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

Disclaimer of Liability
This document has been subjected to rigorous technical review before being published. It is revised at regular intervals, and any modifications and amendments are included in the subsequent issues. The content of this document has been compiled for information purposes only. Although Siemens AG has made best efforts to keep the document as precise and up-to-date as possible, Siemens AG shall not assume any liability for defects and damage which result through use of the information contained herein.
This content does not form part of a contract or of business relations; nor does it change these. All obligations of Siemens AG are stated in the relevant contractual agreements.
Siemens AG reserves the right to revise this document from time to time.
Document version: E50417-H8940-C619-A1.01
Edition: 05.2018
Version of the product described: V01.20

Copyright
Copyright © Siemens AG 2018. All rights reserved.
The disclosure, duplication, distribution and editing of this document, or utilization and communication of the content are not permitted, unless authorized in writing. All rights, including rights created by patent grant or registration of a utility model or a design, are reserved.

Registered Trademarks
SIPROTEC®, DIGSI®, SIGUARD®, SIMEAS®, and SICAM® are registered trademarks of Siemens AG. Any unauthorized use is illegal. All other designations in this document can be trademarks whose use by third parties for their own purposes can infringe the rights of the owner.
Preface

Purpose of the Manual

This document is a guideline for administrators and system engineers to design a substation based on SIPROTEC and SICAM products in a secure manner. The guideline addresses following domain:

- Secure network topology
- Firewalls and network-based Intrusion Detection Systems (NIDS)
- Malware protection and prevention
- User management and role-based access control
- Business continuity and disaster recovery
- System hardening

Target Audience

Protection system engineers, commissioning engineers, persons entrusted with the setting, testing and maintenance of automation, selective protection and control equipment, and operational crew in electrical installations and power plants, security experts, and security-versed administrators and integrators.

Scope

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

Indication of Conformity


This conformity is proved by tests conducted by Siemens AG in accordance with the Council Directive in agreement with the generic standards EN 61000-6-2 and EN 61000-6-4 for EMC directive, and with the standard EN 60255-27 for the low-voltage directive.

The device has been designed and produced for industrial use.

The product conforms with the international standards of the series IEC 60255 and the German standard VDE 0435.

Other Standards

IEEE Std C 37.90

The technical data of the product is approved in accordance with UL.

For more information about the UL database, see certified.ul.com

Select Online Certifications Directory and enter E194016 as UL File Number.
Additional Support

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

Support

Our Customer Support Center provides a 24-hour service.

Phone: +49 (180) 524-7000
Fax: +49 (180) 524-2471
E-Mail: support.energy@siemens.com

Training Courses

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

Siemens AG
Siemens Power Academy TD

Humboldtstraße 59
90459 Nürnberg
Germany

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

Notes on Safety

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

⚠️ **DANGER**

_DANGER_ means that death or severe injury _will_ result if the measures specified are not taken.

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

⚠️ **WARNING**

_WARNING_ means that death or severe injury _may_ result if the measures specified are not taken.

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

CAUTION means that medium-severe or slight injuries can occur if the specified measures are not taken.
✧ Comply with all instructions, in order to avoid moderate or minor injuries.

NOTICE

NOTICE means that property damage can result if the measures specified are not taken.
✧ Comply with all instructions, in order to avoid property damage.

NOTE

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

Qualified Electrical Engineering Personnel

Only qualified electrical engineering personnel may commission and operate the equipment (module, device) described in this document. Qualified electrical engineering personnel in the sense of this manual are people who can demonstrate technical qualifications as electrical technicians. These persons may commission, isolate, ground and label devices, systems and circuits according to the standards of safety engineering.

Proper Use

The equipment (device, module) may be used only for such applications as set out in the catalogs and the technical description, and only in combination with third-party equipment recommended and approved by Siemens.

Problem-free and safe operation of the product depends on the following:
• Proper transport
• Proper storage, setup and installation
• Proper operation and maintenance

When electrical equipment is operated, hazardous voltages are inevitably present in certain parts. If proper action is not taken, death, severe injury or property damage can result:
• The equipment must be grounded at the grounding terminal before any connections are made.
• All circuit components connected to the power supply may be subject to dangerous voltage.
• Hazardous voltages may be present in equipment even after the supply voltage has been disconnected (capacitors can still be charged).
• Operation of equipment with exposed current-transformer circuits is prohibited. Before disconnecting the equipment, ensure that the current-transformer circuits are short-circuited.
• The limiting values stated in the document must not be exceeded. This must also be considered during testing and commissioning.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>3</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>9</td>
</tr>
<tr>
<td>1.1 Scope/Overview</td>
<td>10</td>
</tr>
<tr>
<td>1.2 Principles</td>
<td>10</td>
</tr>
<tr>
<td>2 Network Security</td>
<td>11</td>
</tr>
<tr>
<td>2.1 Principles of a Secure Substation Configuration</td>
<td>12</td>
</tr>
<tr>
<td>2.2 Network Segmentation</td>
<td>12</td>
</tr>
<tr>
<td>2.3 Recommendations</td>
<td>13</td>
</tr>
<tr>
<td>2.4 VPN</td>
<td>13</td>
</tr>
<tr>
<td>2.4.1 General</td>
<td>13</td>
</tr>
<tr>
<td>2.4.2 Windows IPSec Implementation</td>
<td>14</td>
</tr>
<tr>
<td>2.4.2.1 General</td>
<td>14</td>
</tr>
<tr>
<td>2.4.2.2 Windows IPSec Configuration</td>
<td>14</td>
</tr>
<tr>
<td>2.4.2.3 IP Security Monitoring</td>
<td>50</td>
</tr>
<tr>
<td>2.4.3 IPSec VPN Appliance Siemens SCALANCE S</td>
<td>51</td>
</tr>
<tr>
<td>2.4.3.1 General</td>
<td>51</td>
</tr>
<tr>
<td>2.4.3.2 Siemens SCALANCE S Configuration</td>
<td>52</td>
</tr>
<tr>
<td>2.5 Firewall</td>
<td>59</td>
</tr>
<tr>
<td>2.5.1 Host-Based Firewalls</td>
<td>59</td>
</tr>
<tr>
<td>2.5.2 SCALANCE S Firewall Functionality</td>
<td>61</td>
</tr>
<tr>
<td>2.6 Parallel Redundancy Protocol (PRP)</td>
<td>61</td>
</tr>
<tr>
<td>2.7 Secure Communication with the IEC 60870-5-104 Protocol</td>
<td>62</td>
</tr>
<tr>
<td>2.7.1 Fulfilling the IEC 62351-3</td>
<td>62</td>
</tr>
<tr>
<td>2.7.2 IEC 60870-5-104 protocol</td>
<td>64</td>
</tr>
<tr>
<td>2.7.3 Preconditions</td>
<td>65</td>
</tr>
<tr>
<td>2.7.4 Creating Key Material</td>
<td>65</td>
</tr>
<tr>
<td>2.7.5 Building Your Own PKI (Public Key Infrastructure)</td>
<td>66</td>
</tr>
<tr>
<td>2.7.5.1 Preparation of OpenSSL and Easy-RSA-PKI Scripts</td>
<td>66</td>
</tr>
<tr>
<td>2.7.5.2 Usage of Easy-RSA-PKI</td>
<td>69</td>
</tr>
<tr>
<td>2.7.6 Securing Application with Stunnel</td>
<td>77</td>
</tr>
<tr>
<td>2.7.6.1 General</td>
<td>77</td>
</tr>
<tr>
<td>2.7.6.2 Stunnel</td>
<td>79</td>
</tr>
<tr>
<td>2.7.6.3 SICAM 230 Configuration for stunnel</td>
<td>90</td>
</tr>
<tr>
<td>2.7.6.4 Checking installation</td>
<td>90</td>
</tr>
<tr>
<td>2.7.7 Securing SICAM PAS</td>
<td>91</td>
</tr>
<tr>
<td>2.7.7.1 Installation and Configuration</td>
<td>91</td>
</tr>
<tr>
<td>2.7.7.2 Transmission Parameters</td>
<td>91</td>
</tr>
<tr>
<td>2.7.7.3 Checking installation</td>
<td>94</td>
</tr>
<tr>
<td>2.7.8 Additional information</td>
<td>95</td>
</tr>
<tr>
<td>2.7.8.1 Firewalling</td>
<td>95</td>
</tr>
</tbody>
</table>
2.7.8.2 Using More than One SICAM PAS........................................................................................................... 95

3 User Management................................................................................................................................................... 100
3.1 Least Privilege.................................................................................................................................................. 101

4 Logging............................................................................................................................................................. 103
4.1 General.......................................................................................................................................................... 104
4.2 Logging with Event Viewer - Step by Step Manual for Windows 7 (Local Site) and Windows Server 2008 (Remote Site).................................................................................................................. 106
4.3 Logging with Syslog......................................................................................................................................... 110
4.4 Syslog Client.................................................................................................................................................. 111
4.5 Syslog Server................................................................................................................................................ 112
4.5.1 General.................................................................................................................................................. 112
4.5.2 Syslog Server with NXLog.................................................................................................................. 112
4.5.3 RsYlog with LogAnalyzer.................................................................................................................. 114
4.5.3.1 Preconditions.................................................................................................................................. 114
4.5.3.2 Installation...................................................................................................................................... 114
4.5.3.3 Using LogAnalyzer.................................................................................................................. 114
4.5.3.4 Administration of Syslog Server.......................................................................................... 115
4.6 CrossBow.................................................................................................................................................. 117
4.6.1 General................................................................................................................................................ 117
4.6.2 Customer Benefit.................................................................................................................................. 117
4.6.3 Environment of a CrossBow System.......................................................................................... 118
4.6.4 Installation of a CrossBow System.......................................................................................... 119
4.6.5 Configuration of a CrossBow System.......................................................................................... 119
4.6.5.1 General...................................................................................................................................... 119
4.6.5.2 CrossBow Server.................................................................................................................. 119
4.6.5.3 CrossBow System Configuration.......................................................................................... 122
4.6.6 Elementary Usage of CrossBow concerning EM DG PRO Products.................................................. 127
4.6.6.1 Login to CrossBow Client....................................................................................................... 127
4.6.6.2 Licenses for CAMs.................................................................................................................. 128
4.6.6.3 Execute Special Operations on a Device.............................................................................. 130
4.6.6.4 Execute Crossbow Application Modules .............................................................................. 132
4.6.6.5 CrossBow Debug Logger....................................................................................................... 134

5 Malware Protection/Prevention........................................................................................................................... 135
5.1 Motivation.................................................................................................................................................. 136
5.2 Virus scan.................................................................................................................................................. 136
5.3 Whitelisting, McAfee Whitelisting.............................................................................................................. 136
5.3.1 Overview............................................................................................................................................... 136
5.3.2 Product Description .......................................................................................................................... 137
5.3.3 Offline Solution – AC and CC with CLI......................................................................................... 137
5.3.3.1 General...................................................................................................................................... 137
5.3.3.2 Area of Operation.................................................................................................................. 138
5.3.3.3 Procedure Overview.............................................................................................................. 138
5.3.4 Online Solution – AC and CC with ePO......................................................................................... 138
5.3.4.1 General...................................................................................................................................... 138
5.3.4.2 Area of Operation.................................................................................................................. 139
5.3.4.3 Procedure Overview.............................................................................................................. 140
5.3.5 Maintenance of a Solidified System............................................................................................. 141
5.4 Further Preventive Measure (Software Signature, Firmware)............................................................. 142
# Table of Contents

## 6 Hardening

6.1 Product-Hardening Tips ................................................................. 145
6.2 PC Hardening ............................................................................... 145
6.2.1 General ................................................................................ 145
6.2.2 Summary of Measures for Hardening the System .................... 145
6.3 Remote Access .................................................................... 146
6.3.1 Product Side VPN ................................................................. 146
6.3.2 VPN Solution for Remote Access ........................................ 147
6.3.3 Configuration Example .......................................................... 147
6.3.3.1 SCALANCE S with Softnet Security Client ......................... 147
6.3.3.2 Site2Site VPN ................................................................. 148
6.3.3.3 Windows Remote Desktop Solution .................................... 149
6.4 Patch Management .................................................................. 150
6.4.1 General Instruction ............................................................... 150
6.5 WSUS Offline ........................................................................ 151
6.5.1 Scope/Overview ................................................................. 151
6.5.2 Objectives ......................................................................... 151
6.5.3 Download ........................................................................ 152
6.5.4 Installation ....................................................................... 152
6.5.5 Restrictions ....................................................................... 152
6.5.6 Procedure ........................................................................ 152
6.5.6.1 Overview ..................................................................... 152
6.5.6.2 Overview of the Siemens Workflow .................................. 153
6.5.6.3 Download and Install WSUS Offline Update ...................... 153
6.5.6.4 Store or Copy Stored WOU Exclude Lists ....................... 153
6.5.6.5 Create Download Link Files ........................................... 154
6.5.6.6 Download ..................................................................... 154
6.5.6.7 Distribution .................................................................. 156
6.5.6.8 Installation .................................................................... 156
6.5.6.9 Delivery/Update ExcludeList ........................................... 157
6.5.6.10 Create Siemens WSUS Offline Update Configuration Packages .................................................................................. 157
6.5.6.11 Overview of the Customer Workflow ............................... 159
6.5.6.12 Download and Install Siemens WSUS Offline Update Configuration Package ................................................................. 159

## A Appendix

A.1 Abbreviations ...................................................................... 165

## B List of Required Open Ports

B.1 SICAM PAS/PQS, SICAM SCC .................................................. 167
B.2 SICAM A8000 Series, Toolbox .................................................. 170
B.3 SIGUARD PDP ..................................................................... 171
B.4 SIPROTEC 5 / DIGSI 5 ............................................................... 172
B.5 SIPROTEC 4 / DIGSI 4 ............................................................... 173
B.6 CrossBow ............................................................................. 173

## Literature

........................................................................................................... 175
1 Introduction

1.1 Scope/Overview 10
1.2 Principles 10
1.1 Scope/Overview

Many of the actual computer systems – servers, PCs, and automation devices – are highly interconnected. This exposes entire networks to security threats such as hacking, malware, worms, and viruses. In addition, the increased use of common software and operating systems, for example, Windows® and Linux, and standard communication protocols such as TCP/IP-based protocols, have also raised vulnerability.

To thwart attacks and ensure system viability, cyber security must be an integral part of the network planning and design process. Planning for security at the outset provides for a more complete and cost-effective system. Advance planning also ensures that security features are supportable – attempting to retrofit secure measures into existing environments is often ineffective and cost-prohibitive. Security must be addressed at all levels of the development process.

This document provides guidelines for designing secure automation systems that employ the Siemens Energy Automation products. The guide is intended for use throughout the product lifecycle and is updated whenever major changes are made to the described products.

1.2 Principles

Targeted protection is not possible against every current or future threat or method of attack from the inside or outside.

With that said, this security concept deals with general defense strategies designed to protect against the following threats:

• Denial of service
• Circumvention of specific security mechanisms, such as Man in the middle
• Intentional maloperation through permitted actions, such as password theft
• Maloperation through non-configured access rights
• Data spying, for example, of recipes and business secrets or operational plans for plants and their security mechanisms
• Manipulation of data, for example, to downplay the importance of alarms
• Deletion of data, for example, log files to cover up attack activities

The following defense strategies serve as an overall approach to supplement the required:

• Defense in dept
• Appropriate network-topology design
• Least privilege principle
• Malware prevention/protection
## Network Security

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Principles of a Secure Substation Configuration</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>Network Segmentation</td>
<td>12</td>
</tr>
<tr>
<td>2.3</td>
<td>Recommendations</td>
<td>13</td>
</tr>
<tr>
<td>2.4</td>
<td>VPN</td>
<td>13</td>
</tr>
<tr>
<td>2.5</td>
<td>Firewall</td>
<td>59</td>
</tr>
<tr>
<td>2.6</td>
<td>Parallel Redundancy Protocol (PRP)</td>
<td>61</td>
</tr>
<tr>
<td>2.7</td>
<td>Secure Communication with the IEC 60870-5-104 Protocol</td>
<td>62</td>
</tr>
</tbody>
</table>
### 2.1 Principles of a Secure Substation Configuration

In the following chapters, several security measures will be described to support your implementing for the communication network of a substation automation system together with Siemens Energy Automation products. The compatibility of these cited measures, used network topologies, security products, or power-system components with communication protocols used in this environment has been proved.

It is crucial to implement security measures fitting the actual needs of a specific plant. To achieve this, a threat analysis considering the targets and impacts of security attacks on a plant is necessary starting with the planning phase of a plant.

Siemens recommends checking this analysis regularly and adapting it if the threat conditions change. Setting up a secure substation configuration follows a few principles. The first and easiest one is the network segmentation as described in the next chapter. To avoid an incident or limit the damage of an incident that already happened, the secure substation has to be set up as an environment where the communication possibilities are as restricted as possible. To reach that goal, the network borders must be secured using firewalls. Furthermore, the communication between the network segments must be secured, for example, with a virtual private network (VPN).

The correct configuration of a firewall and a VPN is as important as the firewall and the VPN themselves. A firewall must be configured with a default drop rule where every packet that is not explicitly allowed will be dropped. This default rule must be active for packets coming from the directly connected network but also coming from the VPN tunnel. After that, only dedicated and known communication relations have to be allowed. This can be done with the IP address of the source and the destination and the protocols port used in that specific communication relation.

It would be easier to have one VPN group for all participants but that is against the strategy of network segmentation because a VPN connects networks on IP layer. Therefore, every communication relation needs a VPN group. Of course, one VPN group is enough for more than one communication relation, which are using the same VPN gateways.

Another important principle is the monitoring of your network. To identify attacks or suspicious irregularities, it is important to have a central logging server collecting critical information from all involved components of the secure substation like dropped packets of a firewall or error entries in a Windows event log system.

### 2.2 Network Segmentation

Since no security measure provides 100% security and prevents every security incident, the system, including its network topology, must be designed in a way to limit the damage caused by an incident. One possibility is the segmentation of a substation network into subnetworks. This approach should be accompanied by controlling the network traffic across the borders of the subnetworks using Virtual Private Networks (VPN) and firewall technologies.

This chapter describes how a substation network could be segmented into different zones.

#### Description of the Certain Zones

**Process Bus Zone**

This zone contains the SIPROTEC 4 and SIPROTEC 5 devices. A mixed configuration with both optical and electrical network interfaces should be part of the configuration.

**Serial IED Process Zone**

IEDs connected via a serial protocol like IEC 60870-5-101, IEC 60870-5-103, Modbus (ASCII or RTU), or DNP3 are located in the serial IED process zone. For maximum security requested by some customers, the interfaces for configuration are separated from the process-data interface. As the SIPROTEC 4 device has only one Ethernet interface, the serial interface is used for remote configuration. In order to make it accessible via network, an Ethernet hub is used. It must be possible to access the SIPROTEC devices from an engineering PC located outside of the substation.
Remote HMI Access Zone
This zone is reserved for the HMI services. These services are available via Web interface from outside of the substation, like SICAM SCC and SICAM Diamond.

Automation Zone
The SICAM PAS and the local HMI (SICAM SCC) are located in the automation zone. A typical configuration shall be used for this:
- SICAM PAS installed on SICAM Station Unit with Full Server and DIP (option: redundant configuration)
- SICAM SCC installed on regular PC with Windows 7 with latest SP
For the user management, the SIMATIC Logon component shall be used in order to implement a centralized user management for HMI. This Logon component is part of SIMATIC WinCC V7.0.
- Syslog collection

Installation on the PC boxes:
- Updated operating system incl. all available patches and hotfixes
- Latest version of Siemens products
- Installed antivirus software
- All boxes have to be members of an Active Directory (AD) domain
- Active Directory server has to be used as central computer and user management for Windows
- Applications have to be configured for use of AD users

2.3 Recommendations
This manual describes the configuration without a Domain Controller. For easy computer and user management (creating user accounts, password policies, password changing, etc.), Siemens recommends installing a Microsoft® Domain Controller and grouping the included systems and users in a single domain.
For more information about installation and configuration of Microsoft Domains, see the Microsoft TechNet site:

2.4 VPN

2.4.1 General
A Virtual Private Network (VPN) protects your network transmitted data, granting the integrity and the confidentiality of data. The VPN types are split in two main branches – IPSec-based VPNs and TLS-based VPNs. In general, IPSec connects networks and TLS secures protocols because IPSec runs on network layer and TLS on transport layer according the OSI layer model.
The decision which VPN implementation is to be used depends on the physical environment and operating conditions. You can select between specialized devices, for example, Siemens SCALANCE S, or general purpose implementations like IPSec included in Microsoft systems or strongSwan for Linux/FreeBSD/Mac OS X.
2.4.2 Windows IPSec Implementation

2.4.2.1 General

The IPSec VPN integrated in MS Windows supports several authentication mechanisms suitable for different needs. The pre-shared-key (PSK) authentication described in this document fits most substation environments with a small to medium number of VPN end points. If integration of the VPN in the public key infrastructure (PKI) or Kerberos environment of a company is required, follow the guidelines of the security officer of the company.

Summary:
- IPSec is included among others in Windows 7 and Windows Server 2008
  No third-party software required
- Uses certificate, Kerberos, or PSK authentication
- Runs with many other third-party IPSec solutions

![Diagram of Windows IPSec Configuration](diagram.png)

2.4.2.2 Windows IPSec Configuration

Including the IPSec Snap-In in the Management Console

- Start the Windows management console.
- Select File > Add/Remove Snap-in...
Add IP Security Policy in Management Console

- In the **Select Computer or Domain** dialog, select the option **Local computer**.
Creating Policy and Filters

- A right-click to the IP Security Policies Snap-in shows 2 main tasks, **Create IP Security Policy**... and **Manage IP filter lists and filter actions**....
  With the Wizard, you can create the necessary IPSec Policy and the proper rules and filter actions. You always need both directions for rules and filters as shown in the following.

Filter Actions

- Right-click **IP Security Policies on Local Computer**.
Select Manage IP filter lists and filter actions... to create the necessary filters and Add... a new Filter Action.

Click Manage Filter Actions and Add to create a new filter action.
Add a name for the filter action.
Select **Negotiate security**.
Select **Do not allow unsecured communication**.
Figure 2-9  Dialog Communication with computers

✧ Select **Custom > Next > Edit Properties > OK.**
Figure 2-10  IP Traffic Security

- Select **Negotiate security and Use session key perfect forward secrecy (PFS)**.
Figure 2-11  Properties of the PDP Server/User Interface

- Click **Edit...** to continue with the further setup.
- Select ESP for encryption and data-integrity method. Select SHA1 for integrity and 3DES for encryption. Select the recommended session-key settings.
IP-Filter Lists

- Create a Policy with 2 IP filters: UserInterface2PDPServer and PDPServer2UserIntervace, both using PSK for authentication.
- In Manage IP Filter Lists tab click Add.
Create a name for the IP-Filter List `UserInterface2PDPServer > Add`. 

Figure 2-13  Manage IP Filter Lists
Check Mirrored ...
Select **A specific IP Address or Subnet** in IP Traffic Source.
Configure the Source address.

Figure 2-16  IP-Traffic Source
Figure 2-17   Source address

✧ Select **A specific IP Address or Subnet** in IP Traffic Destination.
Configure the Destination address.
Figure 2-19  Destination address

❖ Select Any for IP Protocol Type > Next > Finish.
IP Security Policies

- Create a Security Policy.
Figure 2-21   IP Security Policy

❖ Create a Security Policy Name.
Figure 2-22  IP Security Policy Name

Request for Secure Communication > Next > Edit Properties.
Figure 2-23   Requests for Secure Communication

✧ Click **Add** in Security Policy Properties > **Next**.
Select the tunnel endpoint in tab **Tunnel Settings**. Fill in the IPv4 tunnel endpoint.
In the **Connection Type** tab, select **LAN > Next**, select **Filter List > Next**, select **Filter Action > Next**.
In the Authentication Methods tab, Preshared Key is set as authentication method.

Select a minimum 10 signs long passphrase with alphanumerical and special characters > **Next > Edit Properties**.
Select the **UserInterface2PDPServer** and click **Edit**.

The dialog Edit Rule Properties opens.

Mark **UserInterface2PDPServer** and click **Edit**.
Figure 2-28  Edit Rule Properties

- Select Engineering/UI system IP or domain name as **Source Address**.
- Select server system IP or domain name as **Destination Address**.
- Select **Any** protocol, **Source Port**, and **Destination Port** to ensure that all traffic is routed through the IPSec secured tunnel.
In the **Tunnel Setting** tab, select the tunnel endpoint. In this first IP Filter list entry, the Destination Address is the tunnel endpoint of Server system.
In the **Connection Type** tab, select LAN.

![Connection Type](image)

**Figure 2-31** IP Connection Type

In the **Authentication Methods** tab, **Preshared Key** is set as authentication method.
Select a minimum 10 signs long passphrase with alphanumerical and special characters.

**NOTE**
This is not a passphrase you have to communicate to users. By establishing a secure way to provide the exported configuration file to all VPN endpoints, for example, encrypted mail, secure storage token, you can avoid having to enter the passphrase manually thus selecting an even more complicated phrase.

Now, you need the IP Filter List in the other direction.

✧ Select PDPServer2UserInterface and click Edit...
The **Edit Rule Properties** dialog appears.

- Select PDPServer2UserInterface and click **Edit**.
Figure 2-34   IPSec Filter List

✧ Select Server system IP or domain name as Source Address.
✧ Select PDP Engineering/UI system IP or domain name as Destination Address.
✧ Select Any protocol, Source Port, and Destination Port to ensure that all traffic is routed through the IPSec secured tunnel.
In the Tunnel Settings tab, select the tunnel endpoint. In this first IP Filter list entry, the Destination Address is the tunnel endpoint of Server system.
✧ In the **Connection Type** tab, select LAN.

![Edit Rule Properties](image)

**Figure 2-37  Connection Type**

✧ In the Authentication Methods tab, Preshared Key is set as authentication method.
Exporting and Assign Policy

For the other system, export the configuration file and, because of passphrase, bring it to the other system via a secure way.

- Import this *.IPSec configuration file also via this snap-in.

After that, the system is updated.

- Activate the Policy on both systems by assigning it.
Now, your complete IP-based traffic between Server and Engineering/UI system is encrypted. You can add additional end points by repeating the steps above, for example, to access multiple servers by one engineering system, or allow multiple engineering systems to access the same server. If you want to check your encrypted connection, use the IP Security Monitoring snap-in.

### 2.4.2.3 IP Security Monitoring

- Select the own server and navigate through the tree to **Quick Mode > Statistics**. Bytes sent in tunnel or bytes received in tunnels are the important values. Tunnel means IPSec tunnel.
The configuration for all involved components and the IP addresses are described in this chapter. Furthermore, the firewall/VPN settings of the Siemens SCALANCE S modules and the Cisco Firewall are described in a detailed way.

2.4.3 IPSec VPN Appliance Siemens SCALANCE S

2.4.3.1 General

The configuration for all involved components and the IP addresses are described in this chapter. Furthermore, the firewall/VPN settings of the Siemens SCALANCE S modules and the Cisco Firewall are described in a detailed way.
2.4.3.2 Siemens SCALANCE S Configuration

General Procedure Setting up a SCALANCE S

The SCALANCE S and the Softnet Security clients get their configurations via the Security Configuration Tool (SCT). First of all, create a project and add the SCALANCE S and Softnet Security clients. For initially loading the configuration to the SCALANCE S, it is important to add the MAC address to each device in the project. The SCT sets the IP address via the configured MAC address on Layer 2 of the OSI reference model. Therefore, the SCT computer must be in the same network segment as the SCALANCE S for initially loading the configuration.

Every SCALANCE S must have a default "drop" rule as described in the next section. For all SCALANCE S, a special "allow" rule is needed. Otherwise, the default "drop" rule has no influence on traffic going through a tunnel.

These 2 special rules can be seen in the following screenshots and have always the same format. The rule with the direction from the tunnel to the internal interface must have the external IP of the SCALANCE S as destination IP. The second rule with the other direction must have this IP as source.

Default Rule

All SCALANCE S modules have a global IP firewall rule with the name "Default-Drop-Rule". This rule must be the last rule in the firewall configuration of each SCALANCE S module. This rule is necessary because all dropped packets must be logged to the syslog server. Furthermore, without this rule, all traffic going through the tunnel would be allowed.
To avoid that every SCALANCE S module can establish a VPN tunnel with another SCALANCE S module, it is necessary to create VPN groups. Only SCALANCE S modules within the same group can establish a VPN tunnel between each other.

<table>
<thead>
<tr>
<th>Name</th>
<th>Authentication</th>
<th>Group membership until</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC-ePO-SICAM</td>
<td>Certificate</td>
<td>5/25/2037</td>
</tr>
<tr>
<td>Leitstelle</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>PAS-PASCC-Diamond</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>DC-EngineeringPC</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>DC-LocalHMI</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>DC-RemoteHMI</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>PAS-SIP4</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>PAS-SerialSwitch</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>Client-Diamond</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>DIGSI-SIP4</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>DIGSI-Toolbox-Hub</td>
<td>Certificate</td>
<td>11/23/2037</td>
</tr>
<tr>
<td>Engineering-1703ACP</td>
<td>Certificate</td>
<td>8/23/2037</td>
</tr>
<tr>
<td>Engineering-1703emic</td>
<td>Certificate</td>
<td>7/27/2037</td>
</tr>
</tbody>
</table>

The naming of the groups is based on the communication partners of a group. The naming of the SCALANCE S modules is based on the abbreviation SEM for “security module” and the number of the module which is shown in <<ref to Figure 8 - Test Configuration>>.

Groups: group members
Control Center: SEM2, SEM8, SEM3
PAS-PASCC-Diamond: SEM4, SEM8
DC-EngineeringPC: Engineering, SEM1
DC-LocalHMI: SEM8, SEM1
DC-RemoteHMI: SEM4, SEM1 PAS-SIP4: SEM7, SEM8
PAS-SerialSwitch: SEM5, SEM8
Client-Diamond: SEM4, Engineering
DIGSI-SIP4: SEM7, Engineering
Syslog Configuration

All SCALANCE S modules must be configured to log all dropped packets coming from the tunnel or external network to the syslog server.

SCALANCE Configurations

IP-Address Overview
### Table 2-2: IP-Services Overview

<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Target Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPC</td>
<td>tcp</td>
<td>*</td>
<td>135</td>
</tr>
<tr>
<td>LSA</td>
<td>tcp</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>LDAP</td>
<td>tcp</td>
<td>*</td>
<td>389</td>
</tr>
<tr>
<td>LDAP2</td>
<td>udp</td>
<td>*</td>
<td>389</td>
</tr>
<tr>
<td>LDAPSSL</td>
<td>tcp</td>
<td>*</td>
<td>636</td>
</tr>
<tr>
<td>LDAPGC</td>
<td>tcp</td>
<td>*</td>
<td>3268</td>
</tr>
<tr>
<td>LDAPGSSSL</td>
<td>tcp</td>
<td>*</td>
<td>3269</td>
</tr>
<tr>
<td>DNS</td>
<td>tcp</td>
<td>*</td>
<td>53</td>
</tr>
<tr>
<td>DNS2</td>
<td>tcp</td>
<td>*</td>
<td>53</td>
</tr>
<tr>
<td>KERBEROS</td>
<td>udp</td>
<td>*</td>
<td>88</td>
</tr>
<tr>
<td>KERBEROS2</td>
<td>udp</td>
<td>*</td>
<td>88</td>
</tr>
<tr>
<td>SMB</td>
<td>tcp</td>
<td>*</td>
<td>445</td>
</tr>
<tr>
<td>IEC104</td>
<td>tcp</td>
<td>*</td>
<td>2404</td>
</tr>
<tr>
<td>PASCSC</td>
<td>tcp</td>
<td>*</td>
<td>10501</td>
</tr>
<tr>
<td>DiamondSer</td>
<td>tcp</td>
<td>*</td>
<td>7912</td>
</tr>
<tr>
<td>IEC61850</td>
<td>tcp</td>
<td>*</td>
<td>102</td>
</tr>
<tr>
<td>SNMP</td>
<td>udp</td>
<td>*</td>
<td>161</td>
</tr>
<tr>
<td>HTTP</td>
<td>tcp</td>
<td>*</td>
<td>80</td>
</tr>
<tr>
<td>UPFDIGSI</td>
<td>udp</td>
<td>*</td>
<td>50000</td>
</tr>
<tr>
<td>NTPtcp</td>
<td>tcp</td>
<td>*</td>
<td>123</td>
</tr>
<tr>
<td>NTPudp</td>
<td>udp</td>
<td>*</td>
<td>123</td>
</tr>
<tr>
<td>OPC</td>
<td>tcp</td>
<td>*</td>
<td>135</td>
</tr>
<tr>
<td>OPCXML</td>
<td>tcp</td>
<td>*</td>
<td>8081</td>
</tr>
<tr>
<td>HTTPS</td>
<td>tcp</td>
<td>*</td>
<td>443</td>
</tr>
<tr>
<td>Modbus</td>
<td>tcp</td>
<td>*</td>
<td>502</td>
</tr>
<tr>
<td>DNP3</td>
<td>tcp</td>
<td>*</td>
<td>20000</td>
</tr>
<tr>
<td>PASDiam</td>
<td>tcp</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Syslog</td>
<td>udp</td>
<td>*</td>
<td>514</td>
</tr>
<tr>
<td>SNMPTrap</td>
<td>udp</td>
<td>*</td>
<td>162</td>
</tr>
</tbody>
</table>

**Network Security**

**2.4 VPN**

---

*SICAM / SIPROTEC, System Hardening, User Guide*

E50417-H8940-C619-A1, Edition 05.2018
<table>
<thead>
<tr>
<th>Name</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Target Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>MoxaCom1</td>
<td>tcp</td>
<td>*</td>
<td>966</td>
</tr>
<tr>
<td>MoxaData1</td>
<td>tcp</td>
<td>*</td>
<td>950</td>
</tr>
<tr>
<td>EthHub</td>
<td>udp</td>
<td>*</td>
<td>3497</td>
</tr>
<tr>
<td>ePOCom</td>
<td>tcp</td>
<td>*</td>
<td>443</td>
</tr>
<tr>
<td>ePOREac</td>
<td>tcp</td>
<td>*</td>
<td>8081</td>
</tr>
<tr>
<td>ePOConsole</td>
<td>tcp</td>
<td>*</td>
<td>8443</td>
</tr>
<tr>
<td>ePOAgtUeb</td>
<td>tcp</td>
<td>*</td>
<td>8082</td>
</tr>
<tr>
<td>ePOServCom</td>
<td>tcp</td>
<td>*</td>
<td>8444</td>
</tr>
<tr>
<td>ePOSichbed</td>
<td>tcp</td>
<td>*</td>
<td>8801</td>
</tr>
<tr>
<td>Toolbox</td>
<td>tcp</td>
<td>*</td>
<td>2001</td>
</tr>
</tbody>
</table>

For Toolbox additional settings have to be done in ‘definition of IP services’ configuration.
SEM 1: SCALANCE to Domain Controller

You can find a description of how to configure a firewall for domains and trusts under the following link:
http://support.microsoft.com/kb/179442

SEM 3: SCALANCE to SICAM 230
SEM 4: SCALANCE to Remote HMI PC

Before starting the test, the port to NPORT switch has to be identified and written in the rules.

SEM 5: SCALANCE to Serial Zone

Before starting the test, the port to NPORT switch has to be identified and written in the rules.

SEM 6: SCALANCE to Remote Serial Zone

Before starting the test, the port to NPORT switch has to be identified and written in the rules.
SEM 7: SCALANCE to Domain Controller

![SEM7 FW Config](image1)

Select whether NTP is communicating over UDP or TCP.

SEM 8: SCALANCE to Automation Zone

![SEM8 FW Config](image2)

Firewall

2.5 Firewall

2.5.1 Host-Based Firewalling

According to the Defense-In-Depth strategy, Siemens recommends enabling also the host-based included firewall functionality.

- In Windows, open your Firewall configuration, **Change settings** and activate the Firewall.
Add a Server Port for accepting incoming connections if necessary. For example, if the Server acts as NTP server, accept incoming connections also on UDP Port 123.
Besides the “network core” service, you can also need:

- The Exception for File and Printer Service (Port 139 / 445) for shared folders on Server or Network Discovery if desired.

### 2.5.2 SCALANCE S Firewall Functionality

Besides the IPSec VPN, the SCALANCE S provides firewall functionality to restrict communication tunneled through the VPN.

To allow certain connections, specify the client, the server IP, and the protocols to be tunneled. All other connection attempts are blocked and discarded by the "Default-Drop-Rule". See also chapter 2.4.3.2 Siemens SCALANCE S Configuration.

### 2.6 Parallel Redundancy Protocol (PRP)

One method increasing availability of a system is the implementation of redundancy. The implementation of redundant communication paths is an appropriate approach for substation networks.

The Parallel Redundancy Protocol (PRP) is one of the standards for a bumpless redundancy. The following figure provides information that must be considered in a PRP network. PRP is based on layer 2 (L2) of the OSI reference model and is not suitable for layer 3 (L3) routed networks. Therefore, the SCALANCES have to be
configured as layer-2 bridged mode devices not as layer-3 routed devices as used in secure substation configuration. In a secure substation configuration environment, the components using PRP as a matter of principle are in one zone, that means, in one subnet. Because of that fact, depending on the components using PRP, the secure substation configuration has to be adapted.

### Figure 2-61
Parallel Redundancy Protocol (PRP)

<table>
<thead>
<tr>
<th>2.7</th>
<th>Secure Communication with the IEC 60870-5-104 Protocol</th>
</tr>
</thead>
</table>

#### 2.7.1 Fulfilling the IEC 62351-3

The scope of the IEC 62351 standards is information security for power system control operations.
IEC 62351-3 specifies how to provide the following for SCADA and telecontrol protocols that use TCP/IP as a message transport layer:

- Confidentiality
- Tamper detection
- Message level authentication

IEC 62351-3 specifies how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) (defined in RFC 5246 for TLS 1.2) so that they are applicable to the telecontrol environment of IEC TC57.

As recommended in the IEC 62351 standard, this solution also uses the following:

- X.509 certificates
- A Certifying Authority environment
- TLS authentication and encryption

SICAM PAS has an IEC 62351-3/-5 and IEC 60870-5-7 conform implementation via Security Add-on package for the TCP protocols DNP3 and IEC 60870-5-104. The SICAM 230 as a legacy product as also older versions of SICAM SCC are extensible to support also IEC 62351-3 for IEC 60870-5-104.
In general, the IEC 60870-5-104 protocol is a plaintext protocol. If not secured, you can read and change any communication between the control center like SICAM SCC or SICAM 230 and the Substation automation system like SICAM PAS. If you want to communicate over an open network or over security perimeter zones, Siemens recommends protecting the communication with encryption and authentication of the transmitted data as requested in IEC 62351-3.

For single protocol encryption and authentication, the best selection is a firewall-friendly TLS implementation as also required according IEC62351-3. This selection also presents the advantage that you do not need to change your communication protocol because it is placed in the presentation layer (layer 6) of the OSI reference model below the application layer (layer 7).
Your application does not always support TLS, but you can add a third-party encryption module, for example, the Open Source Software stunnel to secure your protocol. You can find more information on stunnel in chapter 2.7.6.2 Stunnel.

You can also easily create your own key material. You can find more information thereon in chapter 2.7.4 Creating Key Material. As TLS is an RFC standard, many products are compatible. This chapter describes the secured communication between SICAM PAS with the security add-on module and the SICAM SCC and SICAM 230 with the third-party stunnel empowered add-on.

For the SICAM PAS security add-on installation and configuration, read the SICAM PAS manual.

For creating key material and empowering the SICAM SCC and SICAM 230 for security, read this manual.

2.7.3 Preconditions

Install your SICAM SCC or SICAM 230 and SICAM PAS as usual.
Configure the SICAM PAS as IEC60870-5-104 Slave listening on TCP port 2404.
Try netstat –na in a command shell to check if the SICAM PAS is listening on this port.
Configure the SICAM SCC or SICAM 230 as IEC60870-5-104 Master.
The master makes the TCP connect to the slave. You can check it also with netstat –na on both systems as soon as the connection is established.

NOTE
The TCP connection is established from the Master to the Slave.
Make sure that your firewall system is right configured. The TCP connection from the SICAM SCC or SICAM 230 to the SICAM PAS must be allowed. Create such a rule in your firewalls if firewalls are used in your system.

If this configuration runs well, you can switch to the security configuration. As a particularity, the SICAM PAS uses the same port for the TLS encryption communication as for the plaintext communication before. That means, no new firewall rules and firewall adjustments are necessary in general. (Please note other systems can have another behavior because according IEC60870-5-7 TCP port 19998 has to be used for the secured connection)

2.7.4 Creating Key Material

For a secure TLS communication, it is essential to have a mutual authentication between the communication partners. For TLS in general, X.509 certificates are used.
You have different options to get these certificates:
• You can get these certificates from an external PKI as Symantec.
• You can get these certificates from your internal PKI.
• You can create own certificates with the Open Source Software tool OpenSSL.

Certificates
Certificates are a set of keys and information.
You need the following keys:
• Private key
  The pure key is in general an RSA key with a length of 1024 bits (for legacy usage) or better of 2048 bits.
  The private key stays in your access and will be used for signature and decryption.
• Public key
  You need a corresponding public key with the same length.
  The public key can distribute to the public and will be used for verifying the signature or for encrypting a message or file.
X.509 Certificate

An X.509 certificate is more than the public key. The X.509 certificate includes, besides others, the following data:

- Public key
- Information about the issuer
- Subject
- Validity
- Certificate signature of the Certifying Authority (CA)

This means that the public key with all the additional information is signed by a CA private key to verify the authenticity of the public key and information by the communication partner in a later step.

You can find more information on creating a CA, a private key, a public key, and a certificate with OpenSSL in the following chapters.

TLS Function

In the following, you can find a simplified description of the handshake process.

For more information, refer to the RFC5246 "The Transport Layer Security (TLS) Protocol" in chapter 2.7.6.3 SICAM 230 Configuration for stunnel.

Both communication partners own their certificate, their private key, and the CA certificate. Starting the communication means starting also the TLS handshake. The first partner sends his certificate to the communication partner. The second partner gets the certificate and can verify the certificate at first with the CA certificate. Now, the second partner knows that the certificate of the first partner is not modified and comes from a trusted CA. This means that the second partner can trust the certificate of the first partner and, hence, the second partner can trust the first partner.

Now, the second partner checks, for example, the validity or if the certificate is placed on a black list etc. if he wants to know to accept the certificate (adjusted by policies etc. This document does not treat certificate handling in such a detailed way). After that, the second partner sends his certificate to the first partner and this partner performs the same checks.

Now both partners know and trust each other. Additionally, both partners have the public key of the other partner to encrypt messages or files. In TLS, the encryption of all TCP packages with this RSA key (called asymmetrical keys) would be too slow. Therefore, one partner creates a symmetrical key, for example, AES, for encryption and sends the key encrypted with the public key of the other partner to the other partner. The other partner can now decrypt the symmetrical key with his private key. In this way, both partners have the same symmetrical key for encryption and decryption of messages. Things like renegotiation, resumption or Diffie-Hellman key-exchange mechanisms improve the performance and security of a TLS connection as readable in the corresponding RFCs.

In the following chapters, you will find a description of how to create useful X.509 key material.

2.7.5 Building Your Own PKI (Public Key Infrastructure)

2.7.5.1 Preparation of OpenSSL and Easy-RSA-PKI Scripts

Most Secure Way

Download the OpenSSL from the OpenSSL Internet site http://www.openssl.org and build the executable as illustrated in the download package. You can build the executable with a cygwin environment or Visual C++, see also the INSTALL.W32 in OpenSSL source package.

Additionally, download the Easy-RSA-Scripts on https://github.com/OpenVPN/easy-rsa-old/tree/master/easy-rsa/Windows

Depending on how you have build your OpenSSL, you need the OpenSSL.exe and additional the files libeay32.dll and ssleay32.dll.
Trust OpenVPN

If you trust the OpenVPN product, you can download the Open Source Software community OpenVPN package with the OpenSSL executable and the Easy-RSA-CA scripts inside on https://openvpn.net/index.php/download/community-downloads.html because OpenSSL offers no binaries on their homepage. Use the newest windows installable to obtain the easy-rsa scripts together with the OpenSSL binaries, download for example, https://swupdate.openvpn.org/community/releases/openvpn-install-2.4.4-I601.exe

Install the basis components together with Certificates Management Scripts.

Copy the OpenSSL binaries and scripts in one folder (called easy-rsa in this document). You will find the OpenSSL binaries inside the <installation-path>\OpenVPN\bin and the scripts inside the <installation-path>\OpenVPN\easy-rsa folder. After that, you can uninstall the OpenVPN package if not needed for other reasons besides creating key material.

Easy-RSA-PKI

In both cases, you should have now at least the following files in your easy-rsa folder. If you are using the GitHub link, the folder contains two additional bat-files. Additionally, create a keys folder in the easy-rsa folder.
Environment Setup

Now, you can set up your environment. To do so, proceed as follows:

Adjust the following settings replacing the default values:

```
vars.bat.sample
```

- `set HOME=d:\easy-rsa` # your path to these files
- `set KEY_CONFIG=openssl-1.0.0.cnf` # file-name of the openssl.cnf configuration file
- `set KEY_DIR=keys` # sub directory of generated keys
- `set KEY_SIZE=2048` # key length, use 1024 for legacy products or low performance systems
- `set KEY_COUNTRY=DE` # your state
- `set KEY_PROVINCE=Bavaria` # your province
- `set KEY_CITY=Nuremberg` # your city
- `set KEY_ORG=Siemens AG` # your company name
- `set KEY_EMAIL@mail@host.domain` # company mail
- `set KEY_CN=PAS` # common name
- `set KEY_OU=EA PRO` # organization unit
set KEY_NAME=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234

All individual things can be adjust later during certificate generation.

Edit also the view information in the OpenSSL configuration:

*OpenSSL-1.0.0.cnf*

**default_days** = 3650    # how long to certify for
**default_crl_days** = 30    # how long before next CRL (only important for CRL usage)
**default_md** = sha256   # signature algorithm, change to SHA256, do not use MD5/SHA1

For **default_days**, Siemens recommends a maximum of 10 years.

Comment out the name extension:

# name = optional
# name = Name

**NOTE**

If you need another validity, change your **default_days** in the OpenSSL-1.0.0.cnf, for example, 10 years for CA certificate and 3 years for client-server certificates.

After the expiry of the certificate validity, no new connection will be established. Change your key material in time.

**build-key-pkcs12.bat**

- Copy build-key-pkcs12.bat to build-key-pkcs12-server.bat.
- Open the build-key-pkcs12-server.bat file and add “-extensions server” to the command line as follows:
  - Change the line
    ```
    openssl ca -days 3650 -out %KEY_DIR%\%1.crt -in %KEY_DIR%\%1.csr -config %KEY_CONFIG%
    ```
  - to
    ```
    openssl ca -days 3650 -out %KEY_DIR%\%1.crt -in %KEY_DIR%\%1.csr -config %KEY_CONFIG% -extensions server
    ```

**2.7.5.2 Usage of Easy-RSA-PKI**

**Initialization**

- Open a command shell.
- Execute init-config.bat.
- Execute vars.bat.
- Execute clean-all.bat.
NOTE

Every time you open the command shell again, you have to execute the vars.bat script to set the variable environment if you have not adjusted your global Windows variable environment (not part of this manual).

Now, you can create your Certifying Authority.

Creating a CA

✧ Execute `build-ca.bat`:

✧ If you open the `ca.crt` in your /keys folder with Windows, you will find all certificate information now:
Creating Server Key Material

Now, you can create your Server key material as follows:

- Execute `build-key-pkcs12-server.bat <Name of certificate file>`:
Enter Export Password: <insert a free password for PKCS11 container encryption>

Verifying - Enter Export Password

NOTE

Entering a password is mandatory because of a SICAM PAS behavior for importing the key material.

Now, you have created a key-pair (a public and a private key), entered additional information, and signed the request (CSR – Certificate Signing Request) with the CA private key.

The last step was to put all certificates (the PAS Server and CA certificate) and the private key in a container, called also PKCS#12 (P12-) container closed with a PIN (here called Export Password).

NOTE

If you use OpenSSL to can have a look in the container with the following command line:

OpenSSL pkcs12 -info -in keys\PAServer.p12

Use the selected Export Password.
Creating Client Key Material

Now, you can create your Client key material, for example, for stunnel. In this example both mechanisms are introduced, the first one using three single files (key-file, cert-file, ca-cer-file) and second one using a p12 container as mentioned before.

As the Client system is also a server, you can decide if the private key is encrypted or not. If you want an encrypted key, remove the parameter –nodes from build-key.bat or use build-key-pass.bat. For the usage with stunnel, in this example, three single files are used and not the P12 container, that is, a private-key file, a certificate file for the Client, and the certificate file for the CA are used.

Now, you can create your Client key pair for control center.

 Execute build-key SICAM230:

```
E:\easy-rsa>build-key SICAM230
Generating a 2048 bit RSA private key
..........................................................***
writing new private key to 'keys\SICAM230.key'

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter ‘,’ the field will be left blank.

Country Name [2 letter code] [DE]:
State or Province Name [full name] [Bavaria]:
Locality Name [eg, city] [Nuremberg]:
Organization Name [eg, company] [Siemens AG]:
Organizational Unit Name [eg, section] [EM DG PRO]:
Common Name [eg, your name or your server’s hostname] [PAS]:SICAM230
Email Address [email@siemens.com]:Admin.Sicam230@siemens.com

Please enter the following 'extra' attributes to be sent with your certificate request
A challenge password [I]:
An optional company name [I]:
WARNING: can’t open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE: ‘DE’
stateOrProvinceName :PRINTABLE: ‘Bavaria’
localityName :PRINTABLE: ‘Nuremberg’
organizationName :PRINTABLE: ‘Siemens AG’
organizationalUnitName :PRINTABLE: ‘EM DG PRO’
commonName :PRINTABLE: ‘SICAM230’
emailAddress :IA5STRING: ‘Admin.Sicam230@siemens.com’
Certificate is to be certified until Jun 26 14:57:16 2022 GMT (3650 days)
Sign the certificate? [y/n/y]:
1 out of 1 certificate requests certified, commit? [y/n/y]:
Write out database with 1 new entries
Database Updated
```

Or with a password input
By the way, the PEM format is an ASCII file.

Open it ...

If your private key is encrypted you will see it:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIICxjBABgkqhkiG9w0BBQowMzAIBgkqhkiG9w0BBQowDgkJPlPevb/6lqAcsCAggAM
MBQGCCqGSIb3DQMBBAGg0BcYxfWbd4q5 ...
-----END ENCRYPTED PRIVATE KEY-----
```

If the private key is not encrypted, you will also see it:

```
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAMAwIBAgIJAQggIwCw+DQYJKoZIhvcNAQEF
x1gcQHDKIYb/pnQ...
-----END PRIVATE KEY-----
```

Now, you have a key material for the Client and Server.

**NOTE**

In general, the Client starts the TLS connection to a TLS Server, listening on a Server-Port. The Client certificate can act for **Client Authentication**, the Server certificate can act for **Server Authentication**.
Network Security

2.7 Secure Communication with the IEC 60870-5-104 Protocol

Figure 2-71  Certificate Details
Transport, for example, the SICAM230.key, SICAM230.crt, and ca.crt in a secure way to your control center and the PASServer.p12 container and the ca.crt to the PAS.

**NOTE**

Though the CA certificate is part of the container, you have to import the ca.crt separately.

**NOTE**

You have many options with OpenSSL, the CA with a password, the key material in another format, or OpenSSL for file encryption or X.509 certificates for S/MIME e-mail encryption. Use it if you want, OpenSSL is a well supported tool with a large propagation in industry and private usage.
Securing Your Easy-RSA-PKI Generated Keys

As mentioned in chapter Creating Client Key Material, Page 73, you have to transfer the key material in a secure way to your devices.

Siemens recommends avoiding the transfer of the critical key material via your unsecure network. Siemens recommends transferring the key via another medium, for example, via an USB stick. Additionally, you can use an encrypted USB stick for transporting the keys. Use for example VeraCrypt https://www.veracrypt.fr/en/Home.html for encryption and a very long password. If you have trusty persons in your organization, you can also encrypt the packed keys with OpenSSL to send the keys via the network and use a very long password transmitted via phone or Fax (a real Fax, not via IP network).

- Encrypt packed key-archive with an AES256bit symmetrical key:
  
  openssl enc -aes256 -e -in <plain_archive> -out <encrypted_archive> openssl -k <passphrase>

- Decrypt:
  
  openssl enc -aes256 -d -in <encrypted_archive> -out <plain_archive> -k <passphrase>

Securing and Backing Up Your PKI Environment and Keys

It is a good idea to run your PKI on an offline notebook. If you have an old slow notebook, use it only as a Certifying Authority. Store the notebook in a safe. With the Easy-RSA.PKI, it is easy to make a backup.

- Store all files and folder mentioned in chapter Easy-RSA-PKI, Page 67 to a USB stick.
- Place the USB stick in another safe.
- If other persons have access to the safe, encrypt your notebook and USB stick, for example, with VeraCrypt: https://www.veracrypt.fr/en/Downloads.html

NOTE

Only the responsible security persons get the PIN for USB stick and the notebook. Store the password at a secure place, paper is a good option.

NOTE

Every time you create keys, you have to store the files and folder to the backup USB stick again.

2.7.6 Securing Application with Stunnel

2.7.6.1 General

If your application does not support TLS encryption, you can add this feature to your application without modification of your application using the Open Source Software stunnel. You only need to modify your IP target to localhost.

NOTE

stunnel is based on OpenSSL, supports TCP-based applications and supports also SOCKS if useful (see wiki for more information about SOCKS: http://en.wikipedia.org/wiki/SOCKS). Stunnel is not included in the TCP stack and you have to modify your application for target localhost if not supporting SOCKS.

Function

- Install stunnel on control-center site, together with the SICAM SCC or SICAM 230 software.
- Set up stunnel and listen on 127.0.0.1:2404 for SICAM SCC, SICAM 230 incoming IEC60870-5-104 connection.
- Set up stunnel to connect to the secured PAS on Port 2404.
Local application > connect local via TCP to stunnel listen on e.g. IP 127.0.0.1 Port 2404 > stunnel connect to server, listen on regular secured server port, understanding TLS, e.g. IP 192.168.3.16 Port 2404
If the application establishes a connection, the TCP packet is sent to stunnel. Stunnel starts the TLS handshake with the counterpart. If the handshake is completed, the application package is encrypted and transmitted to the counterpart.

Figure 2-73  Securing Application with Stunnel
2.7.6.2 Stunnel

Installation


**NOTE**

stunnel is an Open Source Software and distributed under the GPLv2 or later version. Using stunnel causes no Copyleft effect, that means, your tunneled application is not handled like a derivate work. See also the copyright information of stunnel https://www.stunnel.org/sdf_copying.html.

- Execute the setup and agree to the license conditions:

![Stunnel Setup](image)

**Figure 2-74 Stunnel Setup**

- Install for anyone
Deselect the Tools and install
Figure 2-76  Stunnel Setup
Click Close to finish the installation.

In the windows menu, you can install stunnel as a Windows service. This is recommended for securing the key material.
To configure the stunnel.conf, proceed as follows:

- Save your key material in a preferred folder.
  - You have all Microsoft possibilities to protect the access to the key material. An easy way to protect the copy and the visibility of the key file is to install stunnel as a service and give only the "System" user the read access to the key file.
  - In this example, the files are stored in D:\stunnelkeys.

- Open the stunnel.conf
2.7 Secure Communication with the IEC 60870-5-104 Protocol

- Insert following entries:
  ```
  [secure104]
  client = yes
  accept = 127.0.0.1:2404
  connect = <target-IP for the PAS>:2404
  cert = D:\stunnelkeys\SICAMSCC.crt
  key = D:\stunnelkeys\SICAMSCC.key
  CAFile = D:\stunnelkeys\ca.crt
  verifyChain = yes
  ```

  if you want or need logging, set debug to 7 and enable this parameter: debug = 7

---

**NOTE**

The SICAM PAS uses the TCP Port 2404 for secured and unsecured 104 connection. According IEC60870-5-7 port 19998 have to be used for the secured connection. Using another products can lead to change the port to 19998 for the "connect" parameter

- Disable all other entries with ";" inside the configuration file
- Save the stunnel.conf and start the service and GUI using the menu:

![Stunnel menu](image)

Figure 2-80  Stunnel Users

- Now, you can find a new icon in the notification area:
Have a look at the log file.

Check the log entry via tray icon menu:

![Stunnel Configuration](image1)

![Stunnel Log Entry](image2)

The log file is OK.

Have an additional look by command shell with netstat –na and search for listening on:
Your connection between SICAM SCC and SICAM PAS is now authenticated and encrypted for the IEC60807-5-104 protocol.

Securing Your Key with Windows

In this example, the protected SICAMSCC.key file is stored under D:\stunnelkeys together with the certificates. You can limit the access more and more with an own account etc. However, at first, it should be enough to limit the key access to the “System”.

NOTE

This runs only well if you have installed stunnel as a service because only the system is allowed to have access to the private key.

Adjust your Windows security settings with Administrator rights.

Have a look to the rights:
Figure 2-85  User Rights

- Click **Advanced** and uncheck the Checkbox:
Figure 2-86  Advanced Security Settings

- Click Add

Figure 2-87  Windows Security

- Remove Administrators and Users from the list of allowed users and adjust SYSTEM for Read & Execute and Read only.
Click **Apply**.

Your private key (SICAMSCC.key) is protected against opening, copying, and changing.

**NOTE**

Start your system now with access rights to protect the changeability of the file properties. Be aware that your system service for stunnel is configured with **Automatic start** (default value).

- Additionally, you can change now the logfile because the GUI is not longer usable. Therefore insert a new parameter in the stunnel.conf:
  
  ```
  output = d:\stunnelkeys\stunnel.log
  ```

- Additionally, you can avoid the access to stunnel.exe, remove the access rights for Users to stunnel.exe in the program folder with the Windows mechanisms as described for the private key.
2.7.6.3 SICAM 230 Configuration for stunnel

You have to modify the gw1703.ini file. Proceed as follows:
- Open the SICAM 230 Editor.
- Navigate to your Project > Files > Drivers > STR
- Open the GW1703.ini file.
- Check whether OwN_IP is set correctly to the IP address of SICAM 230 machine.
- Set Mode=CONTROLLING
- Set CON1-LAN*127.0.0.1:2404

Figure 2-89 GW1703.ini – Stunnel Configuration

2.7.6.4 Checking installation

The master SICAM 230 establishes the TCP connection to the slave SICAM PAS. You can check the listening state with netstat –na if the connection is listening and also the connection state if SICAM 230 is connected to the SICAM PAS.

Command shell > netstat –na

Extracted result for port 2404 on SICAM PAS:

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:2404</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.3.16:2404</td>
<td>192.168.7.3:1330</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>
The first line shows that SICAM PAS is listening on all interfaces on TCP Port 2404 (socket 0.0.0.0:2404). The second line shows an established connection from SICAM 230 with IP 192.168.7.3 and TCP port 1330 to SICAM PAS with IP 192.168.3.16 and TCP Port 2404.

### 2.7.7 Securing SICAM PAS

#### 2.7.7.1 Installation and Configuration

The application SICAM PAS Secure Communication Add-on V7.01 must be installed on the machine where SICAM PAS UI Configuration is parameterized. To do so, proceed as follows:

- Double-click **Siemens_SICAM_PAS_SecureCommunication_Addon.msi**.
- Enable the add-on in the Feature Enabler using the license key included in the scope of delivery.

The following configurations must be done in SICAM PAS UI Configuration:

- Configure an **IEC 60870-5-104 Slave Application**.
- In the created application, configure the **Interface** Sicam 230.
- Create the **Control Center** Sicam 230.
- Create the **List** General interrogation list.

#### 2.7.7.2 Transmission Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Port</td>
<td>2404</td>
</tr>
<tr>
<td>Remote IP address</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>
Security-TLS Encryption

<table>
<thead>
<tr>
<th>TLS activated</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local certificate and private key</td>
<td>PASServer This certificate has to be generated and then added to the Templates Certificate Store, see also 2.5 Firewall.</td>
</tr>
<tr>
<td>Client authentication activated</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Figure 2-91 SICAM 230, SICAM PAS Configuration

Importing Your SICAM PAS Key Material

- Navigate to Templates > Certificate Stores > Certificate Store and double-click Certificate Store.
- Click Add and select the already generated PKCS#12 Certificate File (see chapter Creating Server Key Material, Page 71), for example, PASServer.p12.
- Enter the password for PKCS11 container encryption (see chapter Creating Server Key Material, Page 71) and confirm with OK.

Importing the CA Certificate

- Navigate to Templates > Certificate Stores > Certificate Authority Store and double-click Certificate Authority Store.
- Click Add, select the already generated Certificate File, for example, ca.crt and confirm with OK.
Checking installation

The master SICAM 230 establishes the TCP connection to the slave SICAM PAS. You can check the listening state with `netstat -na` if the connection is listening and also the connection state if SICAM 230 is connected to the SICAM PAS.

Command shell > netstat -na

Extracted result for port 2404 on SICAM PAS:

<table>
<thead>
<tr>
<th>Proto</th>
<th>Local Address</th>
<th>Foreign Address</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>0.0.0.0:2404</td>
<td>0.0.0.0:0</td>
<td>LISTENING</td>
</tr>
<tr>
<td>TCP</td>
<td>192.168.3.16:2404</td>
<td>192.168.7.3:1330</td>
<td>ESTABLISHED</td>
</tr>
</tbody>
</table>

The first line shows that SICAM PAS is listening on all interfaces on TCP Port 2404 (socket 0.0.0.0:2404). The second line shows an established connection from SICAM 230 with IP 192.168.7.3 and TCP port 1330 to SICAM PAS with IP 192.168.3.16 and TCP Port 2404.
2.7.8 Additional information

2.7.8.1 Firewalling

**NOTE**
Ensure that your firewall system is well configured. The TCP connection from the SICAM 230 has to be allowed to the SICAM PAS.

The Siemens SCALANCE S configuration is shown as an example:

<table>
<thead>
<tr>
<th>Action</th>
<th>From</th>
<th>To</th>
<th>Source IP addr.</th>
<th>Destination IP</th>
<th>Service</th>
<th>Bandwidth (Mbps)</th>
<th>Logging</th>
<th>No.</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Tunnel</td>
<td>Internal</td>
<td>192.168.3.16</td>
<td>192.168.7.3</td>
<td>IEC104</td>
<td>IP-R_1</td>
<td></td>
<td></td>
<td>To SICAM 230 from PAS</td>
</tr>
<tr>
<td>Allow</td>
<td>Internal</td>
<td>Tunnel</td>
<td>192.168.7.3</td>
<td>192.168.3.16</td>
<td>IEC104</td>
<td>IP-R_2</td>
<td></td>
<td></td>
<td>To PAS from SICAM 230</td>
</tr>
</tbody>
</table>

Figure 2-93 SICAM 230 – Firewall

Using More than One SICAM PAS

**General**
In general, you want to address more than one SICAM PAS with your SICAM 230 or SICAM SCC. As the connection from SICAM 230 or SICAM SCC to the SICAM PAS is not direct and only a local connection is established from SICAM 230 to stunnel, you have to find a way to map the local connections to the real SICAM connections.

To do so, you have 2 possibilities:
- Use different ports for a IEC60870-5-104 connection on the SICAM 230 or SICAM SCC system.
- Use the Microsoft Loopback Adapter to use more than one additional virtual address on the SICAM 230 system.

Both possibilities are described in the following chapters. The Loopback Adapter solution is the standard on your system because it uses always TCP port 2404. The easier way to configure maybe is the different port solution. Select your favorite.

Using Different IEC60870-5-104 Ports on SICAM 230

In general, the IEC60870-5-104 protocol is using TCP Port 2404, but SICAM 230 also supports ports differing from 2404. Use one TCP port for one SICAM PAS you want to address.

Adjust your stunnel.conf in the following way:

- `[secure104_PAS_01]`
  client = yes
  accept = 127.0.0.1:2404
  connect = 192.168.3.16:2404

- `[secure104_PAS_02]`
  client = yes
  accept = 127.0.0.1:2405
  connect = 192.168.3.17:2404
Using Microsoft Loopback Adapter

One way to address more than one local listening socket on the same port is to install a Microsoft Loopback Adapter via the **Add Hardware** menu item in the **Control panel**.


Configure your Loopback Adapter with the same number of IP addresses you have to support also for SICAM PAS.

**NOTE**

Use another Subnet for the Loopback IP address range as for your real network interface address. See also: [http://en.wikipedia.org/wiki/Subnetwork](http://en.wikipedia.org/wiki/Subnetwork).
2.7 Secure Communication with the IEC 60870-5-104 Protocol

Figure 2-96   Loopback Adapter
Change your stunnel settings corresponding to your selected IPs:

- **[secure104_PAS_01]**
  - client = yes
  - accept = 192.168.1.1:2404
  - connect = 192.168.3.16:2404

- **[secure104_PAS_02]**
  - client = yes
  - accept = 192.168.1.2:2404
  - connect = 192.168.3.17:2404

- Configure your SICAM 230 to the Loopback addresses.
  If you want connect to SICAM PAS 01 with IP 192.168.3.16, configure the SICAM 230 with connection to IP 192.168.1.1. Maintain an Excel mapping sheet.

The following figure shows a complete connection way.
Figure 2-98  Using Loopback Adapter
3 User Management

3.1 Least Privilege
3.1 Least Privilege

Restricting the Access to the System

Create a special Windows user group for the installed program. Only users that belong to this group should be allowed to start the program and browse to these folders. This user group should have only read access to the program folders, but only if absolutely necessary. Normal Windows user accounts should not have the rights to start the program or browse to the program folders.

Create only users that are members of the Windows user group and your defined program group.

NOTE

Never use an administrator account for normal computing. This measure grants a high level of security to avoid the infiltration of malware DLL or EXE files.

In many cases, it is recommended to establish a domain concept with proper password rules as a local policy-based user group set.

Restricting the Access to the Computers

The first step towards enhanced security is to block the access to a system. Keeping the computers in a locked computer room subject to access control can significantly reduce the risk of unauthorized intrusion into the network.

Be aware of the following additional points:

• Use only personal user accounts. Do not use accounts shared by several users.

• Set the password directives very restrictively:
  – The minimum password length is 8 characters.
  – The password must include uppercase and lowercase letters, numericals, and special characters.

NOTE

Consider the NERC CIP rules for passwords.
• Passwords must expire after 90 days at the latest.

![Local Security Settings][sc_password_security,1, en_US]

Figure 3-1 Password Security

• Users shall only be granted rights which are absolutely necessary for their tasks. For example, only the administrator is allowed to install software or delete Windows events.

• Activate the password-protected screensaver. Siemens recommends using the standard Windows screensaver.

• If not absolutely necessary for operation, only the administrator shall have the rights required for connecting USB devices.
4 Logging

4.1 General 104
4.2 Logging with Event Viewer - Step by Step Manual for Windows 7 (Local Site) and Windows Server 2008 (Remote Site) 106
4.3 Logging with Syslog 110
4.4 Syslog Client 111
4.5 Syslog Server 112
4.6 CrossBow 117
4.1 General

Most of the security requirement catalogs, like NERC CIP and BDEW White Paper, ask for an implementation of a manual or automatic process for monitoring electronic access to the control system. For that purpose, all products provide at least local logging facilities used for logging of security-relevant events like:

- Failed/successful login
- Logout
- Changes in user/password management (user added, deleted, modified,..)
- Software/firmware updates

Additional central logging is required for an easy overview and a fast response. For large systems, it is useful to inspect log files from a centralized point, maybe an administrators workstation. This chapter explains different approaches to implement such a centralized logging.

Central logging with Microsoft included native programs is not so easy. So it is not possible to log all relevant log data to a central Syslog server. For this, you need third-party software, for example, the Datagram Syslog Agent distributed by Datagram Consulting as “Free software” delivered under the GPLv2 license.

http://www.syslogserver.com/syslogagent.html

Windows also supports remote event log access via the included Event viewer. To view the remote log files, you have to observe a few boundary conditions. If you have any troubles, see also the Event Viewer Troubleshooting from Microsoft

(http://technet.microsoft.com/en-us/library/cc738322%28WS.10%29.aspx)
To read the log files, you need administrator rights on the remote machine. This user must also be created on the local machine with the same password. As a security best practice, consider using Run as to perform this procedure. Siemens recommends creating an audit-administrator on the remote and the local machine with administrator rights.

Next, on diverse Windows operating systems, the Remote Registry Service must be started for you to be able to see the Description or Category fields in the property page for an event log.

If the firewall is activated as recommended, open the incoming traffic for remote event logging.

![Windows Firewall Settings](image)

Figure 4-1 Enable Remote Event Log
4.2 Logging with Event Viewer - Step by Step Manual for Windows 7 (Local Site) and Windows Server 2008 (Remote Site)

- Logging with Event Viewer - Step by Step Manual for Windows 7 (Local Site) and Windows Server 2008 (Remote Site)

**NOTE**
For consistence on local and remote site, you always need the same logon and password. For this, a Domain Controller concept is better.

Figure 4-2 Windows 7/2008 User Auditor

- Activate the Remote Event Log Management on remote site.
On local site, start the remote Event Viewer via user interface or command shell.
Now, you are connected to server logs:

After that, you can store log events you want.

✧ Select events you want to store and select the **Save Selected Events...** menu on the right.
Now, you can store the files as .txt or .xml file for further action:
4.3 Logging with Syslog

Normally, Windows programs do not support the syslog protocol. If you have to log to a central Syslog server system, you have to extend the capabilities of the regular Microsoft Windows logging system, which is supported by most applications, to support the standard Syslog protocol. The easiest way is to convert Eventlog messages to syslog messages with a local wrapper. You can use for example the OSS NXLog Community Edition: https://nxlog.co/products/nxlog-community-edition

In concept NXLog is similar to syslog-ng or rsyslog but it is not limited to unix and syslog only. It supports different platforms, log sources and formats so nxlog can be an ideal choice to implement a centralized logging system. It can collect logs from files in various formats, receive logs from the network remotely over UDP, TCP or TLS/SSL on all supported platforms. It supports platform specific sources such as the Windows Eventlog, Linux kernel logs, Android device logs, local syslog etc. Writing and reading logs to/from databases is also supported for many database servers. The collected logs can be stored into files, databases or forwarded to a remote log server using various protocols.
NOTE
You can use NXLog as syslog server and also as a syslog client that is reading the events from the MS event viewer, converting to syslog format and forward to a centralized syslog server. For help see https://nxlog.co/docs/nxlog-ce/nxlog-reference-manual.html

4.4 Syslog Client

The 3rd party Software NXLog in the community version supports the reading of Microsoft event logging and the converting to the syslog format defined in the RFC 5224. Filter can be used as is from the Microsoft event viewer filter in XML format. The converting will be happen automatically but can be also adjusted if necessary. See the NXLog documentation for more information. Enclosed an example for reading the event logging for Windows/Security critical and error

XML output:
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*[System[(Level=1 or Level=2)]]</Select>
  </Query>
</QueryList>

The following example shows the configuration for logging the above shown event log entries stored in a file and transmitted via UDP syslog protocol, both formatted according to RFC 5224.

```xml
<Extension _syslog>
  Module      xm_syslog
</Extension>

<Input in>
  # input from the MS event log
  Module      im_msvistalog
  ReadFromLast True
  # copied from event viewer XML query
  <QueryXML>
    <QueryList>
      <Query Id="0" Path="Security">
        <Select Path="Security">*[System[(Level=1 or Level=2)]]</Select>
      </Query>
    </QueryList>
</Input>
```

## This is a sample configuration file. See the nxlog reference manual https://nxlog.co/docs/nxlog-ce/nxlog-reference-manual.html about the configuration options.

## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
## Running the executable with the -f command line argument will run it in foreground if you don't want to run it as a service.

#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog
define SYSLOGFILE %ROOT%\data\syslog.log

Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log
4.5 Syslog Server

4.5.1 General

First of all, note the following: This is only a short description for installing and using a Syslog server. This chapter shows how you can use a syslog server in your environment. Nevertheless, for large installations, you can buy a syslog appliance or a ready SIEM system (Security Information and Event-Management) with many filter options and nice usability.

Additionally, use the rsyslog wiki for more information: [http://wiki.rsyslog.com/index.php/Main_Page](http://wiki.rsyslog.com/index.php/Main_Page)

4.5.2 Syslog Server with NXLog

As described in the chapter before NXLog can also be used as a syslog server. In this case the NXLog server is listening on the dedicated UDP port as defined in the RFC 5426.

Enclosed an example of a NXLog server listening on UDP port 514 and writing all inputs to a local file. Additional the logfile is rotating and storing the older one:

```plaintext
define ROOT C:\Program Files (x86)\nxlog
define SYSLOGFILE %ROOT%\data\syslog.log
```

```plaintext
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
```
LogFile %ROOT%\data\nxlog.log

<Extension _syslog>
  Module  xm_syslog
</Extension>

<Input in>
  Module  im_udp
  Host    167.87.41.10
  Port    514
</Input>

<Output out>
  Module  om_file
  File    '%SYSLOGFILE%'
</Output>

<Route 1>
  Path  in => out
</Route>

#check the size of the Syslog file periodically (e.g. every hour) and rotate it if it is larger than e.g. 1Mb.
#I.e. 'file' will be moved to ''file'.1''.
#If ''file'.1'' already exists it will be moved to ''file'.2'' and so on,
#until e.g. 5 files reached, then oldest file will be removed.
<Extension fileop>
  Module  xm_fileop

  <Schedule>
    Every 1 hour
    Exec if (file_size('%SYSLOGFILE%') >= 1M) file_cycle('%SYSLOGFILE%', 5);
  </Schedule>
</Extension>

Of course the NXLog can also be used as an intermediate syslog server and can forward the syslog messages additional to an external (central) syslog server.

<Output file>
  Module  om_file
  File    '%SYSLOGFILE%'
</Output>

<Output centralsyslog>
  Module  om_udp
  Host    172.17.17.245
  Port    514
</Output>

<Route 1>
4.5 Syslog Server

4.5.3 Rsyslog with LogAnalyzer

4.5.3.1 Preconditions

- Use a well long-term supported Linux distribution. Use, for example, an Ubuntu LTS operating system. It is not necessary to install a desktop environment.
- Use the rsyslog package.
- Use LogAnalyzer for a graphical Syslog display and analysis. LogAnalyzer is licensed under the GNU GENERAL PUBLIC LICENSE Version 3 (see copyright file after download).
- You need Apache Webserver and PHP5 for using LogAnalyzer for web-based access to Syslog information.

4.5.3.2 Installation

- First, configure rsyslog daemon for external usage.
  - Change the /etc/rsyslog.conf file.
  - # provides UDP syslog reception
  - $ModLoad imudp
  - $UDPServerRun 514
  Now, rsyslog is listening on UDP Port 514
  - “sudo aptitude install apache2” (Web server)
  - “sudo aptitude install php5” (open source general-purpose scripting language)
  - With the preceding link – we are using the syslog diskfile (/var/log/syslog)
  - Web server needs access to the syslogfile: “usermod –a –G adm www-data”

4.5.3.3 Using LogAnalyzer

- Open your favorite Web browser from any remote system to connect to your Syslog server.
- Open LogAnalyzer via Web link to the rsyslog server to analyze the syslog entries, for example, http://192.168.114.131/index.php.
4.5.3.4 Administration of Syslog Server

As the Syslog server is a Linux server, you can find enclosed a short overview for Windows users:

✧ First, you can use the server via local console for administration.
✧ If you want to use your local HMI windows computer for administration, use PuTTY for Secure-Shell (SSH) access to the Server [http://www.putty.org/](http://www.putty.org/).
✧ If sshd is not installed, use aptitude to install it on server:
  
  ```bash
  sudo aptitude install ssh.
  ```
✧ Use PuTTY from the Windows start folder to run PuTTY.
✧ Establish a new connection to the server. You can now log on to the server via ssh as you know it from your console logon.
If you want to copy files from your server to your local HMI Windows computer, use WinSCP to copy files via SSH from your server to the windows system:

   http://winscp.net.

Use WinSCP from the Windows start folder to run WinSCP. Establish a new connection to the server. You can now copy files between the Windows computer and the Linux server.
4.6 CrossBow

4.6.1 General

Siemens RUGGEDCOM CROSSBOW is a proven secure access management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices. The Siemens RUGGEDCOM CROSSBOW solution focuses on delivering productivity gains for administrators and users while achieving full NERC compliance in managing, securing and reporting on remote access. The combination of the CROSSBOW Secure Access Management server and CROSSBOW Station Access Controller for local substation access form an integrated, comprehensive solution with a seamless configuration environment.

The Siemens RUGGEDCOM CROSSBOW application addresses the need for utilities to interactively access remote field IEDs for maintenance, configuration, and data retrieval. Siemens RUGGEDCOM CROSSBOW allows a native IED application to communicate remotely with its associated IEDs, as if the user was connected directly to the IED with a serial cable or network connection. The appropriate authentication model (e.g. RSA SecurID) governs user access and all user activity is logged and reported per the NERC CIP specification.

4.6.2 Customer Benefit

Secure remote access for authenticated users only

- User login activities are logged
- Connections are logged

Integration in a potentially existing centralized user administration, e.g. Microsoft Active Directory Server is possible

- User and password management by only one system only
One System for multiple functions: remote access + password management + configuration monitoring + firmware/software monitoring

- A single alarm system for security violations, e.g. unauthorized firmware updates, configuration changes, and others

IEDs from other vendors are supported as well
- Not only substation automation devices
- Network devices, like routers, gateways, and others are also supported

Supports customer to comply with requirements of NERC/CIP, BDEW White Paper, WIB and other standards
Following Siemens EM DG PRO products are implemented:
- SIPROTEC 4 + DIGSI 4
- SIPROTEC 5 + DIGSI 5
- SICAM PAS PQS
- SICAM SCC

4.6.3 Environment of a CrossBow System

A Crossbow system consists of
- Crossbow Server, Secure Access Manager (SAM)
  It is an application that provides services to communicate with a database allow clients to access information stored within the database, event log distribution as well as receive syslog messages.
- Crossbow Client
  Allows users to connect to IEDs
  Administer Crossbow specifically:
  – Device Configuration
  – User Configuration
  – Access Control Configuration
  – Schedule Activities
  – Reporting
  View Data within the Crossbow Database
  Manipulate Data within the Crossbow Database
  Fully Customizable concerning what non-admin users can view in the Crossbow system
- Crossbow Substation Access Controller (SAC)
  CrossBow Station Access Controller is essentially a CrossBow server with a subset of CrossBow features
  CrossBow SAC maintains a local copy of a subset of the enterprise CrossBow database which contains information related to the devices in the local facility only, as well as any other global (non facility specific) configuration information required by CrossBow.
4.6.4 Installation of a CrossBow System

For installation of CrossBow Server, Client and SAC, please refer to the CrossBow Installation Guide. To use the Crossbow features also for the SICAM PAS and SICAM SCC, you have to install the SICAM Security Management Server software. Please refer to SICAM Security Management Server V1.00, Installation and Configuration Guide.

4.6.5 Configuration of a CrossBow System

4.6.5.1 General

In the following, the configuration of the CrossBow Server and an elementary System configuration of CrossBow is described. The products Siprotec 5, Siprotec 4, SICAM PAS and SICAM SCC are considered.

4.6.5.2 CrossBow Server

The installation finished successfully. Now you can go ahead with the configuration of the CrossBow Server:

- Start > All Programs > RuggedCom > CrossBow Server > CrossBow Server.
- Click the Configure button for the CrossBow Main Server.
In the Primary Configuration tab:
✧ Pick the license file (*.xml) that was provided.
✧ In Server Certificate Configuration click on Browse.
   There you have to import a Certificate Subject (for example ‘CrossBow SAM.p12’) which must be created before by Certificate department. The .p12 file already includes the certificate and the certificate authority. This certificate must be imported to Certificate (local computer) > own certificate. (“Certificate symbol has a key”). After import of .p12 file, you will find the certificate (key symbol) and the certificate authority in the folder of certificates. Move the certificate authority to the ‘Trusted Root Certificate Authorities’ > ‘Certificates’.
✧ Click ‘Choose Trusted Certificate Authorities’ and select the Certificate Authority of which the Certificate (for example “CrossBow SAM) was created.
✧ Fill in ‘Admin’ in Group Name.

In the database tab
✧ Specify the SQL Server (typically “<machine name>”).
✧ Test your connection by clicking the “Test” button. In Connection Status, “Connected” should be written.
✧ Specify the appropriate authentication method, and username/password if using database authentication.

![CrossBow Server Configuration](image)
In the Authentication tab:
- Select 'Basic Authentication'
- Click Ok.
- Click Start for the CrossBow Main Server.
4.6.5.3 CrossBow System Configuration

Login to the CrossBow Client

✧ Start > All Programs > RuggedCom > CrossBow Client > CrossBow Client.
✧ File > Connect to Server.
✧ Confirm the message that a certificate is missing.
✧ In case CB client is installed on SAM machine, select the Certificate “CrossBow CA”.

Otherwise you have to install the certificate authority on client machine:

Proceed:

✧ Open mmc console (start > run > mmc).
✧ File > Add/Remove Snap-in...
✧ Select certificates > add > computer account > Local computer > ok.
✧ Select Certificates (Local computer) > Trusted Root Certification Authorities > Certificates.
✧ Right click on certificates >All Tasks > Import.
✧ Welcome to the Certificate… > next > browse for the certificate (which must be delivered by the customer) > Next.
✧ Place all certificates in the following store > Trusted Root Certification Authorities > Next.
✧ Finish.

Complete the Procedure:

✧ Close the CB certificate window by clicking on ok.
✧ In the connection window of CB client, fill in the IP address of the CB Server, Port 21000 and click connect.
✧ Click on File > Preferences > Choose Trusted Certificate Authorities > mark the certificate you imported before > ok > ok.
✧ Click again File > connect to server > IP address of CB server.
✧ Click Proceed.
✧ Login with the default admin account (admin/Admin).
Create a Device Group

- Click the Devices tab.
- Right-click in the left hand pane, click Add Device Group.
- Specify a name.
- In the Access Privileges tab
  - Ensure the checkbox for the Admin group is checked.
- In the Information Privileges tab
  - Check all the boxes for the Admin group, and set the File Access Level to Full.
- Click Ok.

Add Permissions for the Admin User Group

- In the users tab
  - In the left hand pane, right-click on Admin (the root node) and click Properties.
- In the Special Operation Privileges tab
  - Check the All Ops/All Device Groups box, which will check all the boxes automatically.
In the Cam Privileges tab
- Check the All CAMs/All Device Groups box, which will check all the boxes automatically.

**Create Devices**

On the Field Layout tab
- Right-click on the Global Region node, click Add Facility.
- Specify a name, click Ok.
- Right-click on the facility node, click Add Device (for SIPROTECs), or Add Gateway (for SICAMs).
Figure 4-19  Device Identification

- Specify a name.
- Pick a device/gateway type.

Possible device/gateway types are:
- Generic SIPROTEC 4
- Generic SIPROTEC 5
- Generic SICAM SCC
- Generic SICAM PAS

In the Connection tab
- Specify the device's IP address or network name
Initial the password must be set manually in this menu. Otherwise, the special operation cannot be executed.

In the Interfaces tab

For each of the interfaces, select the device group created above.

In the NERC CIP tab
- Click 'Click to set all to No'
  - For BES Cyber System select "No impact"

In the CAMs tab
- Click the checkboxes to enable the Config Compare CAM and Firmware Version CAM
4.6.6 Elementary Usage of CrossBow concerning EM DG PRO Products

4.6.6.1 Login to CrossBow Client

✧ Start > All Programs > RuggedCom > CrossBow Client > CrossBow Client.
✧ File > Connect to Server.
✧ Specify the host name or IP address and then click Connect.
4.6.6.2 Licenses for CAMs

For the use of the CAMs “Config Compare” and “Firmware Compare” it is necessary to install the corresponding license files.

You can check the active licenses in CrossBow Client > Reports > License Limits.
The license file must be copied in the directory:

- for Config Compare CAM
  C:\Program Files\RuggedCom\CrossBow\ConfigCompareCAMLicense-SiprotecIntegration200Devices.ccl
- for Firmware Version CAM
  C:\Program Files\RuggedCom\CrossBow\FirmwareVersionCAMLicense-SiprotecIntegration200Devices.ccl
4.6.6.3 Execute Special Operations on a Device

Backup Configuration

- Right-click on the device and click on the following menu item:
  Special Operations > Backup Configuration

![Backup Configuration](image)

This will retrieve the configuration from the device and store it in the database.
To see the file, do the following:
- Right-click on the device, click Show Data > Files.

**NOTE**
If the retrieved file matches the latest version of the file, it will not be added again.

Get And Approve Configuration

- Right-click on the device, and click on the following menu item:
  Special Operations > Get And Approve Configuration.

This will retrieve the configuration from the device, store it in the database, and set that version as the Approved version (i.e. the baseline for the Config Compare CAM).
To see the approved version, do the following:
- Right-click on the device, click Show Data > Files.
- Right-click on the file, click View File Versions.

Retrieve Firmware Version

- Right-click on the device, and click on the following menu item:
  Special Operations > Retrieve Firmware Version.

This will retrieve the firmware version from the device and store it in the database.
To see the approved version, do the following:
- Right-click on the device, click Properties.
- The value is displayed in the Identification tab.

Get And Approve Firmware Version

- Right-click on the device, and click one of the following menu items:
  Special Operations > Get And Approve Firmware Version.
This will retrieve the firmware version from the device, store it in the database, and also make it the approved version (i.e. baseline for the Firmware Version CAM).
To see the approved version, do the following:
- Right-click on the device and click the following menu item:
- In the CAMs tab, click Properties for the Firmware Version CAM.
- The value is displayed in the Firmware Version Override field.

Change Password (only for Siprotec 5 Devices)

- Right-click on the SIP5 device, and click one of the following menu item:
  Special Operations > Change Password.
This will change the Admin Password of the SIP5 device. You have the possibility to create a random or a specific password.

![Image of Device Properties](image)

Figure 4-26    SIPROTEC 5 – Admin Login

Initial the password must be set manually in this menu. Otherwise, the special operation cannot be executed.

NOTE

The progress of special operations can be monitored via the Automation tab (Automation menu item).
- Select the item in the top list to see the details for the devices in scope
- Right-click on a failed device in the lower list and click Retry to attempt the operation again.
4.6.6.4 Execute Crossbow Application Modules

Config Compare CAM

Right-click on the device, and click on the following menu item:
CrossBow Application Modules > Config Compare CAM.

This triggers the Backup Config operation to run. Then the latest version of the configuration will be compared against the approved version of the configuration - an alert will be raised if they do not match.

To see the alert, do the following:
Right-click on the device, and click on the following menu item:
Show Data > Alerts
Figure 4-29  Show Data

Figure 4-30  Alerts Overview

**Firmware Version CAM**

- Right-click on the device, and click on the following menu item:
  CrossBow Application Modules > Firmware Version CAM

This triggers the Retrieve Firmware Version operation to run. The device's firmware version will be compared against the approved firmware version - an alert will be raised if they do not match.

- Right-click on the device, and click on the following menu item: Show Data > Alerts
4.6.6.5 CrossBow Debug Logger

To capture the progress/error of the operations, do the following:

✧ Start > All Programs > CrossBow Logger > CrossBow Logger

✧ In the Logger window, check the Input Filter checkbox, and write siemens in the textbox to the right.

When the special operations are executed by CrossBow, this will show you the bits that have been updated and are of relevance to you.
5 Malware Protection/Prevention

5.1 Motivation 136
5.2 Virus scan 136
5.3 Whitelisting, McAfee Whitelisting 136
5.4 Further Preventive Measure (Software Signature, Firmware) 142
5.1 Motivation

There are different kinds of malicious software, so called malware, such as worms, viruses, trojans, and many more. Especially since a lot of products in industrial automation are based on commercial-off-the-shelf operating systems, the threat of malware became more real.

This chapter describes 3 approaches to prevent from malware:
- First of all, the implementation of an traditional virus scan is explained.
- Chapter 6.2 PC Hardening explains the Whitelisting, a method which controls.
- Chapter 6.3 Remote Access describes how to avoid malicious modifications of firmware and software code by use of integrity check based on digitally signed code.

5.2 Virus scan

Virus scanners are available in different variants, as stand-alone products or for commercial environments as client-server-application. Via OfficeScan-Server, the setup packages, configuration, and updated pattern are deployed. The mechanisms are “push” or “pull” to get the information or software to the systems.

![Client-Server-Application](sc_virusscan_1_en_US)

Figure 5-1  Client-Server-Application

5.3 Whitelisting, McAfee Whitelisting

5.3.1 Overview

General

This chapter gives you detailed information about the usage of the McAfee Whitelisting solutions together with the EA products in a secure substation environment.
Furthermore, it describes the procedure to set up a McAfee Whitelisting solution and the handling of such a system after installation. The intention of the following chapter is not the replacement of the McAfee documentation. It should give you a quick overview of that solution and special handlings with the EA products.

McAfee Whitelisting

The name of the McAfee Whitelisting solution is Embedded Control. This solution contains the products Application Control (AC) and Change Control (CC). These 2 products can be managed with an online Web-based solution named ePolicy Orchestrator (ePO), but can also be managed locally with a command-line interface (CLI) without the ePO.

5.3.2 Product Description

Application Control (AC)

Only programs contained in the McAfee dynamic whitelist can be executed. Other programs (exes, dlls, scripts) are considered unauthorized. Their execution is prevented, and the failure is logged by default. This prevents worms, viruses, spyware, and other malware that install themselves from executing illegitimately. The feature “Memory control” ensures that running processes are protected from malicious attempts to hijack them. Unauthorized code injected into a running process is trapped, halted, and logged. This way, attempts to gain control of a system through buffer overflow, heap overflow, stack execution, and similar exploits are rendered ineffective and are logged.

(source: McAfee ds-embedded-control.pdf)

Change Control (CC)

McAfee Embedded Control detects changes in real time. It provides visibility into the sources of change and verifies that changes were deployed onto the correct target systems; provides an audit trail of changes; and allows changes to be made only through authorized means. It allows you to enforce change control processes by specifying the authorized means of making changes. You can control who can apply changes, which certificates are required to allow changes, what can be changed (for example, you can restrict changes to certain files or directories), and when changes can be applied (for example, update windows can only be opened during certain times of the week).

(source: McAfee ds-embedded-control.pdf)

ePolicy Orchestrator (ePO)

ePolicy Orchestrator software is a scalable, extensible management platform that enables centralized policy management and enforcement of your security products and the systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control. Using an ePolicy Orchestrator server, you can:

- Deploy security products, patches, and service packs to the systems in your network.
- Manage the host and network security products deployed to your systems through the enforcement of security policies, client tasks, and server tasks.
- Update the DATs, Engines, and other security content required by your security software to ensure that your managed systems are secure.

(source: McAfee epo_460_product_guide_en-us.pdf)

5.3.3 Offline Solution – AC and CC with CLI

5.3.3.1 General

The Application Control and Change Control product can be installed, configured, and maintained offline. That means that such systems can be set up and maintained locally via command-line interfaces (CLI). The name of this solution is Embedded control.
5.3.3.2 Area of Operation

This solution is suitable for a small number of whitelisted (solidified) systems within an encapsulated network without connection to the outside world.

A disadvantage of this solution could be the maintenance of the solidified systems. This heavily depends on the McAfee mechanism used to update solidified systems.

5.3.3.3 Procedure Overview

Every rectangle in this diagram represents a chapter in this documentation.

5.3.4 Online Solution – AC and CC with ePO

5.3.4.1 General

The Application Control and Change Control product can be installed, configured, and maintained online. That means that such systems can be set up and maintained online via a Web-based management solution named ePolicy Orchestrator (ePO) or Integrity Control.
5.3.4.2 Area of Operation

This solution is suitable for a large number of whitelisted (solidified) systems within a distributed or large network.

A disadvantage of this solution could be the complexity of the ePO because the ePO was developed for managing many McAfee products, not only the Integrity Control feature.

The following figure is an example of an McAfee ePO integration in the environment of a Siemens Energy Automation Secure Substation.

---

Figure 5-3 Area of Operation
5.3.4.3 Procedure Overview

Every rectangle in this diagram represents a chapter in this documentation.
5.3.5 Maintenance of a Solidified System

The installed solidifier prevents the modification of solidified executable and library files. To update a system, the McAfee solution provides several mechanisms to add so-called Installers or Updaters to the system. File changes made by these Updaters are treated as authorized changes.

The following table gives an overview of the mechanisms to add Updaters. These mechanisms describe how a system can be updated with executables and libraries which are not on the whitelist. In some maintenance cases, it could also be necessary to add executables as Updaters which are already on the whitelist.

For each mechanism, Siemens defined security levels from the highest to the lowest security level.

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Mechanism</th>
<th>Short Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH recommended</td>
<td>Signature</td>
<td>Applications can be signed with private RSA (Rivest, Shamir, and Adelman - a form of encryption) key material. Adding the corresponding certificate authorizes the signed application as Updater.</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>Checksum</td>
<td>Applications can be added as Updater with the checksum of the application.</td>
</tr>
<tr>
<td>LOW</td>
<td>Trusted Path</td>
<td>Applications which are stored in a trusted path are authorized Updaters.</td>
</tr>
<tr>
<td>LOW</td>
<td>Trusted Users</td>
<td>Applications which are executed by a trusted user are authorized Updaters.</td>
</tr>
<tr>
<td>LOW</td>
<td>Update Mode</td>
<td>Applications which are executed during the Update Mode can change or add executables and library files. <strong>This mechanism is not recommended!</strong></td>
</tr>
</tbody>
</table>
Another preventive measure for malware protection is the implantation of integrity checks for software and firmware files. Such an approach is used for example in SIPROTEC 5 and SIPROTEC 7SC80. You can find a
description of the used approach in /12/ *SIPROTEC 5 Application Note* and /14/ *SIPROTEC 7SC80 Feeder Automation Controller – Security Guide*.
# Hardening

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Product-Hardening Tips</td>
<td>145</td>
</tr>
<tr>
<td>6.2 PC Hardening</td>
<td>145</td>
</tr>
<tr>
<td>6.3 Remote Access</td>
<td>146</td>
</tr>
<tr>
<td>6.4 Patch Management</td>
<td>150</td>
</tr>
<tr>
<td>6.5 WSUS Offline</td>
<td>151</td>
</tr>
</tbody>
</table>
6.1 Product-Hardening Tips

Hardening a substation automation system starts with activation of security settings of every component of such a system. The Siemens Energy Automation products have a description about product-related hardening. It includes, among others, the following topics:

- Malware prevention
- Appropriate use of role-based access
- Approach to disable unused network ports and services

For product-specific hardening guides, refer to:

- /10/ SICAM PAS PQS Security Manual
- /12/ SIPROTEC 5 Application Note
- /13/ SICAM 230 Hardening Guide
- /14/ SIPROTEC 7SC80 Feeder Automation Controller – Security Guide

6.2 PC Hardening

6.2.1 General

Hardening is usually the overall process of securing the whole IT system to reduce the vulnerability against attacks. Reducing available vectors of attack reduces the vulnerability. The following measures are recommended for hardening your PC boxes.

6.2.2 Summary of Measures for Hardening the System

The following section describes which services are used (ports and protocols) on the system and which protocols are used to communicate with user systems to be able to create customer-specific firewall rules. The keyword is **firewall-friendly protocols**.

- Siemens recommends to activating the Windows desktop firewall and opening only the necessary and known ports for incoming traffic.
- Install only really needed software. Avoid installation of software, for example, e-mail clients, if not necessary.
- Deactivate all unnecessary services. A typical service for this is the **File and Printer sharing for Microsoft networks**. If you do not have to share folders on your system for others, deactivate this service.
- Create a special Windows user group for your installed program. Only this group is allowed to start the specified program and browse to these folders. If ever possible, this group only has read access to the binary folder of the program.
  Only these defined users are allowed to use the installed program. Normal Windows user accounts on this system are not allowed to do this. This measure grants a high level of security to avoid the infiltration of malware .dll or .exe files.
- Create users which are members of the Windows user group and your defined program group.

NOTE
Never use an administrator account for normal computing.
Whenever possible, activate the automatic Windows update function and update also all third-party software products as, for example, Adobe Reader or Oracle Java runtime environment. Many other programs also support an automated update mechanism. If you do not have direct access to the Internet, perform the update manually or implement a Microsoft WSUS service (Windows Server Update Services) for internal automated Microsoft update mechanism.

Install a released virus scanner on your system with the option on access to avoid an infiltration of malware via storage devices (CD, USB stick, ...) or file sharing. Provide the systems automatically or manually with the topic pattern files.

NOTE
Only a daily updated virus pattern signature grants a high level of security

If plaintext protocols are used to communicate with other communication partners, use the Windows integrated IPSec solution (also integrated in numerous Unix systems, for example, strongSwan) to secure and authenticate the connection.

NOTE
A mix between a Windows and Unix system will also work fine. If you use firewalls, open the IPSec protocol on your firewall (ESP/UDP port 500 or UDP port 4500/UDP port 500).

In many cases, it is recommended to establish a domain concept with proper password rules as a local policy-based user-group set.

The 10 Major Configuration Faults

• Never use the Windows Guest account. Always deactivate this account.

• Never allow everyone access to your shared folder. Delete this access right group and add the right user group. Set the read/write rights with the Security feature.

• Never use a user account as a member of administrator group for normal computing.

• Never use easy user-account passwords. Take a minimum of 8 alphanumeric characters together with special signs. The passwords must respect the rules of NERC CIP and BDEW.

• If ever possible, change your passwords periodically.

• Never run Windows without activated Desktop Firewall, unless you have installed your system in a trusted security perimeter zone. Never run an unpatched Windows, unless you have installed your system in a trusted security perimeter zone.

• Never run Windows without an up-to-date virus scanner, unless you have installed your system in a trusted security perimeter or using whitelisting.

• Whenever possible, do not use third-party software with known security vulnerabilities. If necessary, build a trusted security perimeter zone.

• Never install untrusted software on your productive system.

6.3 Remote Access

6.3.1 Product Side VPN

Products like DIGSI 5 or TOOLBOX II use the TLS protocol for connecting to the devices. That means, if Login/password security is enough, you can use these products out of the box via https to connect your devices. In this case, open your firewall for TCP port 443.
6.3.2 VPN Solution for Remote Access

As described in chapter 2.4 VPN, you can use an external IPSec VPN solution for remote access. An external SSL VPN solution is also possible, but not described here. You can use the Siemens IPSec solution SCALANCE S together with the Softnet Security client, the Siemens IPSec client for easy integration in the SCALANCE S environment. Other vendors, like Cisco, also offer VPN solutions. With a sophisticated rule configuration, it is possible to limit the access and protocols.

With these external solutions, you can use PSK (pre-shared key) mechanisms or certificate-based authentication. With both solutions, you can scan your traffic to the devices because of client2site or site2site VPN which means that the connection after VPN end point is plaintext.

For special use, you can implement a CITRIX environment in a special way. This is not described in this document. In this case, you can put the engineering tools in a DMZ (Demilitarized Zone) of your network for separating the connection and protocol splitting. The easiest solution is to put a standard Windows client, for example, Windows 7, in the DMZ together with remote desktop activation. In this case, you can also separate connection and protocol.

NOTE

Only one user can use the client at the same time

In this case, use an additional IPSec or SSL VPN solution or use the built-in IPSec solution from Microsoft, see also chapter 2.4.2 Windows IPSec Implementation for such an example configuration.

6.3.3 Configuration Example

6.3.3.1 SCALANCE S with Softnet Security Client

This is an encrypted connection between remote clients and internal SCALANCE S VPN devices. No scanning of content within the external/internal firewall is possible because of VPN tunnel termination at each SCALANCE S device.
Figure 6-1  VPN Tunnel

- Installation of Softnet Security Client on each remote machine and import of the SCALANCE S environment configuration file
- Installation of all engineering tools on the remote machine
- Ruleset update of involved SCALANCE S
- External firewall adjustment

6.3.3.2 Site2Site VPN

This is an encrypted connection between the remote client side and the external Firewall/VPN device. No scanning of content within the external firewall is possible, but a scan is possible within the internal firewall device because of plaintext after the external firewall. In this example, shown in the following figure, there is only a network segmentation in the Substation Security Perimeter without a VPN and Firewall protection.
Figure 6-2  Maintenance of a Whitelisted System

- Installation of, for example, a DSL router with IPSec implementation, for example, CISCO
- Installation of a VPN engine on external firewall
- Rulesets and configuration (PSK or certificate usage) on external firewall and DSL VPN router

6.3.3.3  Windows Remote Desktop Solution

This is an encrypted connection between remote clients and a DMZ SCALANCE S VPN device. No scanning of content within the external/internal firewall is possible because of VPN tunnel termination at each SCALANCE S device.
**6.4 Patch Management**

### 6.4.1 General Instruction

Microsoft, Adobe, and other producers of software components regularly eliminate security gaps in their products and distribute these corrections as official patches to their customers. There are many different patch classifications ([http://support.microsoft.com/kb/824684/EN-US/](http://support.microsoft.com/kb/824684/EN-US/)), but only **Security Patches** and **Critical Patches** are necessary for the secure and stable behavior of a product.

For this reason, a SICAM and DIGSI test configuration has been built to test the compatibility of the SICAM software with the Microsoft **Security Patches** and **Critical Patches**. This test configuration is always equipped with the actually released SICAM versions. The test configuration keeps up with the updates distributed by Microsoft. The compatibility of the SICAM version with these updates is tested.

The enclosed files SICAM_PAS_Security_patches.xls, DIGSI5_Security_patches.xls, SICAM_TOOL-BOXII_Security_patches.xls, Submitted_defects_SICAM_230.xls, and DIGSI4_Security_patches.xls contain precise pieces of information on the **Security Patches** and **Critical Patches** whose compatibility has been tested. These files are updated at least 8 weeks after the release of a new **Security Patch** or **Critical Patch**.

---

**Figure 6-3**  Site2Site VPN

- Installation of Softnet Security Client on each remote machine and import of the SCALANCE S environment configuration file
- Installation of all engineering tools on the remote machine
- Ruleset update of involved SCALANCE S
- External firewall adjustment
The following guidelines are valid:
The usage of the updates mentioned above is generally allowed for the following operating systems and components:

- Microsoft Windows and Windows Server operating systems
- Microsoft SQL Server
- Microsoft Internet Explorer
- Other third-party components used in SICAM PAS/PQS, DIGSI 5 and DIGSI 4, and Toolbox II and SICAM 230

In rare cases, a patch can have a negative impact on Siemens software. These patches are listed in the Non approved sheet in the .xls files mentioned above.

NOTE
This guideline only applies for versions SICAM PAS V7.00 and higher.

If contraindications appear during our tests, these indications are communicated immediately via Newsletter. This process does not apply for new Microsoft Service Packs. The usage of these Packs still requires an explicit release. If a higher Microsoft software version is necessary for the updates, check via the WinCC Readme or the item ID: 21927773, if these higher software versions or Service Packs are released with the corresponding WinCC version.

You can find further information concerning patches on the following Microsoft Internet sites:
- Microsoft Security Bulletins German
  https://technet.microsoft.com/de-de/security/default.aspx
- Microsoft Security Bulletins English

6.5 WSUS Offline

6.5.1 Scope/Overview

This document gives a brief overview of the WSUS Offline Update (WOU) package. It outlines the relationships of the scripts and the functioning of the entire package. Furthermore, it describes the workflows with Siemens and with customers using the customized package.

6.5.2 Objectives

The WSUS Offline Update package contains a number of scripts to download Microsoft patches for various platforms and subsequently deploy these patches to the clients. Microsoft patches are tested and released within the scope of patch management for EA products. Siemens recommends installing only these released patches.

Since Siemens is not automatically authorized to deliver Microsoft patches to customers due to license restrictions, Siemens wants to provide customers a list of released patches. The WSUS Offline Update package creates this list and forwards it to customers.

The WSUS Offline Update package was not originally intended for this purpose and had to be modified. The procedure and the modifications are described in the following chapters.
### 6.5.3 Download

The DownloadUpdates.cmd initiates the download of the packages. This script requires the version of the operating system and the language. The `/verify` parameter checks that the downloaded packages have the correct checksum. The UpdateGenerator.exe interface can be used to transfer and select the parameters. DownloadUpdates.cmd first downloads the Microsoft wsusscn2.cab cabinet file containing the URLs of all Microsoft patches. Expand.exe extracts this package to several packages.cab and subsequently reformats them to .xml files. The MSXSLT.exe program creates text files from these .xml files using defined filters. The text files contain a simple listing of the URLs of the required patches.

By default, these files are stored temporarily under `%TEMP%`. The `/skipdownload` parameter prevents these files from being deleted. Siemens requires this parameter to create the corresponding lists for the operating system and service-pack level. **WSUS Offline Update** subsequently passes these text files to the Wget program to download the patches from the Microsoft server.

The `/skipdynamic` parameter bypasses the analysis of the wsusscn2.cab file used to determine the dynamic patches, and instead initiates the download based on the lists created with `/skipdownload`. Both Siemens and the customer require this parameter.

We assume that customers already have their systems preinstalled on the corresponding Windows service-pack level released by Siemens. Installation of the corresponding .NET Framework is equally presumed. This should be performed with the Siemens product installation.

Siemens products were always released for a certain service-pack level, .NET Framework version, and Visual-Studio Redistributable version. Therefore, it must be avoided that the **WSUS Offline Update** package updates the customer systems to the latest service-pack level, .NET Framework version, and VisualStudio Redistributable version.

The function of the parameters `/allowsp` and `/allowdotnet` is to prevent these versions from being downloaded.

### 6.5.4 Installation

The `client` subfolder in the **WSUS Offline Update** package is sufficient for installing the patches. It contains all patches and scripts downloaded previously for the installation. It is also possible to create an ISO image. To start the installation, execute the DoUpdate.cmd batch with specific parameters.

The parameters primarily depend on the desired scope of installation, for example, IE10, IE11, .NET. The Updatelinstaller.exe interface can be used to transfer and select the parameters.

### 6.5.5 Restrictions

The **WSUS Offline Update** solution works based on the Windows cabinet file wsusscn2.cab. This file contains all updates classified as critical and safety-relevant, but not necessarily all important and optional patches. The Microsoft Baseline Security Analyzer also classifies the systems as secure; however, there will always be a delta to the online update. The Online Update is an integral element of the operating system. In Windows 7, it can be accessed from the start menu at Programs > Windows Update > Check for updates. In case of conflicts between the Online Update and the **WSUS Offline Update**, the importance of each individual patch must be assessed.

These patches can be added, if necessary, using static link lists in the directory `\wsusoffline\static`. Therefore, it is important to install always the latest version of **WSUS Offline Update**. However, manual intervention may be necessary given the fact that **WSUS Offline Update** only supports the latest service-pack levels.

For additional information, see /15/.

### 6.5.6 Procedure

#### 6.5.6.1 Overview

Basically, the patches must be smoke-tested against the products first. Subsequently, the customer package is compiled using the modified **WSUS Offline Update** package.
This package enables you to download the patches and subsequently distribute them on your system.

### 6.5.6.2 Overview of the Siemens Workflow

The technical workflow for each individual point is explained in the following chapters.

#### 6.5.6.3 Download and Install WSUS Offline Update

- Download the latest **WSUS Offline Update** package from the WSUSOffline Internet site [http://download.wsusoffline.net](http://download.wsusoffline.net).
- Extract the package (wsusofflinversion.zip) to any directory on the server.

**NOTE**

A check for the latest version is run each time WSUSOfflineUpdateGenerator.exe is started and a dialog for downloading the latest version is displayed.

Use always the latest version of the **WSUS Offline Update** package.

#### 6.5.6.4 Store or Copy Stored WOU Exclude Lists

**WSUS Offline Update** always supports only the latest service-pack level of an operating system and the latest .NET Framework. If, for example, Windows 7 Service Pack 2 is released, the **WSUS Offline Update** no longer supports Service Pack 1. Patches published until Service Pack 2 are added to an exclude list of the latest **WSUS Offline Update** version. Several exclude lists with critical patches until the latest service-pack level exist for each operating system as well as several exclude lists for .NET.

These lists are stored in the WOU in the folder `.wsusoffline\exclude`:
- Windows 7: ExcludeList-w61-x86.txt; ExcludeList-w61-x64.txt
- .NET: ExcludeList-dotnet-x86.txt; ExcludeList-dotnet-x64.txt
The further procedure therefore depends on whether patches for an operating system are downloaded on the latest service-pack level or on an outdated service-pack level. The further procedure also depends on the latest .NET version.

**Store WOU Exclude Lists**

When downloading patches for operating systems with a service-pack level and a .NET version that are up-to-date, the exclude lists must be stored in ClearCase. This is necessary in order to re-import these lists in the next step **Copy Stored WOU Exclude Lists** when a new service-pack level or .NET version is published.

**Copy Stored WOU Exclude Lists**

When downloading patches for operating systems with a service-pack level and a .NET version that are not up-to-date, copy the exclude lists for the required service-pack level and .NET version into the WOU package.

**6.5.6.5 Create Download Link Files**

The UpdateGenerator.ini in the folder `..\wsusoffline\wsusoffline` must have the following parameter in the [Miscellaneous] section:

```
skipdownload=Enabled.
```

This creates the dynamic link lists `ValidDynamicLinks*` in the `%TEMP%` folder which are renamed to `StaticDownloadLinks*` and copied into the target folder `..\wsusoffline\static\custom`.

- Start UpdateGenerator.exe and select the desired platform and language.
- Use the Proxy button to enter the Siemens proxy in the following format:
  ```
  http://domain\username:password@<proxy>:<port>
  ```
- Click the Start button to create the link lists.

If you need to create `StaticDownloadLinks` for an operating system with an old service-pack level later, you can proceed as follows at the example of Windows 7.

Windows 7 SP1 is presently available. All Windows 7 SP0 patches are contained in the SP1 and therefore included in the exclude list, for example, `ExcludeList-w61-x86.txt`. If, however, the content of this exclude list is deleted, the SP0 patches are also entered in the `StaticDownloadLinks`. But if Windows 7 SP2 was already available and the patches for SP1 were to be downloaded, make sure that the SP0 patches contained in SP1 are included in the exclude list.

**6.5.6.6 Download**

The UpdateGenerator.ini in the folder `..\wsusoffline` must have the following parameters:

```
[Miscellaneous]
skipdownload=Disabled
skipdynamic=Enabled
```

```
[Options]
allowsp=Disabled
allowdotnet=Disabled
```

This causes the dynamic XSLT analysis of the `wsusscn2.cab` file to be skipped, only static download links are used instead. Service packs and .NET Frameworks are not downloaded.

- Start UpdateGenerator.exe and select the desired platform and language.
Select the desired parameters in the UpdateGenerator GUI.

Use the Proxy... button to enter the Siemens proxy in the following format:

http://domain\username:password@<proxy>:<port>

Click the Start button to load the patches on the basis of the static lists.
All patches are stored in the folder `../wsusoffline/client` in the respective subfolder of each platform and language.

The following dialog indicates that the download has been completed successfully!

![Successful Download](image)

**NOTE**

After the download, install the installation package on a corresponding system and check it subsequently with the Windows Online Update of the operating system. For details, see 6.5.5 Restrictions.

### 6.5.6.7 Distribution

- Before distributing the client packages, copy the exclude list with the non-released patches into the package. Copy the exclude list into the folder `../wsusoffline/client/exclude/custom/`.

The folder `../wsusoffline/client` including all files and subfolders can be distributed on the systems using an USB stick or network drives.

**NOTE**

Optionally, you can create an ISO image, for each language and for all products or for one product and language, during the download. This must be selected accordingly in the UpdateGenerator GUI.

### 6.5.6.8 Installation

- Start UpdateInstaller.exe and select the desired options.
Click Start and start the update

**6.5.6.9 Delivery/Update ExcludeList**

If errors occur during the smoke test due to installed patches, add the KB number of the patch to the exclude list.

This is Excludeliste.txt for the installation client package in the folder ..\wsusoffline\client\excludelist\custom. This list is valid across platforms and architectures.

**6.5.6.10 Create Siemens WSUS Offline Update Configuration Packages**

After successful smoke testing, update the Siemens WSUS Offline Update configuration package with the latest exclude lists and DownloadLink lists on the Siemens Internet site.

The Siemens WSUS Offline Update configuration package contains the following components:

- **Customer operating instruction**
  
  Step-by-step description from the download to the installation of the patches released by Siemens

- **Custom exclude lists**
  
  Black list with the patches that must not be installed

- **WOU exclude lists**
  
  dependent on the service-pack level and the .NET version

- **DownloadLinkLists**
  
  Text files with the links of the patches available at the time of testing

- **Default INI**
  
  A default UpdateGenerator.ini is copied into the corresponding folder if no UpdateGenerator.ini is available yet.
• **Installation batch file**
  By executing the batch file, the WSUSOffline environment for downloading the patches released by Siemens is configured. For this purpose, the latest exclude list and DownloadLinkLists are copied into the corresponding WSUSOffline directories and UpdateGenerator.ini is replaced.

Different **WSUS Offline Update** configuration packages are available. These packages have different platforms and service-pack levels, for example:

- Configuration package Windows XP SP3
- Configuration package Windows 7
- Configuration package Windows 7 SP1

... There are generally 3 different types for these packages.

- **Type 1 at the example of Windows XP SP3:**
  This service-pack level is EndOfLife which means that Microsoft no longer provides patches for them. It can therefore be assumed for this type that this package does not have to be modified any more.

- **Type 2 at the example of Windows 7:**
  This service-pack level is not yet EndOfLife, nor is it the latest service-pack level, which means that Microsoft regularly provides patches. For this type, it can therefore be assumed that this package permanently contains new DownloadLinkLists and maybe new custom exclude lists. Additionally, this package contains the latest valid WOU exclude list before publishing of Windows 7 SP1.

- **Type 3 at the example of Windows 7 SP1:**
  This service-pack level is not yet EndOfLife, nor is it the latest service-pack level, which means that Microsoft regularly provides patches. For this type, it can therefore be assumed that this package permanently contains new DownloadLinkLists and maybe new custom exclude lists. Additionally, this package contains the latest valid WOU exclude list before publishing of Windows 7 SP2.
6.5.6.11  Overview of the Customer Workflow

The technical workflow for each individual point is explained in the following chapters.

Download and Install WSUS Offline Update

See 6.5.6.3 Download and Install WSUS Offline Update

6.5.6.12  Download and Install Siemens WSUS Offline Update Configuration Package

- Download the current Siemens WSUS Offline Update configuration package, depending on the product, from the Siemens Intranet site via your Siemens-Partner.

NOTE

Various product versions are released for different service-pack levels. Therefore, different WSUS Offline Update configuration packages exist for each product or service-pack level.
• Extract the package (WOU_SIEMENS_EMDGPRO_yyyymm.zip).
• Execute ConfigureWSUSOfflineforSiemens.bat.

Figure 6-10 Path of Offline Package
• Enter and confirm the path to the WSUSOffline package.

Content of the config_pack_wsusofflineversion_OS_ServicePackLevel.zip:

The following figure shows the directory structure:

- Custom_ExcludeList:
  Contains the custom exclude list for the installation package
- Default_INI
  Contains a default UpdateGenerator.in for the first installation of the WSUS Offline Update package
- DynamicLinkLists
  Contains the DownloadLinkLists
- WOU_ExcludeList
  Contains the WOU exclude list for the corresponding service-pack level and .NET version
- ConfigureWSUSOfflineforSiemens.bat
  This batch file copies the DownloadLinkLists and exclude lists to the correct locations and adjusts the UpdateGenerator.ini.

Content of the ConfigureWSUSOfflineforSiemens.bat

```batch
@echo off
set /p installpath=Please enter the path to your WSUS Offline package (for example, C:\WOU\wsusoffline72):
set newinstallpath=%installpath%
xcopy.exe /Y Custom_ExcludeList\ExcludeList.txt "%installpath%\wsusoffline\client\exclude\custom"
xcopy.exe /Y DynamicLinkLists\*.txt "%installpath%\wsusoffline\static\custom"
xcopy.exe /Y WOU_ExcludeList\*.txt "%installpath%\wsusoffline\exclude"
FOR /F "delims:=" %%i in ("%installpath%") do (set LW=%%i
goto :ENDE)
:ENDE
```
call set LW=%LW:~1,100%
echo %LW%
call %LW%:

if exist "%installpath%\wsusoffline\UpdateGenerator.ini" {
  echo UpdateGenerator.ini exists
} else {
  xcopy.exe /Y Default_INI\UpdateGenerator.ini "%newinstallpath%\wsusoffline"
}

cd "%newinstallpath%\wsusoffline"

if exist newUpdateGenerator.ini del newUpdateGenerator.ini

set skipdownload=notset
set skipdynamic=notset
set allowdotnet=notset
set sectionoption=notset
set sectionmisc=notset
set allowsp=notset

for /f "tokens=*" %%a in (UpdateGenerator.ini) do call :AddText "%%a
call :CheckOptions
call :CheckMisc
del UpdateGenerator.ini
rename newUpdateGenerator.ini UpdateGenerator.ini
call UpdateGenerator.exe
exit /b

:AddText %1
set Text=%~1%
if /I "%Text%"=="[Options]" ( 
call :SectionChange
set sectionoption=set
  echo %Text% >> newUpdateGenerator.ini
) else if /I "%Text%"=="[Miscellaneous]" ( 
call :SectionChange
set sectionmisc=set
  echo %Text% >> newUpdateGenerator.ini
) else if /I %sectionoption%==set ( 
call :options
) else if /I %sectionmisc%==set ( 
call :misc
) else if /I "%Text:-0,1%"=="[
  call :SectionChange
  echo %Text% >> newUpdateGenerator.ini
) else ( 
  echo %Text% >> newUpdateGenerator.ini
)
exit /b

:options
if /I "%Text%"=="allowdotnet=Enabled" ( 
  echo allowdotnet=Disabled >> newUpdateGenerator.ini
  set allowdotnet=set
) else if /I "%Text%"=="allowdotnet=Disabled" ( 
  echo %Text% >> newUpdateGenerator.ini
  set allowdotnet=set

else if /I "%Text%"=="allowsp=Enabled" (  
    echo allowsp=Disabled >> newUpdateGenerator.ini  
    set allowsp=set  
) else if /I "%Text%"=="allowsp=Disabled" (  
    echo %Text% >> newUpdateGenerator.ini  
    set allowsp=set  
) else {  
    echo %Text% >> newUpdateGenerator.ini  
}  
exit /b
:misc
if /I "%Text%"=="skipdownload=Enabled" (  
    echo skipdownload=Disabled >> newUpdateGenerator.ini  
    set skipdownload=set  
) else if /I "%Text%"=="skipdownload=Disabled" (  
    echo %Text% >> newUpdateGenerator.ini  
    set skipdownload=set  
) else if /I "%Text%"=="skipdynamic=Disabled" (  
    echo skipdynamic=Enabled >> newUpdateGenerator.ini  
    set skipdynamic=set  
) else if /I "%Text%"=="skipdynamic=Enabled" (  
    echo %Text% >> newUpdateGenerator.ini  
    set skipdynamic=set  
) else {  
    echo %Text% >> newUpdateGenerator.ini  
}  
exit /b
:SectionChange
if %sectionoption%==set {  
    set sectionoption=notset  
    call :CheckOptions  
} else if %sectionmisc%==set {  
    set sectionmisc=notset  
    call :CheckMisc  
}  
exit /b
:CheckOptions
if %allowdotnet%==set {  
    echo Parameter allowdotnet existing  
} else {  
    echo Parameter allowdotnet not existing  
    echo allowdotnet=Disabled >> newUpdateGenerator.ini  
    set allowdotnet=set  
}  
echo %allowsp%  
if %allowsp%==set {  
    echo Parameter allowsp existing  
} else {  
    echo Parameter allowsp not existing  
    echo allowsp=Disabled >> newUpdateGenerator.ini  
    set allowsp=set  
}  
exit /b
:CheckMisc
Download

See 6.5.3 Download

Installation

See 6.5.4 Installation
A Appendix

A.1 Abbreviations 165
### Abbreviations


List of **project/document specific** abbreviations:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Application Control</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AD DS</td>
<td>Active Directory Domain Services</td>
</tr>
<tr>
<td>CC</td>
<td>Change Control</td>
</tr>
<tr>
<td>CLI</td>
<td>Command-Line Interface</td>
</tr>
<tr>
<td>CSR</td>
<td>Certificate Signing Request</td>
</tr>
<tr>
<td>DDC</td>
<td>Desktop Delivery Controller</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>EA</td>
<td>Energy Automation</td>
</tr>
<tr>
<td>eASI</td>
<td>ePO Advanced Suite Installer</td>
</tr>
<tr>
<td>ePO</td>
<td>ePolicy Orchestrator</td>
</tr>
<tr>
<td>ESP</td>
<td>Encapsulating Security Payload</td>
</tr>
<tr>
<td>HIDS</td>
<td>Host-Based Intrusion Detection System</td>
</tr>
<tr>
<td>HMI</td>
<td>Human Machine Interface</td>
</tr>
<tr>
<td>IC</td>
<td>IntegrityControl</td>
</tr>
<tr>
<td>ICA</td>
<td>Citrix XenApp Independent Computing Architectures</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IED</td>
<td>Intelligent Electronic Device</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IPSec</td>
<td>Internet Protocol Security</td>
</tr>
<tr>
<td>LTS</td>
<td>Long-Time Support</td>
</tr>
<tr>
<td>MD5</td>
<td>Message-Digest Algorithm</td>
</tr>
<tr>
<td>NIDS</td>
<td>Network-Based Intrusion Detection System</td>
</tr>
<tr>
<td>Nmap</td>
<td>Network Manager</td>
</tr>
<tr>
<td>OpenSSL</td>
<td>Open Source Secure Sockets Layer</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PFS</td>
<td>Perfect Forward Secrecy</td>
</tr>
<tr>
<td>PRP</td>
<td>Parallel Redundancy Protocol</td>
</tr>
<tr>
<td>PSK</td>
<td>Pre-Shared Key</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, and Adelman - an algorithm for public-key encryption</td>
</tr>
<tr>
<td>SaaS</td>
<td>Software-as-a-Service</td>
</tr>
<tr>
<td>SCT</td>
<td>Security Configuration Tool</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WOU</td>
<td>WSUS Offline Update</td>
</tr>
<tr>
<td>WSUS</td>
<td>Windows Server Update Services</td>
</tr>
</tbody>
</table>
## B List of Required Open Ports

The following table lists are excerpts of the Security Manuals of each individual product:

<table>
<thead>
<tr>
<th></th>
<th>Product</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>B.1</td>
<td>SICAM PAS/PQS, SICAM SCC</td>
<td>167</td>
</tr>
<tr>
<td>B.2</td>
<td>SICAM A8000 Series, Toolbox</td>
<td>170</td>
</tr>
<tr>
<td>B.3</td>
<td>SIGUARD PDP</td>
<td>171</td>
</tr>
<tr>
<td>B.4</td>
<td>SIPROTEC 5 / DIGSI 5</td>
<td>172</td>
</tr>
<tr>
<td>B.5</td>
<td>SIPROTEC 4 / DIGSI 4</td>
<td>173</td>
</tr>
<tr>
<td>B.6</td>
<td>CrossBow</td>
<td>173</td>
</tr>
</tbody>
</table>
## B.1 SICAM PAS/PQS, SICAM SCC

The following table lists the programs and services that communicate between members of the network. If 2 members are in different subnetworks, the ports and protocols must be opened in the Firewalls between the subnetworks.

<table>
<thead>
<tr>
<th>Service</th>
<th>Layer4</th>
<th>Layer7</th>
<th>From (Client)</th>
<th>To (Client)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNP3i Master</td>
<td>TCP</td>
<td>DNP3i</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>DNP3i Slave</td>
<td>TCP</td>
<td>DNP3i</td>
<td>Control center</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>Substation communication DSI</td>
<td>TCP</td>
<td>DSI protocol</td>
<td>SICAM PAS/PQS DIP</td>
<td></td>
</tr>
<tr>
<td>Substation communication CFETest</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>10600-10650</td>
</tr>
<tr>
<td>Substation communication CFETest</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>1947</td>
</tr>
<tr>
<td>Substation communication CFG</td>
<td>UDP</td>
<td>Proprietary</td>
<td>Broadcast</td>
<td>1947</td>
</tr>
<tr>
<td>Substation communication CFG</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>19234, 19235</td>
</tr>
<tr>
<td>Substation communication CFG</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>17824</td>
</tr>
<tr>
<td>Substation communication CFG</td>
<td>UDP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>31365, 31366</td>
</tr>
<tr>
<td>Substation communication CFG</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>51119</td>
</tr>
<tr>
<td>IEC 60870-5-104 Master</td>
<td>TCP</td>
<td>IEC 60870-5-104</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>IEC 60870-5-104 Slave</td>
<td>TCP</td>
<td>IEC 60870-5-104</td>
<td>Control center</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>IEC 61850 Client</td>
<td>TCP</td>
<td>IEC 61850</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>IEC 61850 Server</td>
<td>TCP</td>
<td>IEC 61850</td>
<td>SICAM SCC</td>
<td></td>
</tr>
<tr>
<td>LanguageSwitchService.exe</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>Modbus Master</td>
<td>TCP</td>
<td>Modbus</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>Modbus Slave</td>
<td>TCP</td>
<td>Modbus</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Layer4</td>
<td>Layer7</td>
<td>From (Client)</td>
<td>To (Client)</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------</td>
<td>------------</td>
<td>-----------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>OPC DA Client</td>
<td>TCP</td>
<td>OPC DA</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>OPC DA Server</td>
<td>TCP</td>
<td>OPC DA</td>
<td>Control center</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>OPC XML DA Server</td>
<td>TCP</td>
<td>Proprietary</td>
<td>Control center</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>PQ Analyzer backup</td>
<td>TCP</td>
<td>Proprietary</td>
<td>PQ Analyzer</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>PQ Analyzer demo</td>
<td>TCP</td>
<td>Proprietary</td>
<td>PQ Analyzer</td>
<td>Local</td>
</tr>
<tr>
<td>PQ Analyzer runtime</td>
<td>TCP</td>
<td>Proprietary</td>
<td>PQ Analyzer</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>PQ Analyzer runtime</td>
<td>TCP</td>
<td>SMTP</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>SMTP server</td>
</tr>
<tr>
<td>RemoteServer.exe</td>
<td>TCP</td>
<td>.NET commun</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>Diamond Server</td>
</tr>
<tr>
<td>RemoteServer.exe</td>
<td>TCP</td>
<td>.NET commun</td>
<td>Diamond Server</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>SCC Proxy</td>
<td>TCP</td>
<td>Proprietary</td>
<td>WinCC Server/SICAM</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
</tr>
<tr>
<td>SICAM SCC Redundancy</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM SCC</td>
<td>SICAM SCC</td>
</tr>
<tr>
<td>Synchtool.exe</td>
<td>TCP</td>
<td>HTTP</td>
<td>Computer with Web browser</td>
<td>Diamond Server</td>
</tr>
<tr>
<td>SICAM Diamond Client</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Computer with Web browser</td>
<td>Diamond Server</td>
</tr>
<tr>
<td>SICAM PAS/PQS UI –</td>
<td>TCP</td>
<td>HTTP</td>
<td>Computer with Web browser</td>
<td>Diamond Server</td>
</tr>
<tr>
<td>Operation Client</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Computer with Web browser</td>
<td>Diamond Server</td>
</tr>
<tr>
<td>SICAM Q80</td>
<td>TCP</td>
<td>FTP</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>SIMEAS R / PMU</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>Substation communication</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>SICAM PAS</td>
</tr>
<tr>
<td>CfeSimeasRDM.exe</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>IED</td>
</tr>
<tr>
<td>SIPROTEC 4</td>
<td>UDP</td>
<td>Proprietary</td>
<td>DIGSI 4 Service PC</td>
<td>50000</td>
</tr>
<tr>
<td>DIGSI protocol</td>
<td></td>
<td></td>
<td>Computer with Web browser</td>
<td>SIPROTEC 4</td>
</tr>
<tr>
<td>SIPROTEC 4</td>
<td>UDP</td>
<td>JAVA</td>
<td>Computer with Web browser</td>
<td>56797</td>
</tr>
<tr>
<td>Web Monitor</td>
<td></td>
<td></td>
<td>Computer with Web browser</td>
<td>SIPROTEC 4</td>
</tr>
<tr>
<td>SIPROTEC 4</td>
<td>TCP</td>
<td>HTTP</td>
<td>Computer with Web browser</td>
<td>80</td>
</tr>
<tr>
<td>Web Monitor &amp; Communication Module Website</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIPROTEC 5*</td>
<td>TCP</td>
<td>HTTPS</td>
<td>DIGSI 5 Service PC</td>
<td>443</td>
</tr>
</tbody>
</table>

List of Required Open Ports

B.1 SICAM PAS/PQS, SICAM SCC
<table>
<thead>
<tr>
<th>Service</th>
<th>Layer4</th>
<th>Layer7</th>
<th>From (Client)</th>
<th>To (Client)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host</td>
<td>Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To (Client)</td>
<td>Host</td>
</tr>
<tr>
<td>Supervision via SNMP</td>
<td>UDP</td>
<td>SNMP</td>
<td>DIGSI computer</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>Supervision via SNMP</td>
<td>UDP</td>
<td>SNMP</td>
<td>Computer with SNMP browser</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>Supervision via SNMP</td>
<td>UDP</td>
<td>SNMP</td>
<td>Computer with SNMP browser</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>Supervision via SNMP</td>
<td></td>
<td>SNMP</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>Sybase dbsrv9.exe</td>
<td>TCP</td>
<td>ODBC</td>
<td>SICAM PAS/PQS DIP</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>UDP</td>
<td>NTP</td>
<td>SICAM PAS/PQS Full Server/DIP</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>UDP</td>
<td>Syslog</td>
<td>All PC's NTP Server</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>TraceWindowService.exe</td>
<td>TCP</td>
<td>TCP</td>
<td>Proprietary</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>WinCC Web Client</td>
<td>TCP</td>
<td>HTTPS</td>
<td>WinCC Web Client</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>WinCC, Simatic Communication Service SCS</td>
<td>TCP</td>
<td>Proprietary via RPC</td>
<td>WinCC WebNavigator Server</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>WinCC, Simatic Communication Service SCS†</td>
<td>TCP</td>
<td>Proprietary via RPC</td>
<td>WinCC Client</td>
<td>(&gt;1024)</td>
</tr>
<tr>
<td>Windows – Remote Desktop/Terminal-server</td>
<td>TCP</td>
<td>RDP</td>
<td>Windows PC</td>
<td></td>
</tr>
<tr>
<td>Substation communication Btiserver.exe +</td>
<td>TCP</td>
<td>Proprietary</td>
<td>SICAM PAS</td>
<td>10025</td>
</tr>
</tbody>
</table>

* The DIGSI5 application itself needs no special open port because there are no incoming connections. For more information, refer to SIPROTEC 5 Application Notes, Communication Architectures Under Cyber Security Aspects.
† Depending on used WinCC functions, more ports could be in use. For details, see SIMATIC HMI WinCC V6 Basic Documentation.
+ Internal communication between SICAM PAS Full Server and SICAM PAS DIP
For RPC communication, ports are temporarily used and dynamically assigned (1024 through 65635) by the RPC endpoint mapper.
### B.2 SICAM A8000 Series, Toolbox

<table>
<thead>
<tr>
<th>Service</th>
<th>Layer 4 Prot.</th>
<th>Layer 7 Prot.</th>
<th>From Host (Client)</th>
<th>From Port (Client)</th>
<th>To Host (Server)</th>
<th>To Port (Server)</th>
<th>Process Control</th>
<th>System Monitoring</th>
<th>System Diagnostics</th>
<th>System Param set</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Client</td>
<td>UDP</td>
<td>DHCP</td>
<td>SICAM A8000 Series</td>
<td>68/UDP (Client)</td>
<td>PC</td>
<td>67/UDP (Server or Relay-Agent)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>DHCP Server / Relay Agent</td>
<td>UDP</td>
<td>UDP</td>
<td>TFTP</td>
<td>PC</td>
<td>67/UDP (Server or Relay-Agent)</td>
<td>SICAM A8000 Series</td>
<td>68/UDP (Client or Relay-Agent)</td>
<td>-</td>
<td>-</td>
<td>x</td>
</tr>
<tr>
<td>NTP Time Setting</td>
<td>UDP</td>
<td>NTP</td>
<td>SICAM AK, AK3, AK4</td>
<td>123</td>
<td>NTP Server</td>
<td>123 (symmetric mode)</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>NTP Time Setting</td>
<td>UDP</td>
<td>NTP</td>
<td>SICAM AK, AK3, AK4</td>
<td>123</td>
<td>SICAM AK, AK3, AK4</td>
<td>123 (symmetric mode)</td>
<td>x</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SNMP</td>
<td>UDP</td>
<td>SNMP</td>
<td>PC</td>
<td>&gt;1024</td>
<td>SICAM AK3, SICAM A8000 Series</td>
<td>161</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>UDP</td>
<td>SNMP</td>
<td>SICAM A8000 Series</td>
<td>&gt;1024</td>
<td>162</td>
<td>-</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>IPsec VPN</td>
<td>UDP</td>
<td>-</td>
<td>SICAM AK, AK3, AK4</td>
<td>500, 4500</td>
<td>CISCO Router</td>
<td>500, 4500</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Syslog Client</td>
<td>UDP</td>
<td>-</td>
<td>SICAM AK, Toolbox-PC</td>
<td>*</td>
<td>Syslog Server</td>
<td>514</td>
<td>-</td>
<td>x</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>RADIUS authentication protocol</td>
<td>TCP</td>
<td>-</td>
<td>SICAM A8000 Series</td>
<td>&gt;1024</td>
<td>Radius AAA Server</td>
<td>1812</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>NetOp Remote Control</td>
<td>TCP</td>
<td>RDP</td>
<td>Windows PC</td>
<td>&gt;1024</td>
<td>Toolbox PC</td>
<td>6502</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Remote Control</td>
<td>TCP</td>
<td>RDP</td>
<td>Windows PC</td>
<td>&gt;1024</td>
<td>Toolbox-PC</td>
<td>5900</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Remote Control</td>
<td>TCP</td>
<td>RDP</td>
<td>Windows PC</td>
<td>&gt;1024</td>
<td>Toolbox-PC</td>
<td>3389</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>VNC</td>
<td>TCP</td>
<td>RDP</td>
<td>Windows PC</td>
<td>&gt;1024</td>
<td>Toolbox-PC</td>
<td>5900</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>RDP</td>
<td>TCP</td>
<td>RDP</td>
<td>Windows PC</td>
<td>&gt;1024</td>
<td>Toolbox-PC</td>
<td>3389</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Toolbox, Remote Director</td>
<td>TCP</td>
<td>Proprietary</td>
<td>Toolbox-PC</td>
<td>&gt;1024</td>
<td>Toolbox Peer Server</td>
<td>2131</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Toolbox, Database</td>
<td>TCP</td>
<td>Proprietary</td>
<td>Toolbox-PC</td>
<td>&gt;1024</td>
<td>Toolbox Peer Server</td>
<td>1521, 1522</td>
<td>-</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>Layer 4 Prot.</td>
<td>Layer 7 Prot.</td>
<td>From Host (Client)</td>
<td>From Port (Client)</td>
<td>To Host (Server)</td>
<td>To Port (server)</td>
<td>Process Control</td>
<td>System Monitoring</td>
<td>System Diagnostics</td>
<td>System param set.</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>--------------------</td>
<td>--------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Toolbox, File Sharing</td>
<td>TCP</td>
<td>Proprietary</td>
<td>Toolbox-PC</td>
<td>&gt;1024</td>
<td>Toolbox Peer Server</td>
<td>139, 445</td>
<td>–</td>
<td>–</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Toolbox, CAEx Dongle</td>
<td>TCP</td>
<td>Proprietary</td>
<td>Toolbox-PC</td>
<td>&gt;1024</td>
<td>Toolbox Peer Server</td>
<td>3047</td>
<td>–</td>
<td>–</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Toolbox, remote Operation – Start</td>
<td>ICMP</td>
<td>ECHO</td>
<td>Toolbox-PC</td>
<td>–</td>
<td>SICAM AK, AK3</td>
<td>SICAM BC</td>
<td>–</td>
<td>–</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Web</td>
<td>TCP</td>
<td>HTTP</td>
<td>PC with browser</td>
<td>–</td>
<td>SICAM AK, AK3</td>
<td>SICAM BC</td>
<td>80</td>
<td>–</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Web</td>
<td>TCP</td>
<td>HTTPS</td>
<td>PC with browser</td>
<td>–</td>
<td>SICAM AK, AK3</td>
<td>SICAM BC</td>
<td>443</td>
<td>–</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Remote Operation TBII</td>
<td>TCP</td>
<td>HTTP</td>
<td>Toolbox PC</td>
<td>–</td>
<td>SICAM AK, AK3</td>
<td>SICAM BC</td>
<td>80</td>
<td>–</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>WEBcmic</td>
<td>UDP</td>
<td>Proprietary</td>
<td>PC</td>
<td>&gt;1024</td>
<td>SICAM A8000 Series</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>x</td>
</tr>
<tr>
<td>WEBcmic</td>
<td>ICMP</td>
<td>Proprietary</td>
<td>PC</td>
<td>*<em>.</em></td>
<td>SICAM EMIC</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>x</td>
</tr>
<tr>
<td>Ping</td>
<td>ICMP</td>
<td>PING</td>
<td>SICAM AK, AK3</td>
<td>*<em>.</em></td>
<td>SICAM AK, AK3</td>
<td>SICAM BC</td>
<td>–</td>
<td>–</td>
<td>–</td>
<td>x</td>
</tr>
</tbody>
</table>

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.

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

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

### B.3 SIGUARD PDP

<table>
<thead>
<tr>
<th>Service</th>
<th>Layer 4 Prot.</th>
<th>Layer 7 Prot.</th>
<th>FROM</th>
<th>TO</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDPx64.exe</td>
<td>TCP</td>
<td>SSI Read</td>
<td>SIGUARD UI</td>
<td>Managed by operating system</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SIGUARD PDP Server</td>
<td>4714</td>
</tr>
</tbody>
</table>
### B.4 SIPROTEC 5 / DIGSI 5

**List of Required Open Ports**

#### B.4 SIPROTEC 5 / DIGSI 5

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PDPx64.exe</td>
<td>TCP</td>
<td>SSI Write</td>
<td>SIGUARD Application</td>
<td>Managed by</td>
<td>4715</td>
<td>SIGUARD PDP Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>system</td>
<td>operating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDPx64.exe</td>
<td>TCP</td>
<td>C37.118 data-stream</td>
<td>PMU</td>
<td>4712</td>
<td>SIGUARD PDP Server</td>
<td>Managed by Server operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDPx64.exe</td>
<td>UDP</td>
<td>C37.118 data-stream</td>
<td>PMU</td>
<td>4713</td>
<td>SIGUARD PDP Server</td>
<td>Managed by Server operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPWx64.exe</td>
<td>TCP</td>
<td>Siguard</td>
<td>SIGUARD PDP Server</td>
<td>4716</td>
<td>SIGUARD PDP Server</td>
<td>Manage the Master/Standby Switch between two SIGUARD PDP servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process Watcher</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDCServer.exe</td>
<td>TCP</td>
<td>C37.118 data-stream</td>
<td>SIGUARD PDP Server</td>
<td>4712</td>
<td>SIGUARD PDP Server</td>
<td>Managed by Server operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(configured by Engineer)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDCServer.exe</td>
<td>UDP</td>
<td>C37.118 data-stream</td>
<td>SIGUARD PDP Server</td>
<td>4713</td>
<td>SIGUARD PDP Server</td>
<td>Managed by Server operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(configured by Engineer)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Osill2d.exe</td>
<td>TCP</td>
<td>ICCP</td>
<td>SIGUARD PDP Server</td>
<td>102</td>
<td>Control Center</td>
<td>102</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CfeIEC104Slave.exe</td>
<td>TCP</td>
<td>IEC 60870-5-104</td>
<td>SIGUARD PDP Server</td>
<td>Managed by</td>
<td>Control Center</td>
<td>2404</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Server operating system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DAServer.exe</td>
<td>TCP</td>
<td>OPC</td>
<td>SIGUARD PDP Server</td>
<td>Managed by</td>
<td>Control Center</td>
<td>Managed by Server operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Server operating system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Opcenum.exe</td>
<td>TCP</td>
<td>OPC</td>
<td>SIGUARD PDP Server</td>
<td>Managed by</td>
<td>Control Center</td>
<td>Managed by Server operating system</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Server operating system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ntpd-sag.exe</td>
<td>UDP</td>
<td>Clock, NTP</td>
<td>SIGUARD PDP Server</td>
<td>123</td>
<td>SIGUARD PDP Server</td>
<td>123</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**DIGSI 5 Protocol to Automation License Manager**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DIGSI 5 protocol to Automation License Manager</td>
<td>TCP</td>
<td>DIGSI 5 protocol to Automation License Manager</td>
<td>DIGSI 5 PC</td>
<td>4410 (default value)</td>
<td>Automation License Manager on a possible separate server. i.e. local host</td>
<td>4410 (default value)</td>
</tr>
</tbody>
</table>

**DIGSI 5 Communication protocol to SIPROTEC 5**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>DIGSI 5 communication protocol to SIPROTEC 5</td>
<td>TCP</td>
<td>HTTPS</td>
<td>DIGSI 5 PC</td>
<td>&gt;1024</td>
<td>SIPROTEC 5</td>
<td>443</td>
</tr>
<tr>
<td>Service</td>
<td>Layer 4 Protocol</td>
<td>Layer 7 Protocol</td>
<td>Typical Client</td>
<td>Client Port</td>
<td>Typical Server</td>
<td>Server Port</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Reporting / IEC 61850 / MMS</td>
<td>TCP</td>
<td>IEC61850</td>
<td>IEC 61850 client (e.g. SICAM PAS, SICAM A8000)</td>
<td>&gt;1024</td>
<td>SIPROTEC 5</td>
<td>102</td>
</tr>
<tr>
<td>Time Synchronization / SNTP</td>
<td>UDP</td>
<td>SNTP</td>
<td>SIPROTEC 5</td>
<td>123</td>
<td>SNTP Server</td>
<td>123</td>
</tr>
<tr>
<td>Monitoring via Simple Network Management Protocol (SNMPv3)</td>
<td>UDP</td>
<td>SNMPv3</td>
<td>PC with SNMP client (e.g. SICAM PAS/1703/ DIGSI 5 PC/Remote DIGSI 5 PC)</td>
<td>&gt;1024</td>
<td>SIPROTEC 5</td>
<td>161</td>
</tr>
<tr>
<td>DNP3i</td>
<td>TCP</td>
<td>DNP3 TCP</td>
<td>SICAM PAS</td>
<td>20000 or next free port</td>
<td>SIPROTEC 5</td>
<td>20000</td>
</tr>
<tr>
<td>Synchrophasor</td>
<td>TCP</td>
<td></td>
<td>Phasor data concentrator</td>
<td>&gt;1024</td>
<td>SIPROTEC 5</td>
<td>4712</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4713</td>
</tr>
<tr>
<td>MODBUS on TCP</td>
<td>TCP</td>
<td>MODBUS</td>
<td>Substation controller</td>
<td>&gt;1024</td>
<td>SIPROTEC 5</td>
<td>502</td>
</tr>
<tr>
<td>Temperature box</td>
<td>UDP</td>
<td>RTD</td>
<td>Temperature box</td>
<td>&gt;1024</td>
<td>SIPROTEC 5</td>
<td>can be configured</td>
</tr>
<tr>
<td>Syslog Client</td>
<td>UDP</td>
<td>-</td>
<td>SIPROTEC 5</td>
<td>*</td>
<td>Syslog Server</td>
<td>514</td>
</tr>
</tbody>
</table>

### B.5  SIPROTEC 4 / DIGSI 4

<table>
<thead>
<tr>
<th>Service</th>
<th>Layer 4 Protocol</th>
<th>Layer 7 Protocol</th>
<th>Typical Client</th>
<th>Client Port</th>
<th>Typical Server</th>
<th>Server Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIGSI 4 communication protocol to SIPROTEC 4</td>
<td>UDP</td>
<td></td>
<td>DIGSI 4 PC</td>
<td>50000</td>
<td>SIPROTEC 4</td>
<td></td>
</tr>
<tr>
<td>EN100 IEC61850</td>
<td>TCP</td>
<td>IEC61850</td>
<td>IEC61850 client (e.g. SICAM PAS, SICAM A8000)</td>
<td>&gt;1024</td>
<td>SIPROTEC 4</td>
<td>102</td>
</tr>
<tr>
<td>Homepage EN100</td>
<td>TCP</td>
<td>HTTP5</td>
<td>DIGSI 4 PC</td>
<td>80</td>
<td>EN100 Modul</td>
<td></td>
</tr>
<tr>
<td>Time Synchronization / SNTP</td>
<td>UDP</td>
<td>SNTP</td>
<td>SIPROTEC 4</td>
<td>123</td>
<td>SNTP Server</td>
<td>123</td>
</tr>
<tr>
<td>Monitoring via Simple Network Management Protocol</td>
<td>UDP</td>
<td>SNMPv3</td>
<td>PC with SNMP client (e.g. SICAM PAS, DIGSI 4 PC)</td>
<td>&gt;1024</td>
<td>SIPROTEC 4</td>
<td></td>
</tr>
</tbody>
</table>

### B.6  CrossBow

<table>
<thead>
<tr>
<th>Service</th>
<th>Layer 4 Protocol</th>
<th>Layer 7 Protocol</th>
<th>From (Client)</th>
<th>To (Server)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crossbow Communication Client/Server</td>
<td>TCP</td>
<td>Proprietary</td>
<td>Crossbow Client 21000</td>
<td>Crossbow Server 21000</td>
</tr>
<tr>
<td>RSA Authentication SecurID</td>
<td>TCP</td>
<td>RSA protocol</td>
<td>Crossbow Server 5500</td>
<td>RSA Server 5500</td>
</tr>
</tbody>
</table>
## List of Required Open Ports

### B.6 CrossBow

<table>
<thead>
<tr>
<th>Service</th>
<th>Layer 4</th>
<th>Layer 7</th>
<th>From (Client)</th>
<th>To (Server)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius Authentication</td>
<td>UDP</td>
<td></td>
<td>Crossbow Server 1812</td>
<td>Radius Server 1812</td>
</tr>
<tr>
<td>Crossbow Server Computer mutual authentication</td>
<td>TCP</td>
<td>Proprietary</td>
<td>Crossbow Server 21005</td>
<td>Crossbow Station Access Controller 21005</td>
</tr>
<tr>
<td>Active directory</td>
<td>TCP</td>
<td>LDAP</td>
<td>Crossbow Server 389</td>
<td>Domain Controller 389</td>
</tr>
<tr>
<td>Active directory</td>
<td>TCP</td>
<td>LDAP SSL</td>
<td>Crossbow Server 636</td>
<td>Domain Controller 636</td>
</tr>
<tr>
<td>Email</td>
<td>TCP</td>
<td>SMTP</td>
<td>Crossbow Server 25</td>
<td>Email Server 25</td>
</tr>
<tr>
<td>SIPROTEC 4</td>
<td>UDP</td>
<td>Proprietary</td>
<td>Crossbow Server 50000</td>
<td>SIPROTEC 4</td>
</tr>
<tr>
<td>SIPROTEC 5</td>
<td>TCP</td>
<td>SSL</td>
<td>Crossbow Server 443</td>
<td>SIPROTEC 5</td>
</tr>
</tbody>
</table>
Literature

1. ePO: Installation guide: epo_460_install_guide_en-us.pdf
2. ePO: Quick start: Best-Practice-McAfee-ApplicationControl-v6.pdf
3. ePO: Configuration: epo_460_product_guide_en-us.pdf
4. CLI: Installation guide: MFE_SO_WIN_IG_6.0.0.pdf
5. CLI: Reference guide: MFE_SO_ALL_RG_CLI_AC_6.0.0.pdf
8. WSUS Offline Update: WSUSOfflineUpdate.pdf
11. SICAM 1703 Security Administrator Manual
12. SiPROTEC 5 Application Note
13. SICAM 230 Hardening Guide