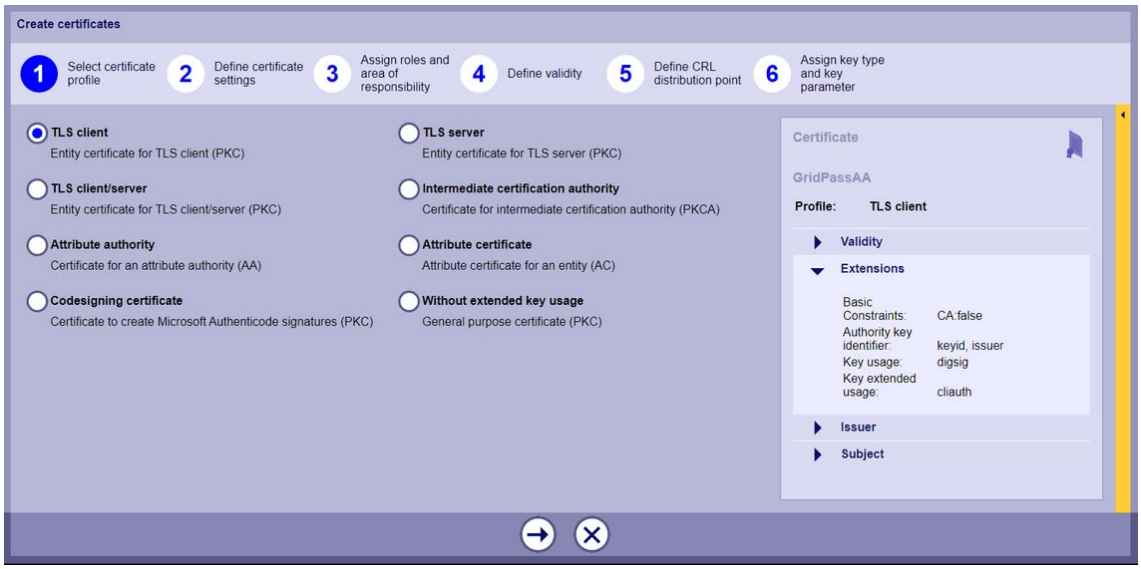
4.2.3.4.2 Generating Certificates

Certificates for TLS encryption have to be stored in the *IN_CERTS* folder on SD-card.

It is recommended that for import, export and creation of certificates SICAM GridPass is used (refer to chapter *Certificate Management* of the respective manual).



GUI of SICAM GridPass

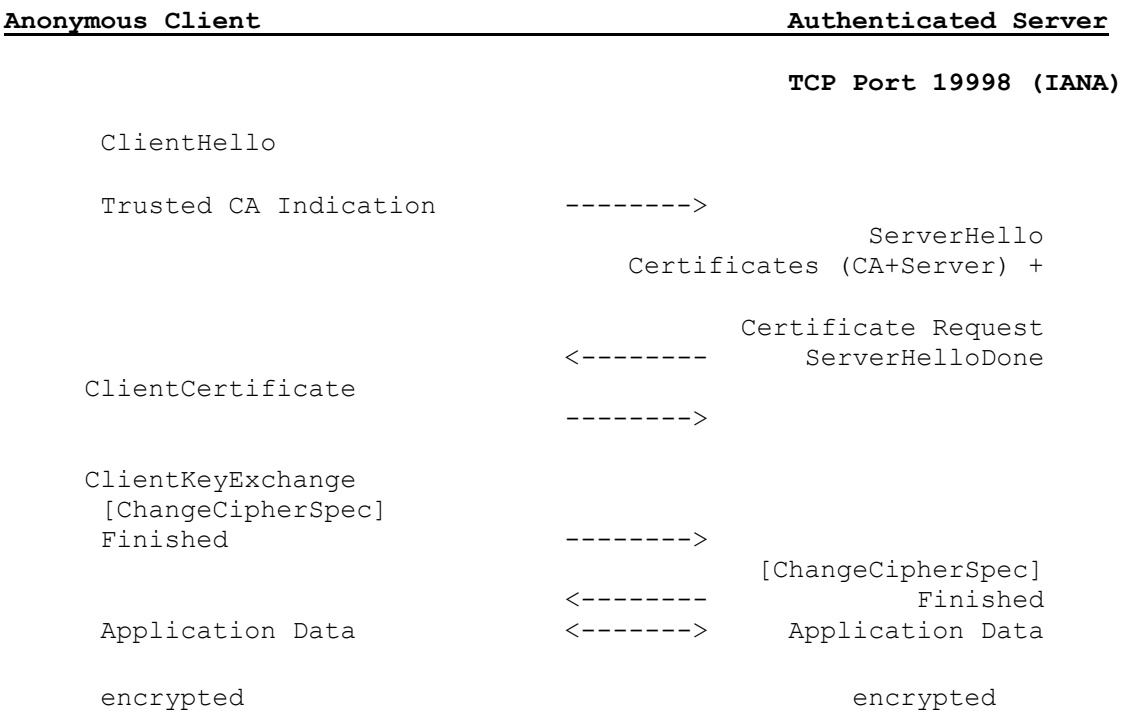


Creating certificates by means of SICAM GridPass

4.2.3.5 EC 60870-5-104 with TLS-Encryption according to IEC 62351-3: Performance and Sizing

TLS-Handshake Diagram (most widely used case)[1)]:

[1)]: Source: http://netsekure.org/2010/03/tls-overhead/



- *ClientHello*: the average size of initial client hello is about 160 to 170 bytes. It will vary based on the number of ciphersuites sent by the client as well as how many TLS *ClientHello* extensions are present. If session resumption is used, another 32 bytes need to be added for the Session ID field.
- *ServerHello*: this message is a bit more static than the ClientHello, but still variable size due to TLS extensions. The average size is 70 to 75 bytes.
- *Certificate Request*: average size 310 to 330 bytes.
- *Certificate:* this message is the one that varies the most in size between different servers. The message carries the certificate of the server, as well as all intermediate issuer certificates in the certificate chain (minus the root cert). Since certificate sizes vary quite a bit based on the parameters and keys used, I would use an average of 1500 bytes per certificate. The other varying factor is the length of the certificate chain up to the root certificate. To be on the more conservative side of what is on the web, let's assume 4 certificates in the chain. Overall this gives us about 6k for this message.
- *Client Certificates:* The message carries the certificate of the client. Since certificate sizes vary quite a bit based on the parameters and keys used, an average of 1500 bytes per certificate is to be assumed
- *ClientKeyExchange:* let's assume again the most widely used case – RSA server certificate. This corresponds to size of 262 bytes for this message.
- Certificate Verify: 264 bytes
- New Session Ticket: 1114 bytes
- *ChangeCipherSpec:* fixed size of 1 (technically not a handshake message)
- *Finished*: For TLSv1.0: 12 bytes.

Messages exchanged have TLS Record header for each record sent (5 bytes), as well as TLS Handshake header (4 bytes).

The most common case can be simplified such that each arrow in the handshake diagram is a TLS Record, so we have 4 Records exchanged for total of 20 bytes.

Each message has the handshake header (except the *ChangeCipherSpec* one), so we have 8 times the Handshake header for total of 32 bytes.

Example:

TLS-104 with 1 CA and RSA:

20 + 32 + 170 + 75 + 330 + 2000 + 2000 + 262 + 264 + 1114 + 2*1 + 2*12 = 6293

Depending on the parameters *time* and *size* a key exchange will be done, minimum once per day.

Overhead in the wire for the encrypted application data:

Once the key exchange was done, every packet is encrypted.

The data is carried in TLS Records over the wire, so there are 5 bytes of header. Since data is encrypted and integrity protected, there is additional overhead that is incurred.

Let's assume that the cipher suite negotiated between the client and the server is TLS_RSA_WITH_AES_128_CBC_SHA256.

Since AES is a block cipher, it requires the data to be sized in multiple of the block size.

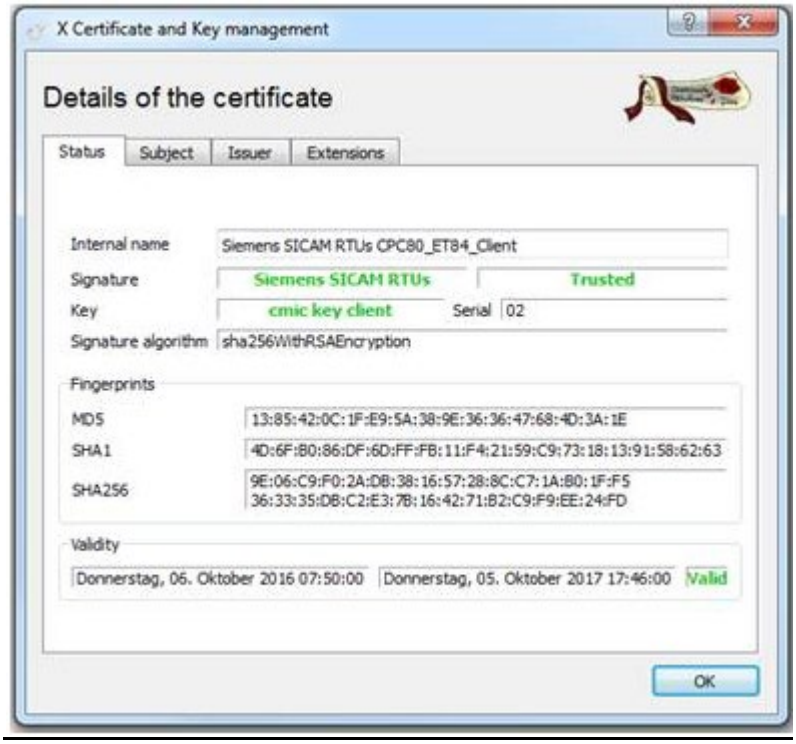
TLS 1.0 defines the encrypted data with block cipher as:

```
block-ciphered struct {
        opaque content[TLSCompressed.length];
        opaque MAC[CipherSpec.hash_size];
        uint8 padding[GenericBlockCipher.padding_length];
        uint8 padding_length;
    } GenericBlockCipher;
```

Since most implementations don't use compression, we can assume the data is the same size.
The MAC in this case is computed using SHA256, so the size will be 32 bytes. AES128 has a block size of 16 bytes, so the maximum padding we can add to the data will be 15 bytes.

In this example, the total overhead of the encrypted data is about 53 bytes (32 +15 + 5)

Certificate with RSA Keys 2048 bit



Certificate with EC Keys 256 bit

4.2.3.6 IP Communication Matrix

In this table, “SICAM A8000 Series” always refers to SICAM A8000 CP-8000 and CP-802x.

Service	Layer 4 Prot.	Layer 7 Protocol	From Host (Client)	From Port (Client)	To Host (Server)	To Port (Server)	Process control	System monitoring	System	System para-meter setting
DNS Client	UDP	DNS	SICAM A8000 Series	>1024	PC	53/UDP				x
DHCP Client	UDP	DHCP	SICAM A8000 Series	68/UDP (Client)	PC	67/UDP (Server or Relay-Agent)				x
TFTP Client	UDP	TFTP	SICAM A8000 Series	>1024		69				x
NTP Time Setting	UDP	NTP	SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC	123	NTP Server	123 (symmetric mode)	x			
NTP Time Setting	UDP	NTP	SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC	123	SICAM AK 3 SICAM BC	123 (symmetric mode)	x			
SNMP	UDP	SNMP	PC	>1024	SICAM AK 3 SICAM A8000 Series	161		x	x	
SNMP Trap	UDP	SNMP	SICAM A8000 Series	>1024		162		x	x	
IPsec VPN	UDP	-	SICAM AK 3 SICAM BC, SICAM A8000 Series	500, 4500	CISCO Router	500, 4500	x	x	x	x
Syslog Client	UDP	-	SICAM AK 3 SICAM A8000 Series Toolbox-PC	514	Syslog Server	514 *)		x		
RADIUS authentication protocol	UDP	-	SICAM A8000 Series	>1024	RADIUS AAA Server	1812 *)	x	x	x	x
NetOp Remote Control	TCP	RDP	Windows PC	>1024	Toolbox PC	6502			x	x

Service	Layer 4 Prot.	Layer 7 Protocol	From Host (Client)	From Port (Client)	To Host (Server)	To Port (Server)	Process control	System monitoring	System	System parameter setting
Remote Control	TCP	RDP	Windows PC	>1024	Toolbox PC	5900			x	x
Remote Control	TCP	RDP	Windows PC	>1024	Toolbox PC	3389			x	x
VNC	TCP	RDP	Windows PC	>1024	Toolbox PC	5900			x	x
RDP	TCP	RDP	Windows PC	>1024	Toolbox PC	3389			x	x
Toolbox, Remote Director	TCP	Proprietary	Toolbox-PC	>1024	Toolbox Peer Server	2131			x	x
Toolbox, Database	TCP	Proprietary	Toolbox-PC	>1024	Toolbox Peer Server	1521, 1522			x	x
Toolbox, File Sharing	TCP	Proprietary	Toolbox-PC	>1024	Toolbox Peer Server	139, 445			x	x
Toolbox , CAEx Dongle	TCP	Proprietary	Toolbox-PC	>1024	Toolbox Peer Server	3047			x	x
Toolbox, remote Operation - Start	ICMP	ECHO	Toolbox-PC		SICAM AK 3 SICAM BC SICAM A8000 Series				x	x
Web	TCP	HTTP	PC with browser		SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC	80			x	x
Web	TCP	HTTPS	PC with browser		SICAM AK 3 SICAM BC SICAM A8000 Series	443			x	x
Remote Operation TBII	TCP	HTTP	Toolbox PC		SICAM AK 3 SICAM BC SICAM A8000 Series	80			x	x
Remote Operation TBII	TCP	HTTPS	Toolbox PC		SICAM AK 3 SICAM BC SICAM A8000 Series	443			x	x
Remote Operation TBII	TCP	Proprietary	Toolbox PC	>1024	SICAM AK 3 SICAM BC SICAM EMIC	2001			x	x

Service	Layer 4 Prot.	Layer 7 Protocol	From Host (Client)	From Port (Client)	To Host (Server)	To Port (Server)	Process control	System monitoring	System	System para-meter setting
Process Communication	TCP	IEC 60870-5-104	SICAM PAS SICAM SCC SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC SICAM PTS	>1024	SICAM PAS SICAM SCC SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC SICAM PTS	2404 *)	x	x	x	x
Process Communication	TCP	DNP(i)	other DNP(i)-System SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC	>1024	other DNP(i)-System SICAM AK 3 SICAM BC SICAM A8000 Series SICAM EMIC	20000 *)	x	x		
Process Communication	TCP	IEC 61850	SICAM PAS SICAM SCC SICAM AK 3 SICAM BC SICAM A8000 Series SICAM PTS	>1024	SICAM PAS SICAM SCC SIPROTEC SICAM AK 3 SICAM BC SICAM PTS	102	x	x	x	x
Process Communication	TCP	MODBUS TCP/IP Slave	SICAM AK 3 SICAM BC	>1024	SICAM AK 3 SICAM BC	502	x	x		
Process Communication	TCP	MODBUS TCP/IP Master	SICAM AK 3, SICAM BC	>1024	SICAM AK 3 SICAM BC	502	x	x		
Debugging in SICAM A8000 Series	TCP	Proprietary	PC	>1024	SICAM A8000 Series	5432 **)				
SICAM PTS Protocol Test System Licence Protection	TCP	Proprietary	PC	>1024	LICENCE	22350 22351 ***)				
WEBcmic	UDP	Proprietary	PC	>1024	SICAM A8000 Series	22222 ****)				X
WEBemic	ICMP	Proprietary	PC	"-"	SICAM EMIC					X
Ping	ICMP	PING	SICAM AK 3 SICAM BC SICAM A8000 Series	"-"	SICAM AK 3 SICAM BC SICAM A8000 Series					x

*) IEC 60870-5-104, encrypted (according to IEC 62351-3): TCP port 19998

The protocols or devices listed are common/typical clients or servers, it can also be third party devices. However this is to be taken from the respective project-specific design documentation. IEC 60870-5-104 and DNP(i): ports are freely adjustable.

*) The RADIUS UDP Port is freely adjustable. The syslog server port is freely adjustable.

**) The given port is used exclusively for debugging. It is deactivated in the SICAM A8000 Series from Rev. 2.

***) SICAM PTS Protocol Test System - Licence Protection
The dongle driver (via USB) opens TCP ports 2235 and 22351. These ports are not used by SICAM PTS Protocol Test System.
It is not possible to deactivate this function within the dongle driver.

***) This port is in the SICAM A8000 CP-8000/CP-802x from Rev. 09 only activated, as long as the default IP address is set. (The IP address can only be changed by means of WEB, as long as the default IP address is set. After changing there is no more change or access possible. The port gets deactivated.)

4.2.4 TCP Keep Alive

If protocols for IEC60870-5-104, which are based on TCP/IP, have not implemented any monitoring function, it is possible to monitor the TCP/IP connection by means of the Function “TCP Keep Alive”.

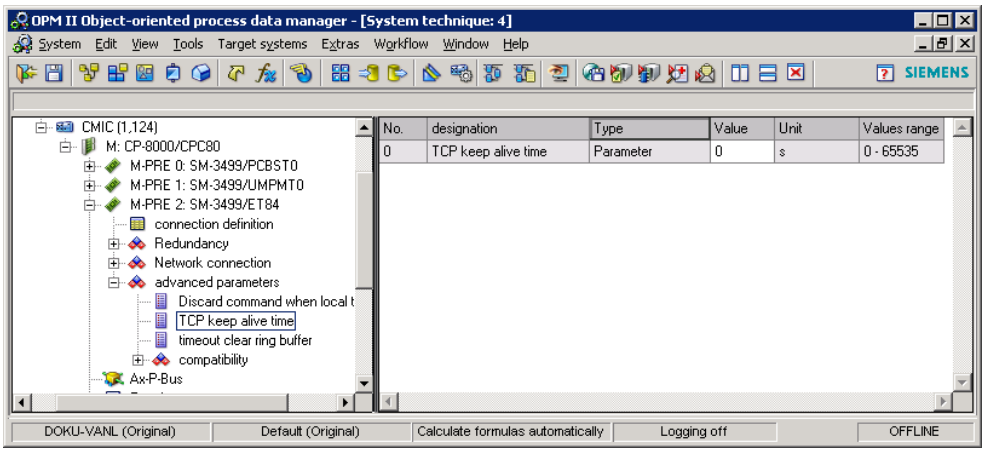
The time interval for the cyclic transmission of the ”TCP Keep Alive“-messages can be set with parameter `TCP Keep Alive Raster`.

The parameter can be found in the system technical parameters of the protocol element under `advanced parameters | TCP keep alive time` . By default this Parameter is set to „0“ (= no transmission).

Availability of the function:

Firmware	from revision
ETA4	02
ET84	02

Example: SICAM CP-8000 with ET84



4.2.5 IEC 61850 – GOOSE

For IEC 61850 – GOOSE there is a specifically defined Etherframe. The transmission takes place periodically on the Ethernet and is very time-critical.

IEC 61850 – GOOSE is transmitted uncoded and is only intended for use in a protected, local area.

4.3 Other Layer 2 Communication Protocols

Besides Ethernet there are also a variety of techniques. On this layer the physical addressing of data packets also takes place.

See also chapter 4.2.3.6, IP Communication Matrix

Hint

If between the individual external devices (Switches, Routers, Modems) a VPN-Tunnel can be constructed through which the data packets can be tunneled, then this is recommended.
In this case the transmission of the data between the SICAM RTUs devices and the terminals takes place uncoded.

4.3.1 Secure Maintenance State

Due to security reasons it may be necessary to disable the integrated switch of the device in case of a fatal error.

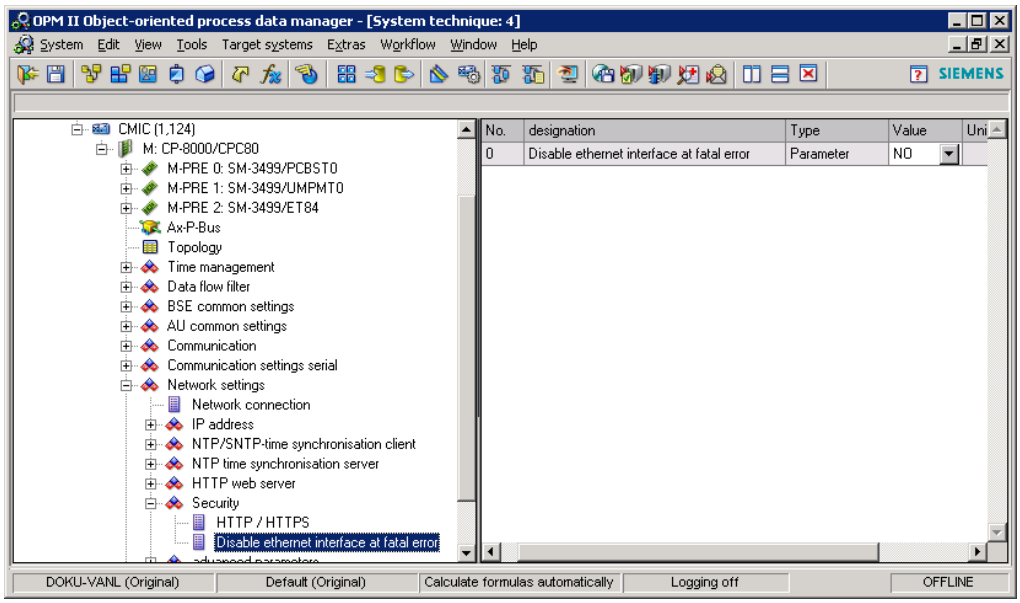
When the ethernet interface is disabled it is not more possible to send messages. That means that also the usage of remote service software is not possible.

The „Secure Maintenance State“ can be set with parameter `Disable ethernet interface at fatal error`.

The parameter can be found in the system technical parameters of the BSE under `Network settings | Security | Disable ethernet interface at fatal error`. By default it is set to „NO“.

Availability of the function:

Firmware	from revision
ETA4	02
ET84	02



SICAM A8000 CP-8031/CP-8050:

The respective parameter for each port of the BSE can be found in the system-technical parameters of the basic system element under `Network settings | Port | Shutdown.`

By default this parameter is set to „NO“

Availability of the function:

firmware	From revision
CPCI85	01

5 Patch Management

Contents

5.1 SICAM A8000 Series / SICAM RTUs 135
5.2 SICAM PTS Protocol Test System 135
5.3 SICAM TOOLBOX II 136
5.4 SICAM Device Manager 137

5.1 SICAM A8000 Series / SICAM RTUs

Every system element of SICAM A8000 Series / SICAM RTUs has its own loadable firmware that is managed centrally by the SICAM TOOLBOX II / SICAM Device Manager. With the SICAM TOOLBOX II / SICAM Device Manager all firmware can be reloaded and updated individually. New firmware are first saved in the SICAM TOOLBOX II / SICAM Device Manager and then distributed to SICAM A8000 Series / SICAM RTUs. For details refer to chapter *5.3.1, Live Update*

SICAM TOOLBOX:

The distribution of the firmware to the SICAM RTUs is carried out with the tool **Load Firmware** (**TOOLBOX II** → **Service Program/OPM** → **Load Firmware**).

SICAM Device Manager:

The distribution of the firmware to the SICAM RTUs is carried out via menu item **Update devices → Firmware…**

Hint

Further information about patching can be found in the following documents:

- *SICAM RTUs User Manuals - Chapter: Updating the System*
- *SICAM TOOLBOX II Online Help*

5.2 SICAM PTS Protocol Test System

The SICAM PTS Protocol Test System is patched by means of Maintenance Releases (Service Packs) and Hotfixes and can be downloaded from the following website:

http://www.siemens.com/sicam

Hint

Information about Update of the SICAM PTS Protocol Test System can be found in the respective release notes.

5.3 SICAM TOOLBOX II

The SICAM TOOLBOX II is patched by means of Maintenance Releases (Service Packs) and Hotfixes. These are available in the Internet as Download.

Hint

Information about Update of the SICAM TOOLBOX II can be found in the document:

- *SICAM TOOLBOX II DVD BOOKLET - Chapter: Update*

5.3.1 Live Update

With the **Live Update** function of the SICAM TOOLBOX II all firmware updates for SICAM RTUs can be imported automated into the SICAM TOOLBOX II, through which the update possibility is simplified considerably.

Call: **TOOLBOX II → Live Update**

The following 2 modes can be selected:

Online Mode

After the start the TOOLBOX II Live Update connects over the Internet to a central server and automatically downloads all missing and more recent master data.

In an overview list version information for the individual master data can be displayed. Before the import to the local SICAM TOOLBOX II a selection can be made of the master data to be imported.

In addition there is a command line mode in which this updating can be performed automated.

Offline Mode

The SICAM TOOLBOX II Live Update can also be operated offline. Thereby the Intranet or Internet is not used for updating the master data, rather the directory in which the already downloaded data of other clients are located. Consequently a configuration can be created, in which only one SICAM TOOLBOX II computer has Internet access, all other clients access a common directory offline (global store).

Hint

Further information about **Live Update** can be found in the:

- *SICAM TOOLBOX II Online Help*

Caution

If a SICAM TOOLBOX II with read-only parameters, on which a system element was updated, is used for a firmware update and this update was not made in the SICAM TOOLBOX II with the original parameters, then following can happen:

Firmware loading with SICAM TOOLBOX II with read-only parameters and afterwards firmware loading with SICAM TOOLBOX II with original parameters equates a firmware downgrade!

5.4 SICAM Device Manager

The SICAM Device Manager is patched by means of Maintenance Releases (Service Packs) and Hotfixes and can be downloaded the website

http://www.siemens.com/sicam.

Hint

Information about Update of the SICAM Device Manager can be found in the respective release notes.

6 Virus Protection

Contents

6.1 General 139

6.1 General

SICAM A8000 Series / SICAM RTUs

The SICAM A8000 Series / SICAM RTUs components are self-developed Embedded Systems, for which no known viruses exist. There is therefore also no protection software available for these systems.

In addition the components are hardened before commissioning, to achieve increased protection against possible malicious software.

SICAM PTS Protocol Test System

The SICAM PTS Protocol Test System comprises neither hardware nor operating system or other standard programs.

SICAM TOOLBOX II

The SICAM TOOLBOX II comprises neither hardware nor operating system or other standard programs.

SICAM Device Manager

The SICAM Device Manager comprises neither hardware nor operating system or other standard programs.

Hint

The virus protection must be designed and realized in the framework of the project planning/implementation.

7 Encryption and Authentication processes

Contents

7.1 SICAM A8000 Series / SICAM RTUs 141
7.2 SICAM TOOLBOX II 144
7.3 SICAM Device Manager 144

7.1 SICAM A8000 Series / SICAM RTUs

Each device has its specific X.509 server certificate RSA2048/SHA256 stored on hardware-security-module The material/signatures are loaded during production process.

Preshared keys and passwords, which are used for authentication, are stored secure in SICAM A8000 Series / SICAM RTUs, refer to chapter 3.3.13, Storage of Passwords in SICAM A8000 Series / SICAM RTUs.

Authentication for SICAM A8000 Series:

When connecting to a device both in remote operation with SICAM TOOLBOX II and via SICAM WEB/SICAM Device Manager the user has to enter a user name and password.

For detailed information about users and roles of SICAM A8000 Series, refer to chapters 3.3.9 Role-Based-Access-Control in SICAM A8000 Series and 12.2.1.

7.1.1 Engineering of SICAM A8000 Series via SICAM WEB

During engineering of the SICAM A8000 CP-8031/CP-8050 via SICAM WEB (RBAC management) or during diagnosis it is possible to encrypt the connection with HTTPS. This is possible from firmware CPCI85 revision 01.

Characteristics:

- Self signed certificates
- TLS 1.2 is supported by means of firmware revision 04.03 of CPCI85.

Supported cipher suites (session keys):

- TLS_RSA_WITH_AES_128_CBC_SHA (only if TLS1.0 is available)
- TLS_RSA_WITH_AES_256_CBC_SHA ((only if TLS1.0 is available)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

7.1.2 Diagnosis of SICAM RTUs Protocols via WEB-Browser

Some SICAM RTUs protocols and some SICAM A8000 protocols support a WEB server for diagnostic purposes (access via WEB browser). Authentication for these WEB pages is not provided for.
Therefore, for normal operation this possibility of access should be deactivated via parameterization.

Characteristics:

- Self signed certificates
- TLS (Transport Layer Security) Connection establishment with RSA 2048/SHA256
  TLS 1.0, TLS 1.1 and TLS 1.2 are supported.

Supported cipher suites (session keys):

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

7.1.3 Engineering via SICAM TOOLBOX II/SICAM Device Manager

During engineering of SICAM A8000 CP-8000/CP-802x / SICAM RTUs via SICAM TOOLBOX II (from V05.11) in remote operation it is possible to encrypt the connection with HTTPS.

SICAM TOOLBOX II V06.01 is necessary for engineering of SICAM A8000 CP-8031/CP-8050.

Precondition:

System	Firmware	PRE	Connection PW
SICAM A8000 CP-8000/ CP-802x	CPC80 from revision 04		supported
SICAM A8000 CP-8031/CP-8050	CPCI85 from Revision 01		Not supported*)
SICAM AK 3	CPCX26 from revision 01 PCCX26 from revision 01		supported
SICAM AK 3; SICAM BC		SM-2558/ETA4 from revision 02 SM-2558/ETA3 from revision 02 SM-2558/ETA5 from revision 01	supported

***) Hint**
The function „Connection Password“ is not available for SICAM A8000 CP-8031/CP-8050.
The connection to the device is supervised by „Role-Based-Access“ (RBAC), refer to chapter 3.3.9

Characteristics:

- Certificates, loaded into SICAM RTUs and SICAM TOOLBOX II during manufacturing
- encrypted, on device level authenticated connection
- TLS (Transport Layer Security) Connection establishment with RSA 1024
  TLS 1.0, TLS 1.1 and TLS 1.2 are supported.

SICAM A8000 CP-8031/CP-8050 (CPCI85 ab Rev. 04.30):

The engineering interface is protected by TLS1.2.

SICAM A8000 CP-8000/2x (CPC80 ab Rev 16):

The engineering interface is protected by TLS1.2.
TLS1.0 is supported per default (because of backward compatibility with older SICAM TOOLBOX II- installations, but TLS 1.2 only can be configured.

Supported cipher suites (session keys):

- TLS_RSA_WITH_AES_128_CBC_SHA (only if TLS1.0 is available)
- TLS_RSA_WITH_AES_256_CBC_SHA (only if TLS1.0 is available)
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

For user authentication in remote operation with SICAM TOOLBOX II it is possible to additionally use the „Connection Password“ in the SICAM A8000 CP-8000/CP-802x / SICAM RTUs. For details see chapter Connection Password .

Characteristics of the „Connection Password“:

- HASH (Challenge Response)

7.1.4 IPSec VPN in SICAM RTUs

IPSec VPN (Internet Protocol Security – Virtual Private Network) is an extension of the Internet Protocol (IP) for encryption and authentication mechanisms. IPSec VPN actively establishes a VPN tunnel (initiator), which guarantees the required confidentiality, authenticity and integrity of data transmission in IP networks.

(See also chapter 4.2.3.1, IPSec VPN in SICAM A8000 Series / SICAM RTUs)

7.2 SICAM TOOLBOX II

During engineering of SICAM RTUs with SICAM TOOLBOX II (from V05.11) in remote operation it is possible to encrypt the connection with HTTPS.

For user authentication in remote operation with SICAM TOOLBOX II it is possible to use additionally the „Connection Password“ in SICAM A8000 CP-8000/CP-802x / SICAM RTUs). For details see chapter Connection Password .

Characteristics of the „Connection Password“:

- HASH (Challenge Response)

(See also chapter 7.1.3, Engineering via SICAM TOOLBOX II)

Hint

The function „Connection Password“ is not available for SICAM A8000 CP-8031/CP-8050.

The connection to the device is supervised by „Role-Based-Access“ (RBAC), refer to chapter 3.3.9

7.3 SICAM Device Manager

During engineering of SICAM RTUs by means of SICAM Device Manager in remote operation it is possible to encrypt the connection with HTTPS.

After connection to the device is established the user has to authenticate with username and password.

8 Backup & Restore

Contents

8.1 General 145
8.2 Data Backup 146
8.3 Restore 148

8.1 General

SICAM TOOLBOX

The entire parameters, applications and firmware of SICAM A8000 Series / SICAM RTUs are centrally managed and stored by the SICAM TOOLBOX II.

With the help of the tool **Data Distribution Center** the following engineering data can be imported or exported:

- Customer (plant management, users • incl. presets)
- System technique (regions and automation units)
- Process technique (ranges, display overview of the image parameterization SICAM BC, CAEx plus project library)
- Display overview (image parameterization SICAM BC)
- Master data
- PSRII data (recorder recordings, customer parameters and customer filters, incident data, transmit menus)
- Logbook data

Every SICAM A8000 CP-8000/CP-802x / SICAM RTUs has its own SD-card on which all relevant data (parameters, firmware) of the AU concerned are also saved.

SICAM A8000 CP-8031/CP-8050 has an internal MMC on which all relevant data (parameters, firmware) of the AU concerned are also saved, and optional a SD-card for backup and spare part concept.

SICAM Device Manager

SICAM Device Manager supports backup and restore of engineering data of a device. All the engineering data of the SICAM Device Manager is stored on the WINDOWS file system. The location can be defined by the user.
For backup purposes the whole directory with all the engineering data can be saved with copy/paste-operation.

Hint

User names and passwords are not part of backup & restore functionality.

8.2 Data Backup

SICAM TOOLBOX

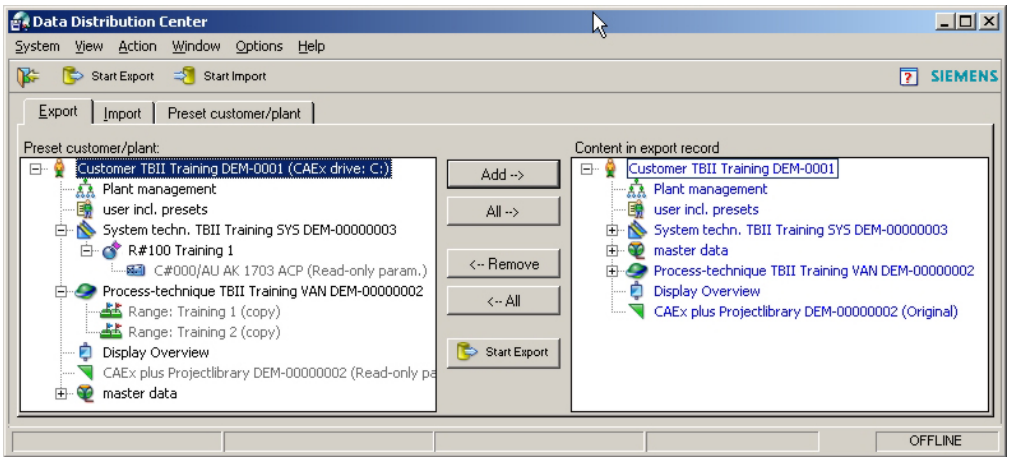
To create a Backup it is necessary to start the **Data Distribution Center** in the SICAM TOOLBOX II and open the tab **Export**.

If a backup of the entire data stock of a customer is created, all data must be dragged from the Export tab into the Export Set tab.

Thereby the CTRL-key must remain depressed, so that the original data stocks are retained after this action. The Export Set contains a backup of the data.

Located in the tab **Export - Preset customer/plant** is the original status.

Located in the right side of the window **Content in export record**, is the backup.



Hint

A backup of SICAM TOOLBOX II data should be performed after every change of data.

The backed up data should be safeguarded in a protected area.

The backed up data should be restored at regular intervals (see also chapter: Restoration of the SICAM TOOLBOX II Data) and also verified.

SICAM Device Manager

For a backup of an entire device within the SICAM Device Manager the desired device has to be selected, then start the backup procedure via the menu entry “Backup device…” The file location (where the backup file should be stored) can be freely defined. Details can be found in *SICAM Device Manager User Manual*.

8.2.1 Automated Backup

SICAM TOOLBOX

In the SICAM TOOLBOX II automated backups can be created. For this first a Control File must be created in the DDC. This Control File can be processed batch-controlled at a later time. In addition it is possible to perform this task in Windows Scheduler.

The Control File is created as follows:

- Open the DDC and switch to the Export tab
- Compile the Export Set. (regardless of the selection always only AU read-only versions and range copies are contained in the generated backup)
- A dialog is opened via the menu item "**Action | Start Export Control**"
- Enter the path and file name
- Optionally the Control File can perform the following 3 automated actions (wildcard functionality)
  - Backup the entire system-technical plant
  - Backup all AU's of the selected regions
  - Backup the entire process-technical plant

  Hint:

  Through these options the control file does not need to be continually updated for changes in the system- and process-technical plant.

The Control File is processed as follows:

- Open a DOS window
- Call DDC Controlfile -dBackupfile [-lLogfile] [-d]
  DDC .. Name of the program
  Control File .. Name and path of the control file (optional choice of name with or without extension)
  - B (Backupfilename) .. Option -B and name and path of the backup file (without space)
  - L (Logfilename) .. Option - L and name and path of the log file (without space). This information is optional.
  - D ... automatic name generation. The name of the backup file and the log file is composed as follows: (Backupfilename)[current date]_[current hours and minutes] (Logfilename)[current date]_[current hours and minutes]

Example

```
DDC C :\TEMP\MYCTRL -BC:\ BACKUP\Sicherung - D
```

RESULT: SICHERUNG15072001_1735.001

The option -? displays the help.

The syntax described above can also be processed in a Batch File (.CMD or .BAT).
Here it is to be observed, that from Version 5 the prefix "%EMGPATH%\BIN\tbiistart.cmd" is necessary for the batch-controlled call.

Caution

Set-Revisions will not be included in a DDC-export.

SICAM Device Manager

For an automated backup of a whole SICAM Device Manager project the user can establish a scheduled task (WINDOWS operating system), where the whole project directory with all the engineering data can be stored to an specific location.

8.3 Restore

8.3.1 Restoration of SICAM A8000 Series / SICAM RTUs

After the exchange of an automation unit or parts of an AU, merely the existing SD-card is to be used. The AU receives the data automatically from the SD-card on Power-Up. No further measures are necessary for the restoration.

8.3.2 Restoration of the SD-Card of SICAM A8000 Series / SICAM RTUs

SICAM TOOLBOX

If an SD-card of an AU has to be restored, there are 2 possibilities:

- Direct writing of the SD-card using SICAM TOOLBOX II
- Initialization and loading of the AU using SICAM TOOLBOX II

SICAM Device Manager

If an SD-card of a device has to be restored, the SD-card can be generated by the SICAM Device Manager.

8.3.2.1 Direct Writing of the SD-Card by means of SICAM TOOLBOX II

To do this an SD-card reader/writer must be connected to the Toolbox-PC, and a suitable SD-card inserted.

With the "OPM II" tool you can select the corresponding destination system (AU) via the menu **Tools** → **System Technique**. Via the context menu of the AU **Flashcard** → **Create files…** you can transfer firmware files to the SD-card.

The details about this can be found in the *SICAM TOOLBOX II Online Help, Chapter "OPM II", Section "System Technique | SICAM 1703 | Load Flashcard"*.

Then insert the SD-card into the master control element and make a power-up in the destination system. The destination system performs a startup, and thereby loads the firmware to the corresponding system elements.

Hint

The loading of the master control element firmware (initialization) for the first time is only possible directly via the Toolbox connection (Serial/USB cable).

8.3.2.2 Initialization and Loading of the AU by means of SICAM TOOLBOX II

The loading of the parameters in the destination system (and consequently to the SD-card of the basic system element) takes place with the tool "Load Parameters" of the SICAM TOOLBOX II. You can start it from the “OPM II” via the menu **Destination systems → SICAM 1703 → Parameter loader**.

After the loading of the parameters an automatic startup of the destination system is performed.

The details about this can be found in the *SICAM TOOLBOX II Online Help, Chapter “Service Programs", Section "Load Parameters”*.

Caution

During a loading operation the master control element must definitely not be switched off, as the data on the SD-Card could be destroyed as a result.

Hint

After the parameter-initialization with the SICAM TOOLBOX II tool "Parameter loader" the firmwares must be loaded.

There may be following special case:

If in the parameter of a BSE another firmware is equipped as actually loaded on the module, then it may be necessary, that after the parameter-initialization and firmware loading, the parameter must be loaded again. Eventually you also have to load the firmwares of the supplementary modules afterwards.

Only then the complete AU is loaded!

8.3.2.3 SD-Card, Direct Writing via SICAM Device Manager

First of all, you have to select a device which the SD-card should be generated for.

Then you have to select the menu entry **Generate SD card**… .

The location where SD card content should be generated can be either on the file system or on SD card.

Finally insert the SD-card into the master control element and perform a power-up in the device. During startup firmware is loaded into the respective system elements.

8.3.3 Restoration of the SICAM TOOLBOX II Data

The restoration of the data of the SICAM TOOLBOX II also takes place in the **Data Distribution Center** in the tab **Import**.

After the import of the backup the statuses of the automation units and ranges must be corrected manually. To do this it is necessary to switch to the tab **Preset Customer/Plant**.

The status can be changed in the context menu of the automation units and the ranges.

Hint

After the restoration it is recommended to perform a parameter comparison between the restored data in the SICAM TOOLBOX II and the data in the SICAM RTUs.

With inconsistent data stock the next procedure is to be checked from case to case. (If backup not current -> import current backup)

8.3.4 Restoration of SICAM Device Manager Project Data

The restoration of an entire SICAM Device Manager project can be done by copying the backup of a project directory and pasting to the project directory location of SICAM Device Manager.

9 Logging

Contents

9.1 Security Logging 151
9.2 Diagnostic 170
9.3 Logbook 173
9.4 Logging with the Windows Event Display 174

9.1 Security Logging

9.1.1 General

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

These data can be sent automatically to an external syslog-server, or in case of SICAM TOOLBOX II, to the Windows Event Log.

The transmission of the data takes place spontaneous and without conformation via UDP when the event occurs. A later readout is not possible. The message texts are always in English language.

Hint

On the syslog-server the data can be protected against manipulation by users with the role "Auditor".

9.1.2 Supported Systems/Firmwares

Syslog is supported by following systems/firmwares:

System	Firmware	Revision	Syslog-Client	Used Interfaces
SICAM A8000 CP-8031 CP-8050	CPCi85	from 01	x	X2,X3, CI-Module (CI-8520)
SICAM A8000 CP-8000 CP-8021 CP-8022	CPC80	from 09	x	X1, X4 X1, X4 X1, X4, X6
SICAM AK 3	CPCX26	from 02	x	X0, X1 on CP-2016
	PCCX26	from 02	x	X0, X1 on CP-2019
	ETA4	from 05	x	X3 on CP-2016 or CP-2019
SICAM BC	CPCX55	from 10	-	CP-5014
	ETA4	from 05	x	CP-5014
SICAM TOOLBOX II		from V5.11	x	
SICAM Device Manager		from 01	-	

9.1.3 Logged Security Events

The number of security logbook entries is limited and the logbook acts as a ring buffer. The oldest entry will be deleted once the limit of entries is exceeded.

SICAM A8000 CP-8031/CP-8050:
maximum number of entries: 8192

Hint

For SICAM A8000 CP-8031/CP-8050: a diagnosis warning will be set if 80% of maximum number of entries have not been read. This warning remains until one of the entries was read.

SICAM A8000 CP-8000/CP-802x / SICAM RTUs
maximum number of entries: 2048

SICAM A8000 / SICAM RTUs

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

SICAM TOOLBOX II

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

  - SICAM TOOLBOX II libraries
  - Updates of SICAM SCALA 250

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

- Login attempts
  - successful login attempts
  - failed login attempts

SICAM Device Manager:

Currently, no events are logged

9.1.3.1 Structure of Security Events

SICAM A8000 CP-8031/CP-8050

A syslog event is built up with following elements:

Element	Description
Date	Date when the event was received/logged from the syslog server
Time	Time when the event was received/logged from the syslog server
Facility	Source of the event – LogAudit – LogAlert
Severity (Level)	Severity of the event – Alert – Warning
HostName	IP address or Host Name of the device sending the event
Message Text	The message part of a syslog event consist of following elements: – yyyy-mm-dd ..... date when the event was created – Thh:mm:ss.ttt ..... time when the event was created – +hh:mm ..... time deviation from GMT Depending on the event the message text can contain variable additional information (%A1%, %A2%, %A3%). These are shown in the following chapter.

Example:

Date	Time	Facility	Level	Host Name	Message Text
2015-12-01	16:41:52	Local2	Notice	10.9.19.250	2015-12-01T16:41:48.128+01:00 R#130_C#004_BSE#020_SSE#254 SICAM_RTUs The Flashcard was inserted

SICAM A8000 CP-8000/CP-802x / SICAM RTUs, SICAM TOOLBOXII

A syslog event is built up with following elements:

Element	Description
Date	Date when the event was received/logged from the syslog server
Time	Time when the event was received/logged from the syslog server
Facility	Source of the event – Security – Authorization – Application
Severity (Level)	Severity of the event – Alert – Critical – Error – Warning – Notice
HostName	IP address or Host Name of the device sending the event

Message Text	The message part of a syslog event consist of following elements: – yyyy-mm-dd .....date when the event was created – Thh:mm:ss.ttt .....time when the event was created – +hh:mm.....time deviation from GMT – R#xxx_.....xxx = Region number (0..255) – C#xxx_.....xxx = Component number (0..255) – BSE#xxx_ .....xxx = BSE number (000-020) – SSE#xxx .....xxx = SSE number (000-254) Depending on the event the message text can contain variable additional information (**%A1%**, **%A2%**, **%A3%**). These are shown in the following chapter.

9.1.3.2 Syslog Events SICAM A8000 CP-8031/CP-8050

By default the security logbook (Syslog-Client) is deactivated. It can be activated if required. Syslog events are transmitted to up to 2 syslog-servers.

Syslog Event Type	Meaning
AuditTrail Event	**Events are defined as authorized activities which can be expected to occur in the routine use and maintenance of the IED.** - spontaneous transmission - local storage of events (actually not supported) - no diagnosis for events!
AuditTrail Alarm	**Alarms are defined as activities which may indicate unauthorized activity** - spontaneous transmission - local storage of alarms (actually not supported) - alarms with local diagnosis (diagnosis information can be converted/transmitted to process information)

Syslog Event	Facility	Severity Level	Event Type	Additional Info 1 [%A1%]	Additional Info 2 [%A2%]	Additional Info 3 [%A3%]	CPCI85	ETI4	ETI5
%A1% login of the user '%A2%' failed via %A3%	LogAudit	Alert	AuditTrail Event	Local, Remote	User name	SICAM WEB, Toolbox II	X		
%A1% User '%A2%' has logged in successfully via %A3%	LogAudit	Warning	AuditTrail Event	Local, Remote	User name	SICAM WEB, Toolbox II	X		
User account '%A1%' created (%A2%)	LogAudit	Warning	AuditTrail Event	Account id	role assignment	-	X		
User account '%A1%' changed (%A2%)	LogAudit	Warning	AuditTrail Event	Account id	role assignment	-	X		
User account '%A1%'deleted (%A2%)	LogAudit	Warning	AuditTrail Event	Account id	role assignment	-	X		
Password for user '%A1%' changed (%A2%)	LogAudit	Warning	AuditTrail Event	User name	User name	-	X		
User '%A1%' ' has logged out via '(%A2%)'	LogAudit	Warning	AuditTrail Event	User name	Tool				
Firmware '%A1%' has been installed with version '%A2%	LogAudit	Warning	AuditTrail Event	Firmware name	version	-	X		
Syslog client ready	LogAudit	Warning	AuditTrail Event	-	-	-	X		
Parameters have been changed	LogAudit	Warning	AuditTrail Event	-	-	-	X		
The 'SICAM TOOLBOX II Remote operation' has been connected successfully	LogAudit	Warning	AuditTrail Event	-	-	-	X		
The 'SICAM TOOLBOX II Local operation' has been connected successfully	LogAudit	Warning	AuditTrail Event	-	-	-	X		
Connection setup from unknown IP address '%A1%' [1)]	LogAudit	Warning	AuditTrail Event	IP-address	-	-		X	X
User data message TI'%A1%' was generated by SICAM TOOLBOX II message simulation	LogAudit	Warning	AuditTrail Event	Type identification	-	-	X		
System message FC'%A1%' was generated by SICAM TOOLBOX II message simulation	LogAudit	Warning	AuditTrail Event	Function code	-	-	X		
Port'%A1%' link status has changed to LINK_UP	LogAudit	Warning	AuditTrail Event	Port number	-	-	X		
Port'%A1%' link status has changed to LINK_DOWN	LogAudit	Warning	AuditTrail Event	Port number	-	-	X		
SICAM TOOLBOX II CAEx online test started	LogAudit	Warning	AuditTrail Event	-	-	-	X		
SICAM TOOLBOX II CAEx online test stopped	LogAudit	Warning	AuditTrail Event	-	-	-	X		

Syslog Event	Facility	Severity Level	Event Type	Additional Info 1 [%A1%]	Additional Info 2 [%A2%]	Additional Info 3 [%A3%]	CPCI85	ETI4	ETI5
Date and time setting by 'SICAM TOOLBOX II maintenance function online' or 'SICAM WEB'	LogAudit	Warning	AuditTrail Event				X		
Disconnection of 'SICAM TOOLBOX II Local operation' initiated by user	LogAudit	Warning	AuditTrail Event				X		
Disconnection of 'SICAM TOOLBOX II Remote operation' initiated by user	LogAudit	Warning	AuditTrail Event				X		
Disconnection of 'SICAM TOOLBOX II Remote operation' caused by timeout	LogAudit	Warning	AuditTrail Event				X		
Mass simulation of messages by 'SICAM TOOLBOX II message simulation'	LogAudit	Warning	AuditTrail Event				X		
Restart initiated by 'SICAM TOOLBOX II' or 'SICAM WEB'	LogAudit	Alert	AuditTrail Alarm				X		
Restart initiated by 'Parameter update'	LogAudit	Alert	AuditTrail Alarm				X		
Restart initiated by 'Remote reset'	LogAudit	Alert	AuditTrail Alarm				X		
Restart initiated by 'CPU exception'	LogAudit	Alert	AuditTrail Alarm				X		
Restart initiated by 'Power on'	LogAudit	Alert	AuditTrail Alarm				X		
Data message in receive direction blocked by activated WhiteList Filter	LogAudit	Warning	AuditTrail Event				X		
Data message in transmit direction blocked by activated WhiteList Filter	LogAudit	Warning	AuditTrail Event				X		
Data message blocked by system internal WhiteList Filter	LogAudit	Warning	AuditTrail Event				X		
High data load from remote station: '%A1%' - '%A2%', Station number '%A3%' [1)]	LogAudit	Warning	AuditTrail Event	System	Protocol	Station num.		X	
High data load to remote station: '%A1%' - '%A2%', Station number '%A3%' [1)]	LogAudit	Warning	AuditTrail Event	System	Protocol	Station num.		X	

1) only supported by some protocol element firmwares

9.1.3.3 Syslog Events SICAM A8000 CP-8000/CP-802x / SICAM RTUs, SICAM Toolbox II

By default the security logbook (Syslog-Client) is deactivated. It can be activated if required. One automation unit can operate up to 20 syslog-clients.

In SICAM A8000 Series / SICAM RTUs syslog-events are sent from different sources to the MCPU and can be transmitted to the syslog-servers via 1 or several interfaces. If the security logbook is activated on a “sending interface“ then the syslog client registers itself on the MCPU. Syslog events are transmitted via all registered syslog clients.

Syslog Event Type	Meaning
Event	**Syslog Events will be sent for authorized/unauthorized activities but not defined as AuditTrail Event/-Alarm.** - spontaneous transmission - no local storage - no diagnosis
AuditTrail Event	**Events are defined as authorized activities which can be expected to occur in the routine use and maintenance of the IED.** - spontaneous transmission - local storage of events (actually not supported) - no diagnosis for events!
AuditTrail Alarm	**Alarms are defined as activities which may indicate unauthorized activity** - spontaneous transmission - local storage of alarms (actually not supported) - alarms with local diagnosis (diagnosis information can be converted/transmitted to process information)

Syslog Event	Facility	Severity Level	Event Type	Additional Info 1 [%A1%]	Additional Info 2 [%A2%]	Additional Info 3 [%A3%]	SICAM TOOLBOX II	SICAM A8000 Series[1]	SICAM AK 3			
									CPCX26 [1]	PCCX26 [1]	ETA4 [1]	
%A1% login of the user '%A2%' failed via %A3%	Authorization	Error	Event	Local, Remote	User name	Tool	X	4)				
%A1% User '%A2%' has logged in successfully via %A3%	Authorization	Notice	Event	Local, Remote	User name	Tool	X	4)				
User '%A1%' ' has logged out via '(%A2%)'	Authorization	Notice	Event	User name	Tool		X	4)				
Import of '%A1%' succeeded (%A3%) (%A2%)	Application	Notice	Event	Database	Windows User, TBII User	File	X					
Export of '%A1%' succeeded (%A3%) (%A2%)	Application	Notice	Event	Database	Windows User, TBII User	File	X					
Import of '%A1%' failed (%A3%) (%A2%)	Application	Warning	Event	Backup	Windows User, TBII User	File	X					
Export of '%A1%' failed (%A3%) (%A2%)	Application	Warning	Event	Backup	Windows User, TBII User	File	X					
ST-Emulation command executed (%A3%) (%A2%)	Application	Notice	Event	-	Windows User, TBII User	Command	X					
Security related configuration changed (%A1%) (%A2%)	Security	Warning	Event	start/stop-eventlog start/stop syslog change syslog server config	Windows User, TBII User	-	X					
User account '%A1%' created (%A2%)	Authorization	Notice	Event	Account id	role assignment		X	4)				
User account '%A1%' changed (%A2%)	Authorization	Notice	Event	Account id	role assignment		X	4)				
User account '%A1%' deleted (%A2%)	Authorization	Warning	Event	Account id	role assignment	Windows User, TBII User	X	4)				

Syslog Event	Facility	Severity Level	Event Type	Additional Info 1 [%A1%]	Additional Info 2 [%A2%]	Additional Info 3 [%A3%]	SICAM TOOLBOX II	SICAM A8000 Series[1]	SICAM AK 3			
									CPCX26[1]	PCCX26[1]	ETA4[1]	
Password for user '%A1%' changed (%A2%)	Authorization	Notice	Event	User name	Windows User, TBII User	-	X	4)				
User role '%A1%' changed (%A2%) (%A3%)	Security	Warning	Event	User role	created/modified/ deleted	Windows User, TBII User	X					
Firmware '%A1%' updated to version '%A2%' (%A3%)	Application	Warning	Event	Firmware name	version	Windows User, TBII User	X					
Installation of firmware '%A1%' version '%A2%' (%A3%)	Application	Warning	Event	Firmware name	version	Windows User, TBII User	X					
Syslog startup	Application	Notice	Event	-	-	-		X	X	X	X	
Syslog ready	Application	Notice	Event	-	-	-		X	X	X	X	
Parameters loaded	Application	Warning	Event	-	-	-		X	X	X	X	
The 'SICAM TOOLBOX II Remote operation' has logged in successfully	Authorization	Notice	Event	-	-	-		X	X	X	X	
Login of 'SICAM TOOLBOX II Remote operation' failed	Authorization	Error	Event	-	-	-		X	X	X	X	
Password for 'SICAM TOOLBOX II Remote operation' changed successfully	Authorization	Notice	Event	-	-	-		X	X	X	X	
Password change for 'SICAM TOOLBOX II Remote operation' failed	Authorization	Notice	Event	-	-	-		X	X	X	X	
Engineering tool SICAM TOOLBOX II connected	Authorization	Notice	Event	-	-	-		X	X	X	X	
Connection setup from unknown IP address '%A1%' [2]	Security	Warning	Event	IP-address	-	-		X	X	X	X	
Firmware updated, file name '%A1%' ('%A2%)	Application	Warning	Event	Firmware name	successful/ unsuccessful	-		X	X	X	X	
User data message TI'%A1%' was generated by SICAM TOOLBOX II message simulation	Application	Notice	Event	Type identification	-	-		X	X	X	X	

Syslog Event	Facility	Severity Level	Event Type	Additional Info 1 [%A1%]	Additional Info 2 [%A2%]	Additional Info 3 [%A3%]	SICAM TOOLBOX II	SICAM A8000 Series[1]	SICAM AK 3			
									CPCX26 [1]	PCCX26 [1]	ETA4 [1]	
System message FC'%A1%' was generated by SICAM TOOLBOX II message simulation	Application	Notice	Event	Function code	-	-		X	X	X	X	
Port'%A1%' link status has changed to LINK_UP	Application	Notice	Event	Port number	-	-		X	X	X	X	
Port'%A1%' link status has changed to LINK_DOWN	Application	Notice	Event	Port number	-	-		X	X	X	X	
Flashcard removed	Application	Notice	Event	-	-	-		X	X	X	X	
Flashcard inserted	Application	Notice	Event	-	-	-		X	X	X	X	
SICAM TOOLBOX II CAEx online test started	Application	Notice	Event	-	-	-		X	X	X	X	
SICAM TOOLBOX II CAEx online test stopped	Application	Notice	Event	-	-	-		X	X	X	X	
Date and time setting by 'SICAM TOOLBOX II maintenance function online' or 'SICAM WEB'	Application	Notice	AuditTrail Event					X	X	X	X	
Engineering tool 'SICAM TOOLBOX II' disconnected	Application	Notice	AuditTrail Event					X	X	X	X	
Logout of 'SICAM TOOLBOX II Remote operation' initiated by user	Authorization	Notice	AuditTrail Event					X	X	X	X	
Logout of 'SICAM TOOLBOX II Remote operation' caused by timeout	Authorization	Notice	AuditTrail Event					X	X	X	X	
Mass simulation of messages by 'SICAM TOOLBOX II message simulation'	Application	Warning	AuditTrail Event					X	X	X	X	
IPSec authentication remote site'%A1%' has been modified	Authorization	Warning	AuditTrail Event	Site number				X	X	X	X	
SNMP user'%A1%' authentication password modified	Authorization	Warning	AuditTrail Event	User number				X	X			
SNMP user'%A1%' encryption password modified	Authorization	Warning	AuditTrail Event	User number				X	X			
SNMP trap authentication password modified	Authorization	Warning	AuditTrail Event					X	X			
SNMP trap privacy password modified	Authorization	Warning	AuditTrail Event					X	X			
SNMP read community hash modified	Authorization	Warning	AuditTrail Event					X	X			

Syslog Event	Facility	Severity Level	Event Type	Additional Info 1 [%A1%]	Additional Info 2 [%A2%]	Additional Info 3 [%A3%]	SICAM TOOLBOX II	SICAM A8000 Series[1]	SICAM AK 3			
									CPCX26[1]	PCCX26[1]	ETA4[1]	
SNMP write community hash modified	Authorization	Warning	AuditTrail Event					X	X			
Radius authentication password modified	Authorization	Warning	AuditTrail Event					X				
No matching user roles found for remote user ‘%A1%‘ during radius authentication	Authorization	Warning	AuditTrail Event	User name				4)				
SICAM WEB backup device settings	Application	Notice	AuditTrail Event					X				
SICAM WEB restore device settings	Application	Notice	AuditTrail Event					X				
SICAM WEB Session expired for user '%A1%'	Application	Notice	AuditTrail Event	User name				4)				
SICAM WEB application-software updated, version '%A1%'	Application	Notice	AuditTrail Event					X				
Logout of 'SICAM WEB' initiated by user	Authorization	Notice	AuditTrail Event					X				
Successful login to 'SNMP agent' (user=%A1%)	Authorization	Notice	AuditTrail Event	User name				X	X			
Successful login to 'SNMP agent' read/write community	Authorization	Notice	AuditTrail Event					X	X			
Unsuccessful login attempts to 'SICAM TOOLBOX II Remote operation'	Authorization	Alert	AuditTrail Alarm					X	X	X	X	
Unsuccessful login attempts to 'SNMP agent' (user=%A1%)	Authorization	Alert	AuditTrail Alarm	User name				X	X			
Unsuccessful login attempts to 'SNMP agent' read/write community	Authorization	Alert	AuditTrail Alarm					X	X			
Restart initiated by 'SICAM TOOLBOX II' or 'SICAM WEB'	Application	Alert	AuditTrail Alarm					X	X	X	X	
Restart initiated by 'Parameter update'	Application	Alert	AuditTrail Alarm					X	X	X	X	
Restart initiated by 'Remote reset'	Application	Alert	AuditTrail Alarm					X	X	X	X	
Restart initiated by 'Reset button'	Application	Alert	AuditTrail Alarm						X	X	X	
Restart initiated by 'inserting SD card	Application	Alert	AuditTrail Alarm					X				
Restart initiated by 'CPU exception'	Application	Alert	AuditTrail Alarm					X	X	X	X	

Syslog Event	Facility	Severity Level	Event Type	Additional Info 1 [%A1%]	Additional Info 2 [%A2%]	Additional Info 3 [%A3%]	SICAM TOOLBOX II	SICAM A8000 Series[1]	SICAM AK 3			
									CPCX26 [1]	PCCX26 [1]	ETA4 [1]	
Restart initiated by 'Power on'	Application	Alert	AuditTrail Alarm					X	X	X	X	
Time synchronization message out of valid range	Application	Alert	AuditTrail Alarm					X	X	X	X	
Verification of X.509 certificate failed	Application	Alert	AuditTrail Alarm					X				
Hardware identification wrong	Application	Alert	AuditTrail Alarm						X	X	X	
Data message in receive direction blocked by activated WhiteList Filter	Application	Warning	Event					X	X	X	X	
Data message in transmit direction blocked by activated WhiteList Filter	Application	Warning	Event					X	X	X	X	
Data message blocked by system internal WhiteList Filter	Application	Warning	Event					X	X	X	X	
GPRS PPP password modified	Authorization	Warning	Event					X[3]				

1) The syslog events can be sent via these LAN interfaces
2) only supported by some protocol element firmwares (e.g. IEC 60807-5-104)!
3) CP-8022 only
4) CP-8000

Example:

Date	Time	Facility	Level	HostName	Message Text
2016-02-01	10:44:14	Local2	Notice	10.9.19.250	2016-02-01T10:44:14.210+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs 'TOOLBOX II CAEx online test' stopped
2016-02-01	10:43:59	Local2	Notice	10.9.19.250	2016-02-01T10:43:59.531+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs 'TOOLBOX II CAEx online test' started
2016-02-01	10:43:33	Local1	Notice	10.9.19.250	2016-02-01T10:43:26.185+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Engineering tool TOOLBOX II connected
2016-02-01	10:43:32	Local1	Notice	10.9.19.250	2001-01-01T00:00:04.230+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Engineering tool TOOLBOX II connected
2016-02-01	10:43:31	Local1	Notice	10.9.19.250	2001-01-01T00:00:01.997+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Engineering tool TOOLBOX II connected
2016-02-01	10:43:30	Local2	Notice	10.9.19.250	2001-01-01T00:00:01.820+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Port'1' link status has changed to LINK_UP
2016-02-01	10:43:29	Local2	Notice	10.9.19.250	2001-01-01T00:00:01.820+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Port'0' link status has changed to LINK_UP
2016-02-01	10:43:28	Local2	Notice	10.9.19.250	2001-01-01T00:00:01.489+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Flashcard inserted
2016-02-01	10:43:27	Local2	Notice	10.9.19.250	2001-01-01T00:00:06.793+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Syslog ready
2016-02-01	10:43:25	Local2	Notice	10.9.19.250	2001-01-01T00:00:06.793+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Syslog startup
2016-02-01	10:43:01	Local2	Warning	10.9.19.250	2016-02-01T10:43:01.351+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Parameters loaded
2016-02-01	10:37:36	Local2	Notice	10.9.19.250	2016-02-01T10:37:36.923+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs System message FC128' generated by 'TOOLBOX II message simulation'
2016-02-01	10:36:56	Local2	Notice	10.9.19.250	2016-02-01T10:36:56.895+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs User data message TI030' generated by 'TOOLBOX II message simulation'
2016-02-01	10:36:20	Local1	Notice	10.9.19.250	2016-02-01T10:36:20.967+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Engineering tool TOOLBOX II connected
2016-02-01	10:34:04	Local1	Notice	10.9.19.250	2016-02-01T10:34:04.844+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Engineering tool TOOLBOX II connected
2016-02-01	10:32:27	Local2	Notice	10.9.19.250	2016-02-01T10:32:28.050+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Port'0' link status has changed to LINK_UP
2016-02-01	10:32:19	Local2	Notice	10.9.19.250	2016-02-01T10:32:19.350+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Port'0' link status has changed to LINK_DOWN
2016-02-01	10:27:51	Local2	Notice	10.9.19.250	2016-01-24T16:17:45.130+01:00 R#130_C#170_BSE#020_SSE#254 SICAM_RTUs Port'1' link status has changed to LINK_UP

9.1.4 Configuration

9.1.4.1 SICAM A8000 Series / SICAM RTUs

The security logbook is deactivated by default. It can be activated on demand via SICAM TOOLBOX II: parameters `Network settings | Security |SysLog client UDP`, `SysLog server 1 IP address` and `SysLog portnr`.

SICAM A8000 CP-8031/CP-8050

In SICAM A8000 CP-8031/CP-8050, the security logbook as a system service can be used on each Ethernet interface (CP-8031/CP-8050 and CI-8520).

The required parameter are in the system-technical parameters of the BSE under `Network settings | SysLog | SysLog Client UDP`

SICAM A8000 CP-8000 / CP-802x

In the SICAM A8000 CP-8000 / CP-802x the security logbook can be used with the protocol element ET84 via the local ethernet interfaces (X1 and X4).

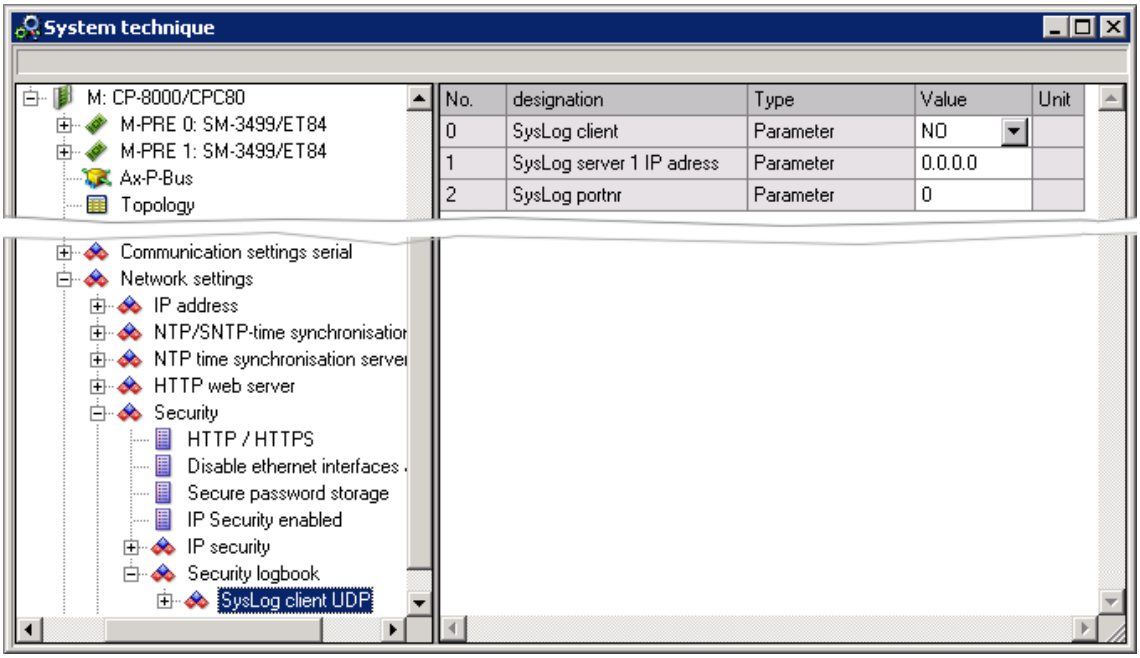
The required parameter are in the system-technical parameters of the BSE under `Network settings | Security | Security logbook | SysLog client UDP.`

SICAM AK 3

In SICAM AK 3 the security logbook can be used in 2 different ways:

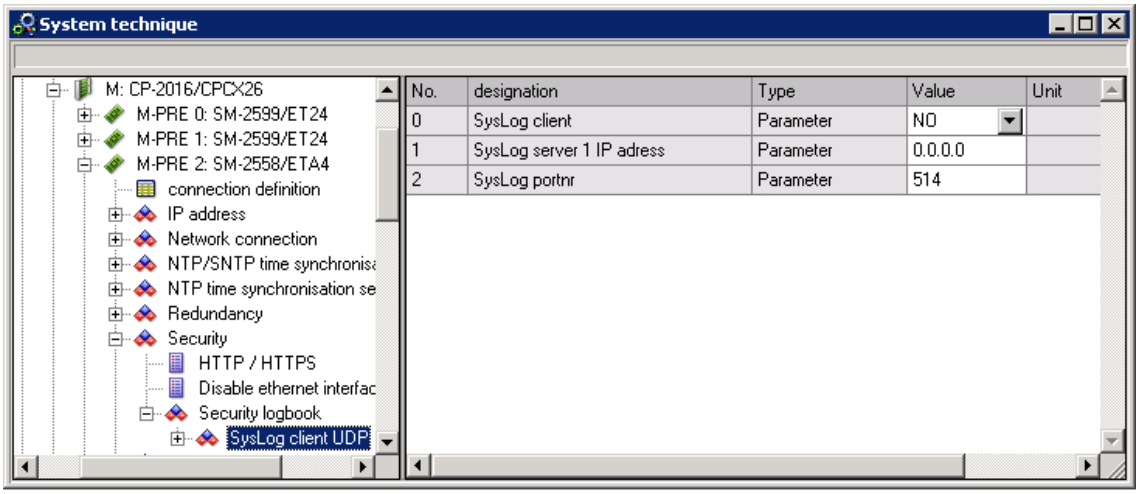
- With the protocol element ET24 via the local ethernet interfaces (X0 and X1) on BSE CP-2016/CPCX26 or CP-2019/PCCX26.

  The required parameter are in the system-technical parameters of the BSE under `Network settings |Security | Security logbook | SysLog Client UDP`.



With protocol element SM-2558/ETA4 on BSE CP-2016/CPCX26 or CP-2019/PCCX26. Used interface: X3

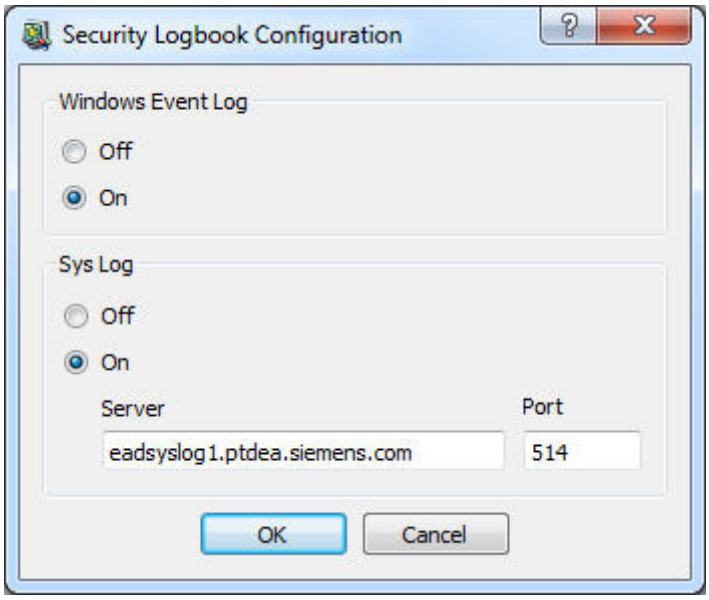
The required parameter are in the system-technical parameters of the PRE under `Security | Security logbook | SysLog Client UDP` .



9.1.4.2 SICAM TOOLBOX II

The security logbook is deactivated by default. It can be activated if required.

The corresponding parameter settings can be made with the SICAM TOOLBOX II–Tool „TOOLBOX II Presets“ via the menu item **Extras → Security logbook configuration**.



If an external syslog-server is used, it is necessary to configure its server name and port number.

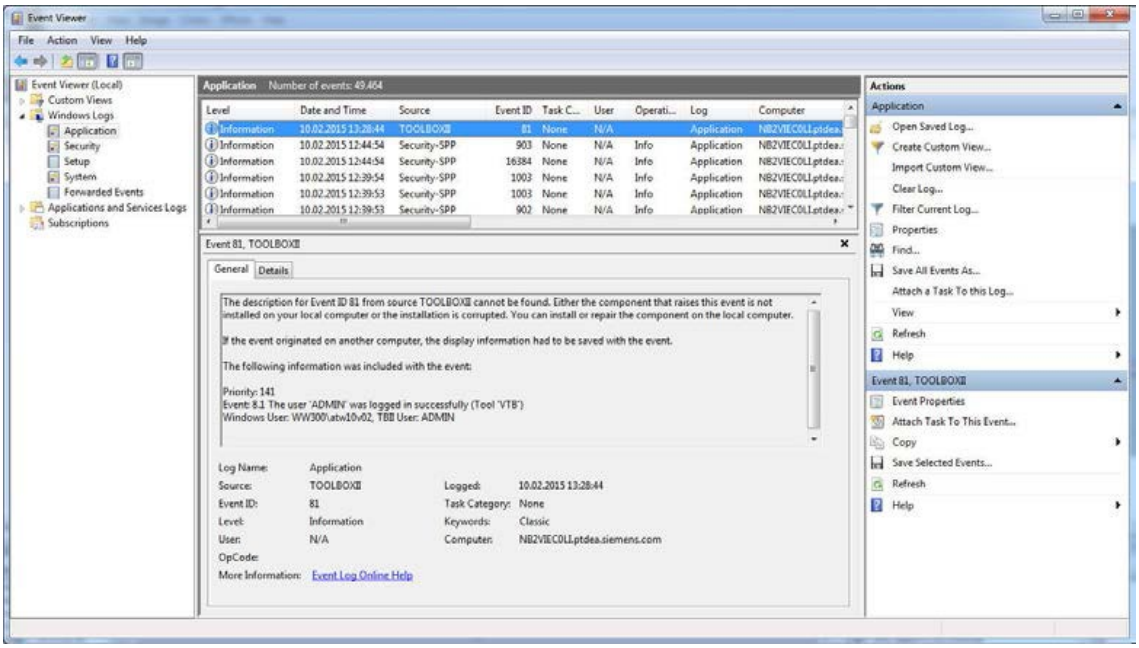
Hint

This menu item is only available for SICAM TOOLBOX II user with the authorization "Security Administrator".

9.1.4.3 Viewing Logbook

Windows Event Log

By means of the **Windows Event Viewer** it is possible to view the events stored on the SICAM TOOLBOX II-PC. Look under **Windows Logs** → **Application**.



Syslog-Server

The data stored on the syslog-server can be read with the syslog-viewer.

9.2 Diagnostic

SICAM A8000 Series / SICAM RTUs contains comprehensive functions for monitoring the system. Since the firmware automatically performs the corresponding error monitoring routines, for this no settings by the user are required.

With the SICAM TOOLBOX II function **Diagnostic** the local error tables of the selected AUs and the global error table are read out and examined for error entries. The result of the check is displayed in legible form (plain text) on the screen and can be printed out if required.

Depending on the selected type of diagnostic information is provided about the automation units and system elements as well as CPUs. Thereby only faulty AUs or system elements are listed.

Since the SICAM TOOLBOX II supports Remote Operation (remote access), the diagnostic is an important component of the remote maintenance.

The access to the Diagnostic function can be regulated via the user administration. Consequently e.g. a SICAM TOOLBOX II user can be set up, who may only perform Logging.

9.2.1.1 Diagnostic Functions

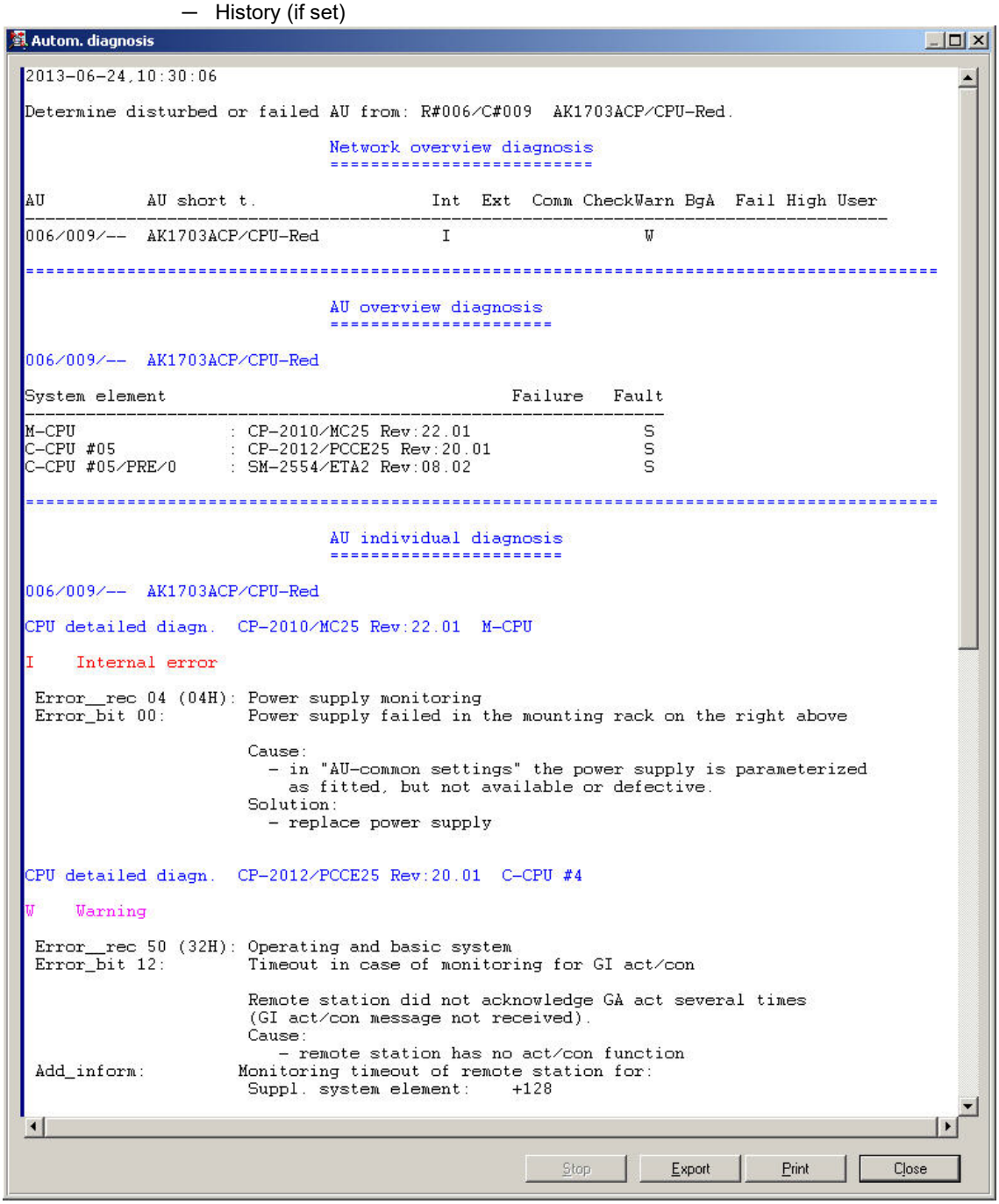
- Automatic Diagnostic

Supplies an overview of the error messages of all automation units located in the network as well as their system elements.

The automatic diagnostic contains information without a time stamp.

The outputs are structured hierarchically into

- Network overview diagnostic
- AU overview diagnostic
- AU individual diagnostic
- History (if set)



- Network overview diagnostic

Supplies a listing of all automation units located in the network for which errors have been recorded.

The Network overview diagnostic contains information without a time stamp.

- AU overview diagnostic

Supplies and error overview for all automation units that are displayed in the network overview diagnostic as faulty.

The AU overview diagnostic contains information without a time stamp.

- History Diagnostic

Supplies the history of error messages.

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

9.2.1.2 Diagnostic Classes

Diagnostic Class	Meaning
A ..... Failure	Signals, that an AU can no longer be reached.
B ..... Module failure	Signals, that the internal communication with a module is no longer possible.
I ..... Internal error	Error in hardware or firmware that can clearly be assigned to the respective module. e.g. checksum error in parameter memory
E ..... External error	Is detected through the monitoring of sensors and actuators. e.g. Live Zero, failure of minute pulse longer than can be tolerated
K ..... Communication	Is detected based on the monitoring of the communication connection.
W .... Warning	Signals, that the system has limited functionality or availability. E.g. failure of minute pulse, but quartz accuracy still adequate.
F ..... Freely configurable user error	User-related summation of diagnostic information
T ..... Test	Signals, that a function for test purposes has been specifically influenced. E.g. block of input information in the function diagram.

Hint

Further information about Diagnostic can be found in the following documents:

- *SICAM TOOLBOX II Online Help – Chapter Diagnostic*
- *SICAM RTUs Common Functions of System and Basic System Elements, Chapter "System Services", Section "Diagnostic"*

9.3 Logbook

The SICAM TOOLBOX II has a logbook, in which selectable user actions can be logged, such as e.g.: parameter change, parameter download, loading firmware into destination system, …

The logbook entries are stored centrally in the SICAM TOOLBOX II database and can be arbitrarily filtered.

The access to the logbook is regulated through the Role Administration (User-Roles LogConfig and LogView) of the SICAM TOOLBOX II. The access rights, consequently also the right to delete or export data records, can be assigned by the SICAM TOOLBOX II Administrator.

Older logbook entries are not overwritten. A “warning threshold” can be defined for a defined number of entries.

The SICAM TOOLBOX II – Logbook cannot be included in a central alarm management.

The SICAM TOOLBOX II – Logbook is called from the **OPM** under **Extras** → **Show Logbook**.

Hint

Further information about the logbook can be found in the following document:

- *SICAM TOOLBOX II Online Help – Chapter “Logbook”*

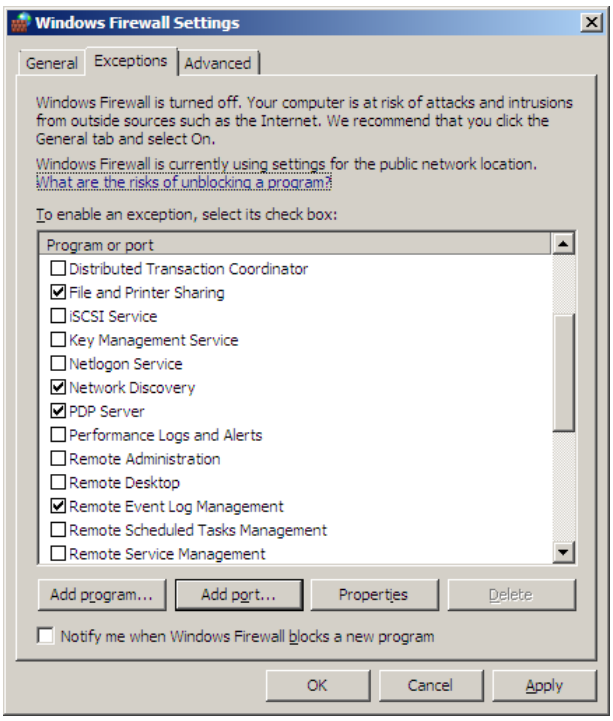
9.4 Logging with the Windows Event Display

Using the Windows Event Display it is possible to log remote accesses. Thereby several conditions are to be observed, in order to display the Remote-Log Files.

For this the Remote Registry-Service must be started on diverse Windows operating systems. With that you can see the descriptions or category fields in the Properties page of the Event Log.

1. Firstly you require Admin rights on the remote computer in order to read the log files. This user must also be created on the local computer with the same password. For reasons of security it is recommended to execute this procedure with *Run as*. In addition it is recommended to create an Audit-Administrator with Admin rights on both computers.

2. If the Firewall is activated as recommended you must open the incoming data traffic for Remote Event Logging.



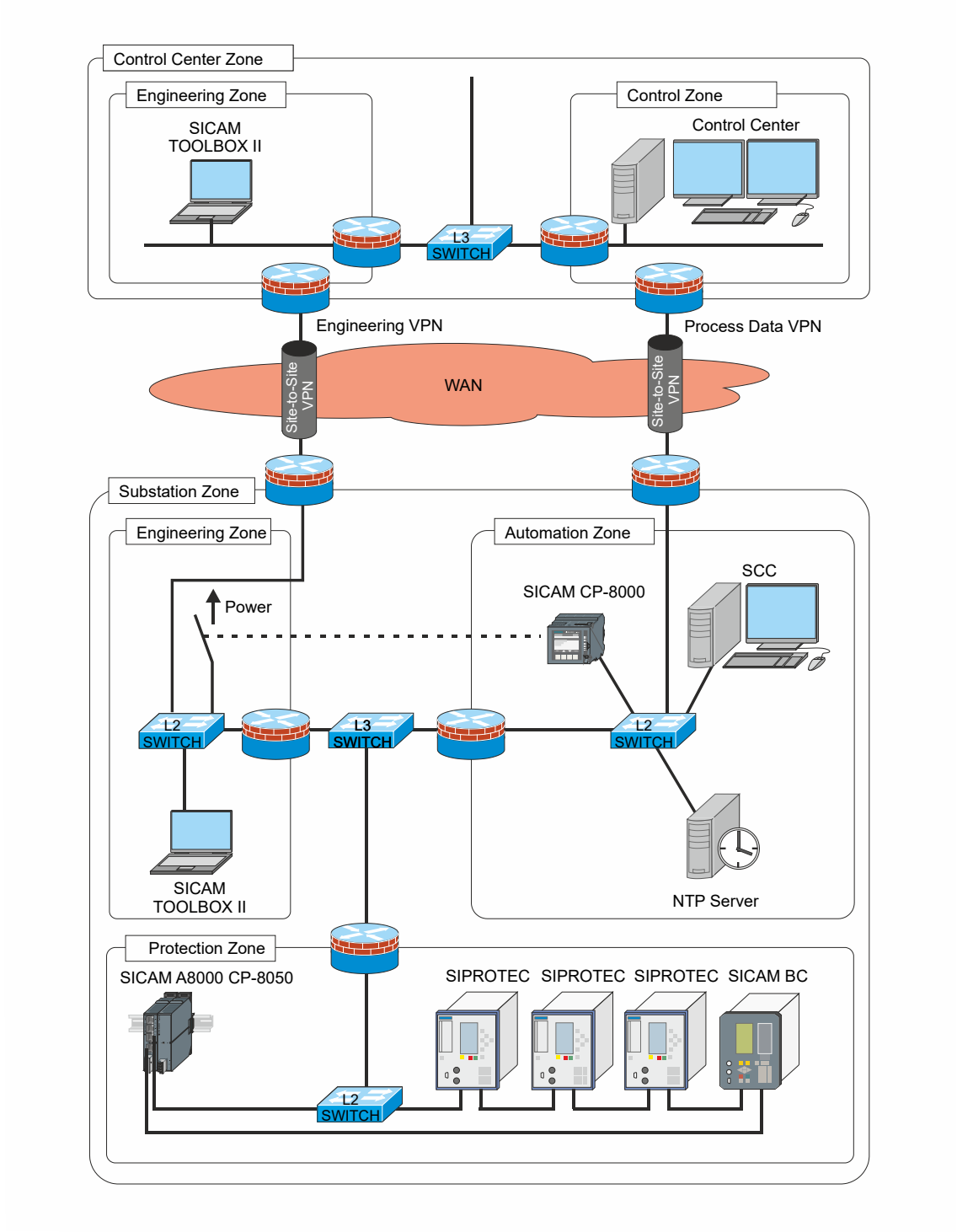
10 Remote Maintenance

Contents

10.1 Remote Maintenance via SICAM TOOLBOX II 177
10.2 Remote Maintenance via SICAM Device Manager 179

10.1 Remote Maintenance via SICAM TOOLBOX II

With the help of the option “web.engineering”, with a controlling PC (remote maintenance control center) one can remotely operate (remote maintenance session) a remote SICAM TOOLBOX II, that can be reached over a data connection (Modem, ISDN, LAN/WAN).



With “web.engineering” all SICAM TOOLBOX II Clients work with a central Web Server, on which the SICAM TOOLBOX II runs. The SICAM TOOLBOX II is thereby operated in the Web Browser.

Hint

Info for system design, product/system service and control center/system operation:

This requirement is not product relevant and is therefore to be taken into account during system design, product/system service and control center/system operation.

10.1.1 Configuration of Servers and Clients

Install *Microsoft Windows* ® with “Terminal Services Web Access” (TS Web Access)on the Web Server. Then install the SICAM TOOLBOX II on this server.

No installation is required on the Clients, the access to the Web Server takes place over *Microsoft Internet Explorer* ® (from Version 5.0).

A detailed description of the configuration can be found in the *SICAM TOOLBOX II Online Help, Chapter “web.engineering”*.

10.2 Remote Maintenance via SICAM Device Manager

All devices can be maintained remotely via Ethernet.

11 User Administration

Contents

11.1 Introduction 181
11.2 SICAM A8000 Series / SICAM RTUs 182
11.3 SICAM TOOLBOX II 184
11.4 SICAM Device Manager 187

11.1 Introduction

SICAM RTUs

With the use of the SICAM TOOLBOX II, in SICAM RTUs there is no user- and role administration, as the user- and role administration takes place in the SICAM TOOLBOX II.

SICAM A8000 Series

SICAM A8000 Series support both with the use of SICAM TOOLBOX II and with the use of SICAM WEB a user- and role administration, refer to chapter 3.3.9 Role-Based-Access-Control in SICAM A8000 Series.

Additionally, you can set a „Connection Password“ in SICAM A8000 CP-8000/CP-802x / SICAM RTUs which is not saved in the SICAM TOOLBOX II (see chapter Connection Password).

Internal/External Authentication (RADIUS-Server)

The SICAM A8000 Series provide different authentication mechanisms. Depending on the settings (parameter `Radius Authentication` = **YES**), SICAM WEB uses the respective role information:

- Authentication via locally stored credentials
  - Usernames, passwords, profiles defined by SICAM A8000 Series will be used
- Authentication via external service (RADIUS server)
  - Usernames, passwords, profiles defined by the RADIUS server will be used
  - Fallback option, if the RADIUS server is not available

Details about authentication via Webbrowser are described in the SICAM A8000 Series manual.

For SICAM RTUs which do not support the WEB parameterization, but have a WEB Server (NIP's), there are no roles. Data can only be viewed.

For external authentication in SICAM A8000 Series via RADIUS refer to chapter 3.3.11.

SICAM TOOLBOX II

In the SICAM TOOLBOX II there exists one user/role function.
Accesses and authorizations can be freely defined role-specific, the users can be assigned roles.

The standard roles of the SICAM TOOLBOX II (ADMIN, PROFI, and STANDARD) can be expanded by a SICAM TOOLBOX II Administrator with additional roles.

Hint
The authorization “Administrator” must be granted for the creation and modification of users, roles and their assignment. Only the password of the logged on user can be changed with the other authorizations.

The following operations can be performed with the User/Role Administration in SICAM TOOLBOX II:

- Definition of users with password
- Definition of roles with associated authorization
- Definition of the assignment of users to particular roles
- Deletion of users

11.2 SICAM A8000 Series / SICAM RTUs

11.2.1 SICAM A8000 Series

The definition of users, their passwords and the assignment of roles to these users is realized via SICAM WEB.

The following user with the role ADMINISTRATOR is predefined

User name	Password	Role
administrator	******** [1)]	ADMINISTRATOR

[1)] CP-8031/CP-8050, CPC80 of CP-8000, CP-802x >= revision 14: no default password set
CPC80 of CP-8000, CP-802x <= revision 07 has default password 1703

Hint
The predefined password must be changed after the first logon. For details see the manual of the SICAM A8000 Series.

User names and passwords are stored in the device and are not part of the master data (any more).

In the course of a firmware update to revision 14 or higher user names and passwords defined in CP-8000, CP-802x, CPC80 < revision 14 are automatically migrated to the new internal local user database

CPC80 < revision 14		CPC80 >= revision 14	
User name	**Password**	**Role**	**Password**
administrator	********	ADMINISTRATOR	[1)]
guest	********	VIEWER	[1)]

[1] password change mandatory

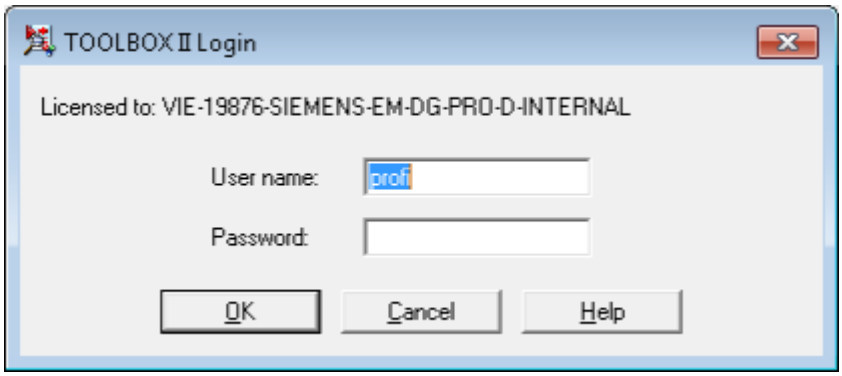
11.2.1.1 Roles

Roles in the SICAM A8000 Series (RBAC) are described in the chapters 3.3.9 (Role-Based-Access-Control in SICAM A8000 Series.

Role Based Access Control when working with SICAM TOOLBOX II

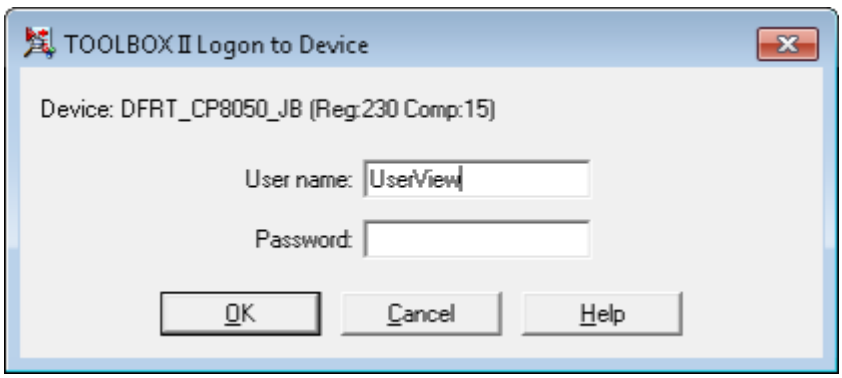
After SICAM TOOLBOX II is started the Login-dialog is displayed.

Enter user name and password.

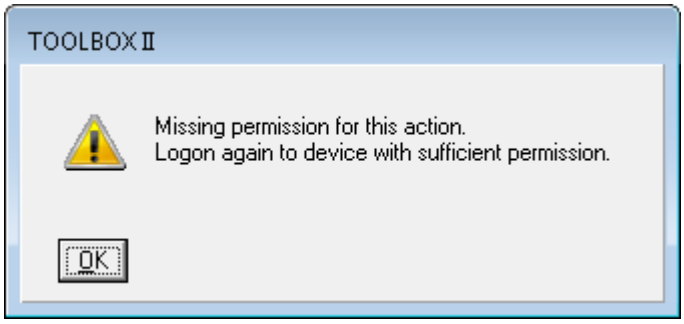


Role based access control becomes effective as soon as you want to perform operational actions via SICAM TOOLBOX II which require an online connection to SICAM A8000 Series (e.g.: diagnosis)

Use a local user, defined via SICAM WEB (user name and password)



The following warning is displayed if a user logged on to the device does not have the corresponding rights to execute the intended action.



You have now the possibility to chose a different user with corresponding rights and to log on again to the device with these different credentials (name and password) to resume the operational action.

After successfully logging in, all actions granted to the current user can be performed without re-logging in.

Hint

A re-logging in will be necessary after 2 minutes of inactivity or in case of disconnection from the device.

11.3 SICAM TOOLBOX II

11.3.1 Defining Users

In the SICAM TOOLBOX II defining users does not only means the creation of new users, but also the deletion of users or the modification of the user password. The associated dialog is called from the SICAM TOOLBOX II tool **Toolbox II presets** (-> **EMII Presets Toolbox**) with the command **Authorization** → **User/Role Administration** → **Define Users ...**.

The following predefined users are available by default:

User	Password	Hint
PROFI	profi	Standard user. These can be deleted.
STANDARD	standard	
ADMIN	admin	
SAT_ROOT	sat_root	These users can be disabled or removed from SICAM TOOLBOX II V5.11 or higher
SAT250	passme	
SAT_ADM	sat_adm	
SAT_INT	sat_int	

Hint

- A maximum of 8 characters (case insensitive) can be used per user and associated password.
- The default passwords for all users must be changed after the initial installation.
- Further details can be found in the SICAM TOOLBOX II Online Help.

11.3.1.1 Define Domain Users

From SICAM TOOLBOX II V5.11 it is possible to create domain users. Such a domain user does not use a specific SICAM TOOLBOX II user role to start SICAM TOOLBOX II, but he uses the user account for the logon on his workstation.

Benefit: The user must not logon again to SICAM TOOLBOX after the logon on his workstation. (Single-Sign-On)

Hint

- The password can contain uppercase and lowercase letters, numbers and special characters according to the security settings of your network.
- The user must keep safe the admin password. There is no way to restore it, if it gets lost!
- You can find further details in the SICAM TOOLBOX II online help.

11.3.2 Defining Roles

A role is a collection of authorizations that can be assigned to a user. The definition of a role is carried out in the SICAM TOOLBOX II tool **Toolbox II presets** (-> **EMII Presets Toolbox**) with the command **Authorization** → **User/Role Administration** → **Define Roles ...**.

The following list shows the authorizations for the predefined roles TB_ADMINISTRATOR, TB_PROFESSIONAL and TB_Standard.

Authorization	TB_ADMINISTRATOR	TB_PROFESSIONAL	TB_Standard
Remote operation	x	x	x
Administrator	x		
Plant management	x	x	
Assembly technique I documentation	x	x	x
HW/FM Configuration (Hardware/Firmware)	x	x	
CAEx online test	x	x	
CAEx plus	x	x	
Data flow test	x	x	x
Diagnosis	x	x	x
Documentation	x	x	x
Load firmware	x	x	x
Import/Export/Backup	x	x	x
Conversion TBI <-> TBII	x	x	
LogConfig (log configure)	x		
LogView (log display)	x	x	x
OPM: Type editing	x	x	x
Object-Oriented Process Data Manager	x	x	x
Load parameters (1703)	x	x	x
Load parameters (protection)	x	x	x
Load parameters (test operation)	x	x	

Authorization	TB_ADMINISTRATOR	TB_PROFESSIONAL	TB_Standard
Start Parameter Loader	x	x	x
Parameter settings	x	x	
Parameter settings protection parameter (operation)	x		
Parameter settings protection parameter (configuration)	x		
Revision interrogation and display	x	x	x
250 SCALA: Start Loader	x	x	x
250 SCALA: Upload PV from CAE into OPMII	x	x	x
SICAM 1703 Up-/Download Function			
ST-Emulation	x		
Safety online	x		
Safety parameter change	x		
Security administrator			
Service window offline	x	x	
Service function online	x	x	
Import Master data	x	x	
Message simulation	x	x	
Topology test	x	x	x
Transformer Preview	x	x	x
Presets CAEx	x	x	
Presets TOOLBOX II	x	x	x

Specific roles can be defined for particular cases of application and projects.

Hint

Further details can be found in the SICAM TOOLBOX II Online Help.

11.3.3 Assignment User <-> Role

The assignment User <-> Role takes place in the SICAM TOOLBOX II tool **Toolbox II presets** (-> **EMII Presets Toolbox**) with the command **Authorization** → **User/Role management** → **Assignment User <-> Role...**.

Hint

Further details can be found in the SICAM TOOLBOX II Online Help.

11.3.4 Changing User Passwords

Each user has the permission to change his password. The definition is done in the SICAM TOOLBOX II-Tool **TOOLBOX II presets** (-> **EMII Presets Toolbox**) with the command **Authorization → User/Role management → Define User** .

Select the user name in the "Define User" window and click "Change Password" to get to the appropriate dialog window.

Hint

The preset password must be changed after the first logon.

11.4 SICAM Device Manager

There is no user/roles-concept within the SICAM Device Manager. RBAC functionality is carried out by the device. When connecting to the device, user authentication is a must.

12 Hardware Interfaces

Detailed information can be found in the respective device manuals.

A Security Measure Plan for Oracle Database

A.1 Checklist according to “Security Measure Plan for Oracle Database 12c”

(Released by Siemens Cert, 2017-02-28. Version 2.0)

System Name: SICAM TOOLBOX II, 6.01 HF01

Version of checked Database: Oracle 12.1.0.1.160719

Chapter No.	Measure No.	Measure	Done
3.1	**M126797**	**Secure Underlying Operating System**	**No**
		The database is embedded in TOOLBOXII. The TOOLBOX II policy according securing of the underlying operating system is to give its responsibility in customer’s hand.	
3.2	**M126112**	**Perform Secure Installation**	**Yes**
3.3	**M126833**	**Apply Oracle Security Patches**	**Yes *)**
		Each new TOOLBOXII release uses the latest Oracle Security Patch. During TOOLBOXII's lifetime it is possible to get current Oracle Security Patches by using special TBII Hotfixes.	
3.4	**M126580**	**Secure the Oracle Data Dictionary**	**Yes **)**
3.5	**M126738**	**Separate Datasets that Belong to Different Application Domains**	**Yes**
		All datasets belongs only to TOOLBOXII. There are no other application domains.	
3.6	**M126734**	**Protect Stored Confidential Data** Database- and TOOLBOX II-Passwords are encrypted. All other data is classified as not confidential, therefore it is not encrypted.	**Yes**
4.1	**M126140**	**Disable Execution of Administrative Commands in TNS Listener**	**Yes**
4.2	**M126876**	**Restrict Access to TNS Listener**	**No**
		By default there is no restriction of network access to TNS Listener. If required, it can be done by System Administrators.	
4.3	**M126621**	**Disable the use of SSLv3**	**Yes**
4.4	**M126360**	**Set Authentication Timeout**	**Yes**
4.5	**M126811**	**Leave Remote Authentication Disabled**	**Yes**
4.6	**M126436**	**Protect Confidential Network Traffic**	**Yes**
		Database- and TOOLBOXII-Passwords are encrypted. All other data is classified as not confidential, therefore it is not encrypted.	
5.1	**M126351**	**Use Secure Logon Version**	**Yes**
5.2	**M126884**	**Change Default Passwords**	**Yes**
5.3	**M126150**	**Disable Unneeded Accounts**	**Yes**
5.4	**M126954**	**Adapt User Profile Password Settings**	**Partly**
		All settings are done, except limitation of maximum password lifetime. Reason: Database only possible client is SICAM TOOLBOX II. It's database passwords are changed at each SICAM TOOLBOX II major release.	

Chapter No.	Measure No.	Measure	Done
5.4	**M126427**	**Check Password Complexity**	**No**
		During login password complexity checking is not enabled. Reason: Database only client is SICAM TOOLBOX II, which uses during one major release the same passwords. Each of these TOOLBOX II passwords follow the required complexity.	
6.1	**M126790**	**Set Unified Auditing**	**No**
		Unified auditing was not set because of: - too much created data, which needs special maintenance - because of many thousands installations regularly reviews of audit logs are practically not possible	
6.2	**M126572**	**Leave TNS Listener Logging Enabled**	**Yes**
7.1	**M126660**	**Apply the Principle of Least Privilege**	**Yes**
7.2	**M126633**	**Restrict or Revoke Access to Directories for UTL_FILE**	**Yes**
7.3	**M126521**	**Revoke Access to PL/SQL Network Utility Packages**	**Yes**
7.4	**M126472**	**Limit External Procedure Privileges**	**Yes**
7.5	**M126368**	**Restrict Dynamic SQL Privileges for PUBLIC**	**Yes**

*) WINDOWS DB BUNDLE PATCH 12.1.0.1.160719
**) WINDOWS DB BUNDLE PATCH 12.1.0.1.160719

B Licensing agreement

B.1 Open Source Software Used in the SICAM A8000 Series

These products contain, among other things, Open Source Software developed by third parties. The Open Source Software used in this product and the license agreements concerning this software can be found in the Readme_OSS. These Open Source Software files are protected by copyright.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between Siemens license conditions and the Open Source Software license conditions, the Open Source Software conditions shall prevail with respect to the Open Source Software portions of the software. The Open Source Software is licensed royalty-free.

Insofar as the applicable Open Source Software License Conditions provide for it you can order the source code of the Open Source Software from your Siemens sales contact - against payment of the shipping and handling charges - for a period of at least 3 years since purchase of the Product.

We are liable for this Product including the Open Source Software contained in it pursuant to the license conditions applicable to the Product. Any liability for the Open Source Software beyond the program flow intended for this Product is explicitly excluded. Furthermore any liability for defects resulting from modifications to the Open Source Software by you or third parties is excluded. We do not provide any technical support for this Product if it has been modified.

Valid for SICAM A8000 CP-8000/ CP-802x (CPC80) only:

The Open Source Software used in these products and the license agreements concerning this software can be found on the the SICAM A8000 CP-8000/CP-802x SD card in the file *ReadmOSS.htm.*

Path for Readme_OSS:
SD card:\OSS\<Firmwarenumber>\<Revision>\ReadmOSS.htm.
e.g.: *SD card:\OSS\CPC80\01.01\ReadmOSS.htm*

Hint
You need an SD card reader and a web browser to read the htm-file.

B.2 Open Source Software Used in SICAM RTUs

This product contains, among other things, Open Source Software developed by third parties. The Open Source Software used in this product and the license agreements concerning this software can be found in the Readme_OSS. These Open Source Software files are protected by copyright.

Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between Siemens license conditions and the Open Source Software license conditions, the Open Source Software conditions shall prevail with respect to the Open Source Software portions of the software. The Open Source Software is licensed royalty-free.

Insofar as the applicable Open Source Software License Conditions provide for it you can order the source code of the Open Source Software from your Siemens sales contact - against payment of the shipping and handling charges - for a period of at least 3 years since purchase of the Product.

We are liable for this Product including the Open Source Software contained in it pursuant to the license conditions applicable to the Product. Any liability for the Open Source Software beyond the program flow intended for this Product is explicitly excluded. Furthermore any liability for defects resulting from modifications to the Open Source Software by you or third parties is excluded. We do not provide any technical support for this Product if it has been modified.

The Open Source Software used in this product and the license agreements concerning this software can be found on the SICAM RTUs SD card in the file *ReadmOSS.htm.*

To readout this file, you need an application which you can download from the Internet. You can find details for the download and the use of the application in the following chapter.

B.2.1 Readout of ReadmOSS.htm

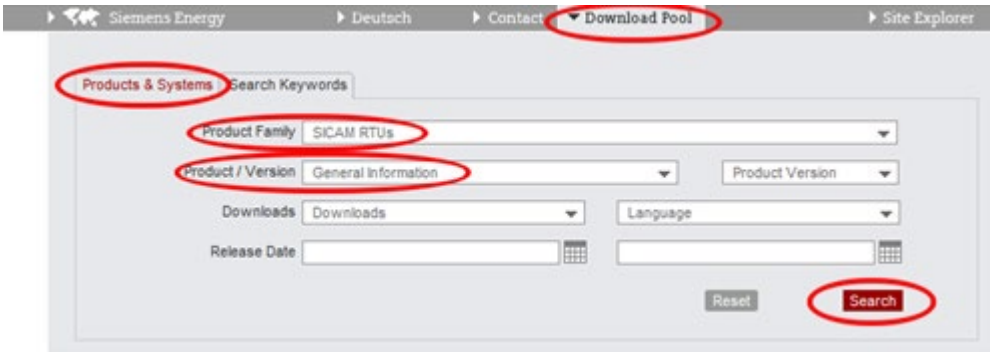
Hint
You need an SD card reader and a web browser to read the htm-file.

The application for the readout of the ReadmOSS-data from the SD-card can be downloaded from following web page: http://www.energy.siemens.com/

Click Download Pool in the menu bar and select on tab Products & Systems following options:

- Product Family: SICAM RTUs
- Product / Version: General Infomation

Click Search

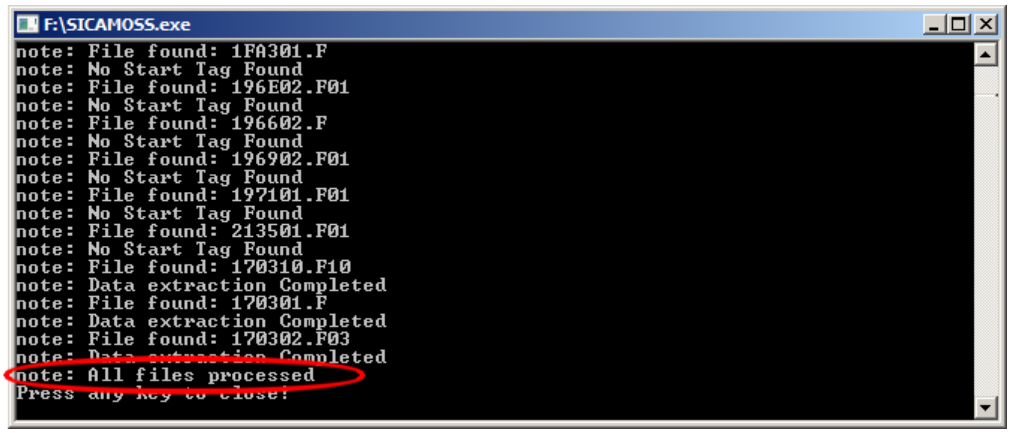


Click on SICAM RTUs OSS Extractor in the result list to start the download.

When the download is finished you will get the file SICAMOSS.zip.

Unzip this file and save the therein contained file (*SICAMOSS.exe*) in the root path of the SD-card from which you want to readout the license agreement.

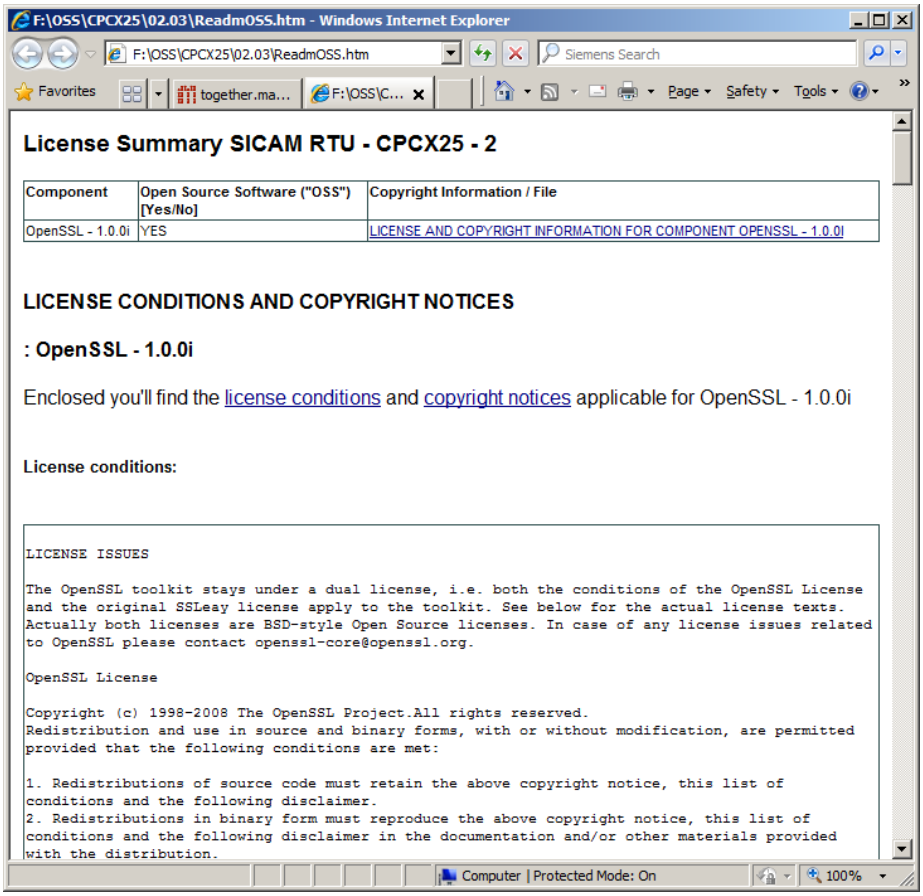
Start now *SICAMOSS.exe*. During the readout process you can see a DOS-window. If the line `note: All files processed` is displayed you can close the DOS-window by pressing any key.



Now you can find on the SD-card the folder *OSS* with several subfolders. One single folder for each firmware which uses open source components. Within these subfolders are again folders for each used firmware revision. These folders contain the corresponding license data.

Path for ReadmeOSS:
SD-Card:\OSS\<Firmwarename>\<Firmwarenumber>\<Revision>\ReadmOSS.htm.
E.g.: *SD-Card:\OSS\ETA4\02.01\ReadmOSS.htm*

B.3 Example of a ReadmOSS.htm:



Literature

White Paper - Requirements for Secure Control and Telecommunication Systems	Version 2.0
Oesterreichs Energie and DKE German Commission for Electrical, Electronic & Information Technologies of DIN and VDE Common instructions for the application of the BDEW White Paper	Working version 2.01
NERC CIP (North American Electric Reliability Corporation - Critical Infrastructure Protection)	www.nerc.com
SICAM A8000 Series RTUs Conformance Statement	DC0-161-1
SICAM RTUs, Ax 1703 Common Functions Protocol Elements	DC0-023-2
SICAM RTUs Common Functions Peripheral Elements According to IEC 60870-5-101/104	DC0-011-2
SICAM RTUs Common Functions System and Basic System Elements	DC0-015-2
SICAM AK 3 User Manual	DC2-028-2
SICAM AK 3 System Description	MC2-025-2
SICAM A8000 Series CP-8000, CP-802x, User Manual	DC8-037-2
SICAM A8000 Series CP-8031, CP-8050 Manual	DC8-026-2
SICAM BC System Manual	DC5-014-2
SICAM A8000 Series RTUs Security Penetration Testing	DC0-134-2
SICAM / SIPROTEC System Hardening for Substation Automation and Protection User Guide	https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&mandator=ic_sg&id1=DLA20_114
SICAM Device Manager, Product Information	D51-001-1
SICAM Device Manager User Manual	D51-003-1
SICAM TOOLBOX II Online Help *)	
SICAM PTS Protocol Test System	SA0-900-7
SICAM GridPass Manual (English only)	E50417-H8940-C598-A6

*) available in the engineering system SICAM TOOLBOX II