SIEMENS

SICAM RTUs

Security Testing

Document Label:
SICRTUs-HBSECURITYTESTINGRTUS-ENG_V2.04
Issuing date:
2017.02.28

Siemens AG
Energy Automation
Humboldtstraße 59
90459 Nürnberg
Deutschland

Preface

Contents of the Manual

As a basis for a secure system design and operation the following information about SICAM RTUs is contained in this manual:

- Security testing

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

Scope of Validity

This document is valid for SICAM RTUs (SICAM AK 3 and the products of the SICAM A8000 Series) with hardware and firmware versions dated February 2014 or later.

More specifically, this includes:

- SICAM AK 3
- SICAM AK
- SICAM BC
- SICAM TM
- SICAM A8000 Series:
  - SICAM CP-8000
  - SICAM CP-8021
  - SICAM CP-8022
  - SICAM CP-8050

Target Group

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

- operation and maintenance
- cyber security responsible

Conventions Used

- Manuals that are referenced are written in italics
  e.g. *Common Functions, System and Basic System Elements*, section *Information Objects*.

Table of Contents

1 Introduction

Contents

1.1 Background

People known as "black-hat hackers" derive pleasure from wreaking havoc on security systems, and some hackers do it for money. Whatever the reason may be, malicious hackers cause nightmares for companies and organizations of almost all sizes. Security devices are favorite targets for hackers. However, this threat can be prevented to a large degree if proper security measures are put in place at the right time.

Some measures for prevention are as follows:

Identify entry points: Use proper scanning software programs to identify all entry points into the internal network(s) of the Smart Grid devices. Any attack on the network needs to start from these points. Identifying these entry points, however is not at all easy task. This should be done with help of skilled ethical hackers who have taken special network security training to perform this task successfully.

Perform attack and penetration tests: By running the attack and penetration tests vulnerabilities can be discovered which might be used by a hacker. After identifying the weak points, measures can be implemented to mitigate the risk of an attack using the weaknesses. The test must be done from both the internal as well as external perspectives to detect all the vulnerable points.

A penetration test is part of the vulnerability management process, and is performed during te system test.

The described security test suite explains which and how IT security testing tools are deployed during system test in order to ensure the IT security of the named SICAM products.

Some of the tools described will also identify weaknesses in the stability and performance of a product.

Note

The hacker accesses the system on the back of a bug.

1.2 Purpose of this document

The purpose of this document is to describe the detailed process of the security test of SICAM RTUs LAN Interfaces implementation in the Device Under Test [further DUT]. The security test was executed at Siemens in Vienna, Austria. Passing the described security tests will result in issuing a certificate of security conformity of the particular product. The certificate represents SIEMENS commitment to produce high quality and secure products the customer can rely on.

1.3 SICAM RTUs Device under Test

The test focus is TCP and UDP. The test will be done at SICAM AK 3, at SM-2558 and at SICAM A8000 Series CP-8000, CP-802x and CP-8050. The position of SM-2558 at SICAM AK 3 (or SICAM AK) does not matter, the basic system element can be either CP-2016 or CP-2019 (or CP-2014, CP-2017, CP-6014, CP-5014).

http WEB Server at TCP port 80 is not secured, it is recommended to use https WEB-Server at TCP port 443 ! http WEB Server at TCP port 80 is not part of security test.

GOOSE (Ethernet Layer) actual is not part of security test.

1.4 Test Methods

Penetration test is a network (LAN interfaces) testing method, to find out weakness of a system. We differentiate between stress test, port scan and vulnerability scan.

1.4.1 Stress Test

Threat:

Attacker launches a Dos “denial of service” attack.

Non availability of system due to high data load.

Risk:

Additional costs if manual interaction with system is required to restore system to operation.

Measure:

All TCP/IP protocols are validated during system test to withstand a longer lasting attack (about 1 hour) and recover automatically after attack within 10 minutes.

Objective:

Provide appropriate resistance against DoS attack.

1.4.2 Port Scan

Threat:

Attacker successfully imports malicious software which leads to malfunction of system. E.g. via FTP TCP port 21.

Risk:

Malfunction of system causes damage to the assets (e.g. Switchgear).

Measure:

Validation during the system test if only documented and required TCP/UDP ports (services) are available (see SICAM TOOLBOX II ADMINISTRATOR Security-Manual /2/).

Objective:

To minimize the number of available services for an attack.

1.4.3 Vulnerability Scan

Threat:

Utilization of known vulnerabilities of the used and documented TCP/UDP ports (services). E.g. via https port 443.

Risk:

Malfunction of system causes damage to the assets (e.g. Switchgear).

Measure:

Validation during system test if known vulnerabilities of documented and required TCP/UDP ports (services) can be used to tamper with the system.

Objective:

It shall not be possible to use known vulnerabilities to tamper with the system.

1.4.4 Protocol fuzzing

Threat:

An Attacker cause a denial of service attack or an targeted system crash, by exploiting access violation or untreated program state.

Risk:

Malfunction of system causes damage to the assets (e.g. Switchgear).

Measure:

Validation of protocol stack during system test if unknown behaviour can be used for system tampering.
Protocols imply norms, which are sometimes blurry, very complicated or badly implemented: that's why developers sometimes mess up in the implementation process (because of time/cost constraints). That's why it can be interesting to take the opposite approach: take a norm, look at all mandatory features and constraints, and try all of them; forbidden/reserved values, linked parameters, field sizes. That would be conformance testing oriented fuzzing.

Objective:

It shall not be possible that the system fails by .

2 Test Result

Please refer to the “Certificate of Security Conformity”, we provide one “Certificate of Security Conformity” for each tested Firmware version (see SharePoint).

3 Toolset

Contents

3.1 Introduction

This section details IT security test tools that are used in system tests for penetration testing.

The main goal for such testing is not the testing itself, it is the validation and comparison against the reference results of each product.

Example: Port Scanning
The open ports are described in the security SICAM TOOLBOX II ADMINISTRATOR Security-Manual /2/. The test results have to be compared against this document, differences have to be solved.

3.2 Mausezahn – Traffic Generator

MZ “Mausezahn” is a fast network traffic generator which allows you to stress your software or hardware system with any kind of packets. MZ graws into your system.

The goal of using this tool is:

- Check the robustness of your product and the specific protocols beginning at layer2 of the OSI reference model up to the layer4 protocols TCP and UDP.
- Check the correct behavior of the system if the packets are malformed or with incorrect content
- Find out the network load limit where a communication with the device is possible without restrictions, with a delay of X seconds or communication is not longer possible
- Check if critical functions are still working under high network load if the test object is not a pure communication product (e.g. SICAM RTUs: Internal Processing must not be influenced under high network load)

3.2.1 Functionality / limitations

Mausezahn allows sending an arbitrary sequence of bytes directly out of the network interface card. Mausezahn do not know any upper layer protocols such as HTTP. Mausezahn allows you to send any (malformed or correct) IP packet. Every field in the IP header can be manipulated but also every single bit of a packet can be changed if you type the whole packet as hex in the command line.

For more information about Mausezahn see http://www.perihel.at/sec/mz/index.html

3.3 Nmap – Port scanning

Nmap (short form of "Network Mapper") is the most widely used utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it also works well against single hosts.
Nmap uses raw IP packets to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Nmap features include:

- Host Discovery - Identifying computers on a network, for example listing the computers which respond to pings, or which have a particular port open
- Port Scanning - Enumerating the open ports on one or more target computers
- Version Detection - Interrogating listening network services listening on remote computers to determine the application name and version number.
- OS Detection - Remotely determining the operating system and some hardware characteristics of network devices.

3.3.1 Functionality / limitations

Nmap tries to audit the networking security state of a remote computer, by identifying the network connections which can be made to it. It does this by connecting to a defined range of either TCP or UDP ports at a given IP address. Hereby, the open ports on a target computer are identified. When open ports are found, Nmap tries to guess the services that are connected to open ports.

Limitations: Nmap can, due to the nature of IP protocols, only detect and verify ports which are reachable and externally visible via a system`s network interface. Services that are either bound to the localhost IP, or services which have access control lists or are even firewalled, cannot be accessed by Nmap.

Please note also that Nmap port scans can crash remote services. This can e.g. happen during the service guess phase, as Nmap is sending common protocol requests (e.g. HTTP GET) when trying to fingerprint a service. If the service lacks proper input validation it will not be able to handle the unexpected data properly which might eventually lead to a crash.

Alternately, it is possible to reconfirm results locally by combining the output of the netstat command with the configuration of the host-based firewall (if applicable).

Also, please note that in some cases Nmap may be falsely reported as security threat by virus scanners (e.g. Trend Micro). On the system of a scan manager, this is obviously a false positive and may only be circumvented by reconfiguring the virus scanner e.g. to restrict certain directories with scanning tools.

For more information about Nmap see http://en.wikipedia.org/wiki/Nmap .

3.3.2 Hint

During NMAP Scan all Scripts shall be activated (-A).

3.4 Nessus - Vulnerability Scanner

Nessus is a powerful tool with features that can help security professionals secure even the most vulnerable networks.

3.4.1 Functionality / limitations

The Nessus User Interface (UI) is a web-based interface to the Nessus scanner that is made up of a simple HTTP server and web client, requiring no software installation apart from the Nessus server.

The primary features are:

- Generates **`.nessus`** files that Tenable products use as the standard for vulnerability data and scan policy.
- A policy session, list of targets and the results of several scans can all be stored in a single **`.nessus`** file that can be easily exported. Please refer to the Nessus File Format guide for more details.
- The GUI displays scan results in real-time so you do not have to wait for a scan to complete to view results.
- Provides unified interface to the Nessus scanner regardless of base platform.
- Scans will continue to run on the server even if you are disconnected for any reason.
- Nessus scan reports can be uploaded via the Nessus UI and compared to other reports.

3.4.2 Hint

Nessus must be used in a Kali Linux machine, all plugins has to be enabled.

TCP uses the namp scan (TCP port 0-65535), at UDP all predefined ports are scanned (no namp UDP scan; A custom range of ports can be selected by using a comma delimited list of ports or port ranges. For example, “21,23,25,80,110”; e.g. `nmap -sU -p123 192.168.122.254`).

3.5 Aegis™ Protocol Fuzzer

ICS / SCADA applications require robust components, but too often software is the weakest link.

Aegis™ is a smart fuzzing framework for a growing number of protocols that can identify robustness and security issues in communications software before it is deployed in a production system. Refer also to hint in chapter 3.5.3.

3.5.1 Functionality / limitations

Aegis is a set of fuzzing test cases for ICS/SCADA protocols. The tests are written using several different methodologies to enhance test coverage:

- modeling of the protocol grammars
- analysis of the protocol specifications themselves
- brute-force (but-repeatable) randomness within appropriate encapsulation

It combines aspects of generational and mutational fuzzing to provide deep coverage of the target software.

Generic concepts

Aegis uses a plug-in architecture internally so that protocol modules and test cases can be easily added to the platform. For the user, this means that the generic concepts you learn for one module are applicable to another. These concepts are the same whether you are using the console or the studio (GUI).

- **Modules** are collections of test procedures for a single protocol. They may provide client and server test procedures, or these may be broken out into separate modules. Modules are also the lowest level at which the software is licensed.
- **Procedures** are sequences of test cases that exercise a specific aspect or layer of a protocol. They range in size from a handful of frames to hundreds of thousands.
- **Test cases** are a single test frame and health check sequence tied to a numeric identifier. Test cases are described in more detail below.
- **Health checks** are known valid messages for the protocol under test that are interleaved in the test sequence to verify that the target hasn't crashed.

Test flow

A single test case consists of a test message, preceded or followed by one more health checks:

<------> optional health check(s)

=======> test message

<------> optional health check(s)

This strategy will typically help the tester identify the exact test case that caused the target to fail. Sometimes, more complex bugs that involve subtle memory corruptions or non-deterministic behavior will require the use of a debugger or companion tooling as described in another section. Future versions of Aegis may "close the loop" with some of these application monitors to provide more direct feedback on fault analysis to the fuzzer.

Test case ids

Test cases are referred to by their incrementing numeric id. This id starts at zero, and increments to the number of the test cases in the procedure (minus one). You can skip to a particular test case at any time using the start parameter in the studio or console. When a start value is supplied, the fuzzer spins through the seeded random number generator and all of the test frames quickly without transmitting them. This ensures that you get the exact same frame within the procedure as if you had run through all the preceding tests.

Other configurable generic test options are described in the studio section of the documentation.

Communications

Aegis uses an abstract channel interface internally. Tests are unaware of how they are communicating with the target. You need to refer to your specific protocol and ensure that you have configured the communications appropriately. This release supports the following channels:

- TCP client (default)
- TCP server
- Serial

For more information about Aegis Fuzzer see https://www.automatak.com/aegis/

3.5.2 About IEC 60870-5-104

IEC 104 is the European cousin of DNP3. It is more complex than Modbus, but a good bit simpler than DNP3. It consists of two layers:

- APCI - Application Protocol Control Information used to denote frame types for 104's network mode.
- ASDU - Application Service Data Unit that contains application layer frames. This is the same for 101 and 104.

The application layer defines a number of Type Ids which can be thought of as function codes. They define the format of the data that follows. Unlike in DNP3, 104 ASDUs can only contain one type of data.

Functions supported

The 104 fuzzer provides support for every TypeId defined in the standard. This doesn't guarantee that all possible bugs will be found, but it does mean there that a significant portion of the application layer is stressed by the fuzzer.

Health checks

The fuzzer queries the device under test (DUT) by sending a U-format frame with TESTFR ACT and expects to receive TESTFR CON in response.

Conformance and parameters

Some parameters in IEC 104 have configurable sizes that both sides must agree upon. Aegis uses the following values:

- A two-octet Cause of Transmission field is used where the one-byte sender address sub-field is utilized.
- A two-octet Common Address field is used.
- A three-octet Information Object Address field is used.

There are the defaults for almost all systems, and the only settings that work with Wireshark.

Handshaking

The fuzzer automatically advances and increments the Transmit and Receive Sequence Numbers in the APCI.

The fuzzer will send (outstation/slave) or receive (master) START_DT automatically.

The fuzzer always answers TESTFR ACT with TESTFR CON.

Parameters

- sender-addr - Sender (Originator) address - The address placed in all 1-octet cause of transmission sender address fields.
- common-addr - Common address (sector) - The common address, or sector, of the DUT.
- retries - Number of health-check retries - The number of attempts the fuzzer will make to query the target with a health check before deciding it has failed.
- timeout - Health-check timeout - The timeout (in milliseconds) for reading a link layer frame from the target during a health-check.

Procedures (outstation/slave)

- app-request - Fuzzes the server's application layer with mutated forms of request TypeIds.
- rand-app-request - Fuzzes the server's application layer with random semi-random requests.

Procedures (master)

- app-response - Fuzzes the client's application layer with mutated forms of response TypeIds
- rand-app-response - Fuzzes the client's application layer with random semi-random responses.

Procedures (either master or outstation/slave)

The following procedures send frames with malformed APCI. You will almost certainly need to run each test case in its own TCP session (i.e. tests-per-session == 1).

- apci - Sends malformed I, U, or S frames with disallowed lengths and a configurable random payload length.
- random-frame - Sends a completely random frame prepended with the 0x68 start characters.

Test Plans

Your Aegis installation of contains recommended test plans for both outstations/slaves and masters.

- plans\iec104-outstation.xml
- plans\iec104-master.xml

In most cases, the only parameter you need to adjust will be the common address.

The recommended test plan repeats some of the procedures with different fill or random seeds. It is recommended that you follow the plan for maximum efficacy, but on slow implementations, this could take a long time. Some implementations can handle hundreds of test cases per second, while others only seem to handle a couple dozen. It may be worth figuring out why the implementation is slow to respond to health checks or requests. You might consider running additional random seeds besides zero if your have enough time.

The last test case in each plan generates random application layer data within appropriate encapsulation. It is arbitrarily set to 250,000 iterations. Run as many iterations as you can tolerate with the speed of your device.

3.5.3 Hint

Actual protocol fuzzing is applied only to IEC 104 protocols.

4 The Security Testing

Contents

4.1 Secure Testing Concept

The above described testing tools are used for performing security tests at SICAM RTUs LAN interfaces.

The security tests are part of system tests, the whole system tests in detail is documented at a separate master test report.

At a PC-based system (which is used for testing) during performing the tests an virus scan must be switched off.

When the test is finished, a system restart of DUT is necessary!

A successful test will result in a “Certificate of Security Conformity”, see chapter 2.

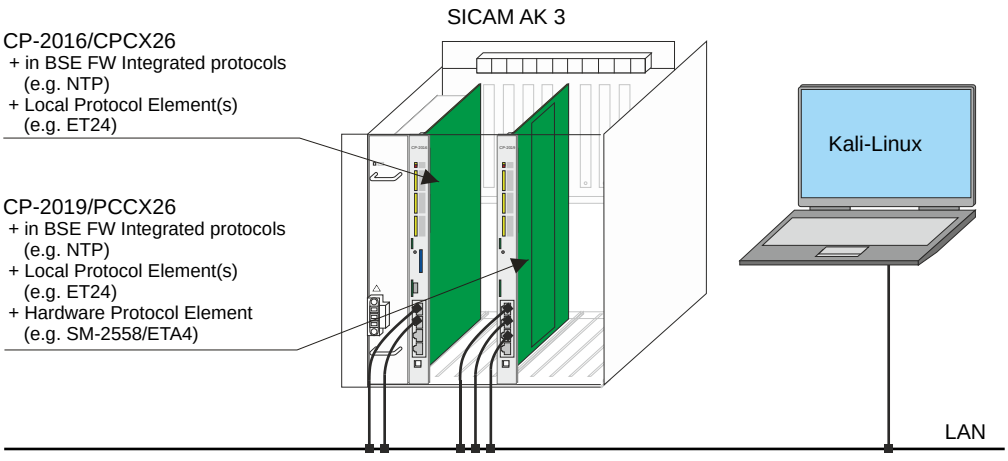
IPSec VPN: penetration test is done

- inside VPN tunnel
- from outside (remote site) into VPN tunnel

We do not test the following services:

- TBII remote operation (Proprietary: port 2001)
  this is legacy, we test TBII remote operation https
- SNTP, we test NTP
- http, we test https

4.1.1 Protocol Elements on SICAM AK 3



Security testing is done at all SICAM AK 3 LAN interfaces.

Protocols integrated in BSE Firmware

Integrated in	Service	Mausezahn	nmap	NESSUS	Fuzzing
CP-2016/CPCX26	NTP-Server	x	x	x	-
	https – TBII-remote operation	x	x	x	-
	SNMP	x	x	x	-
	IPSec VPN	x	x	x	-
	Syslog client	x	x	x	-
CP-2019/PCCX26	NTP-Server	x	x	x	-
	https – TBII-remote operation	x	x	x	-
	IPSec VPN	x	x	x	-
	Syslog client	x	x	x	-

Local Protocol Elements

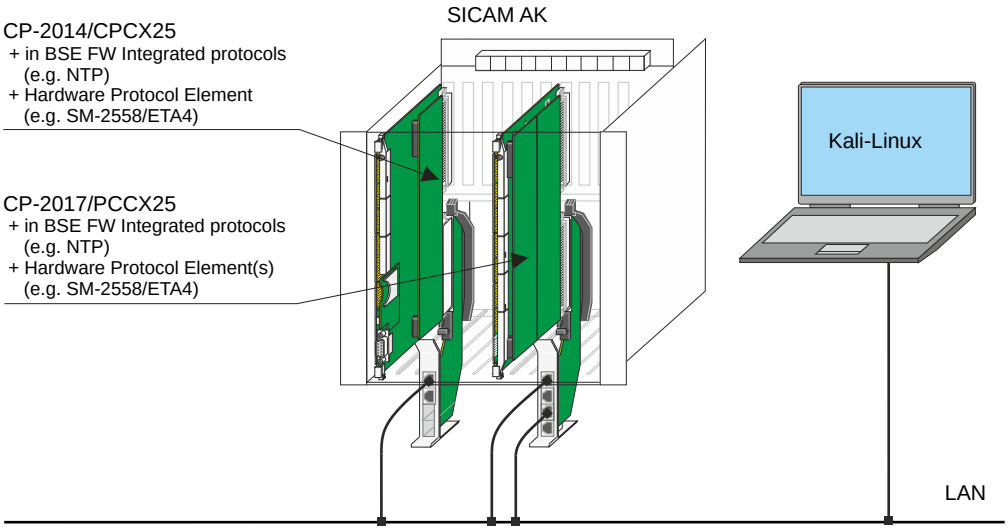
All services via BSE

Designation	Service	Mausezahn	nmap	NESSUS	Fuzzing
ET24	IEC 60870-5-104	x	x	x	x
ET25	IEC 61850 Ed. 2	x	x	x	-

Hardware Protocol Elements

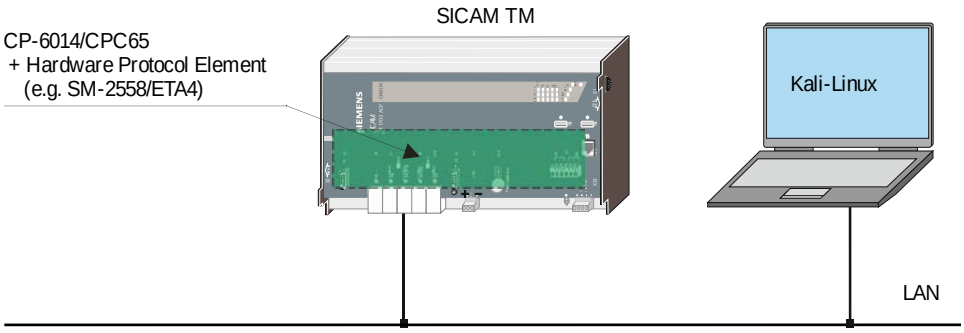
Designation	Service	Mausezahn	nmap	NESSUS	Fuzzing
SM-2558/ETA4	NTP-Server	x	x	x	-
	https – TBII-remote operation	x	x	x	-
	IEC 60870-5-104	x	x	x	-
	IPSec VPN	x	x	x	-
	Syslog Client	x	x	x	-
SM-2558/ETA5	NTP-Server	x	x	x	-
	https – TBII-remote operation	x	x	x	-
	https – WEB	x	x	x	-
	IEC 61850 Ed. 2	x	x	x	-
SM-2558/MBSiA0 (MODBUS TCP/IP Slave)	MODBUS TCP/IP	x	x	x	-
	https – TBII-remote operation	x	x	x	-
SM-2558/MBCiA0 (MODBUS TCP/IP Master)	MODBUS TCP/IP	x	x	x	-
SM-2558/DNPiA1 (DNP3 TCP/IP Slave)	DNP3 TCP/IP Slave	x	x	x	-
	https – TBII-remote operation	x	x	x	-

4.1.2 Protocol Elements on SICAM AK



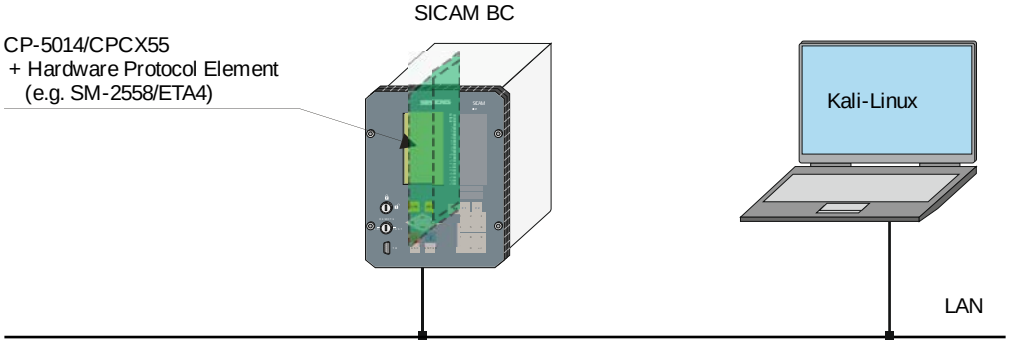
The protocols at SICAM AK are not tested separately, the SICAM AK 3 tests meet this requirements.

4.1.3 Protocol Elements on SICAM TM



SM-2558 at SICAM TM is not tested separately, the SICAM AK 3 tests meet this requirements.

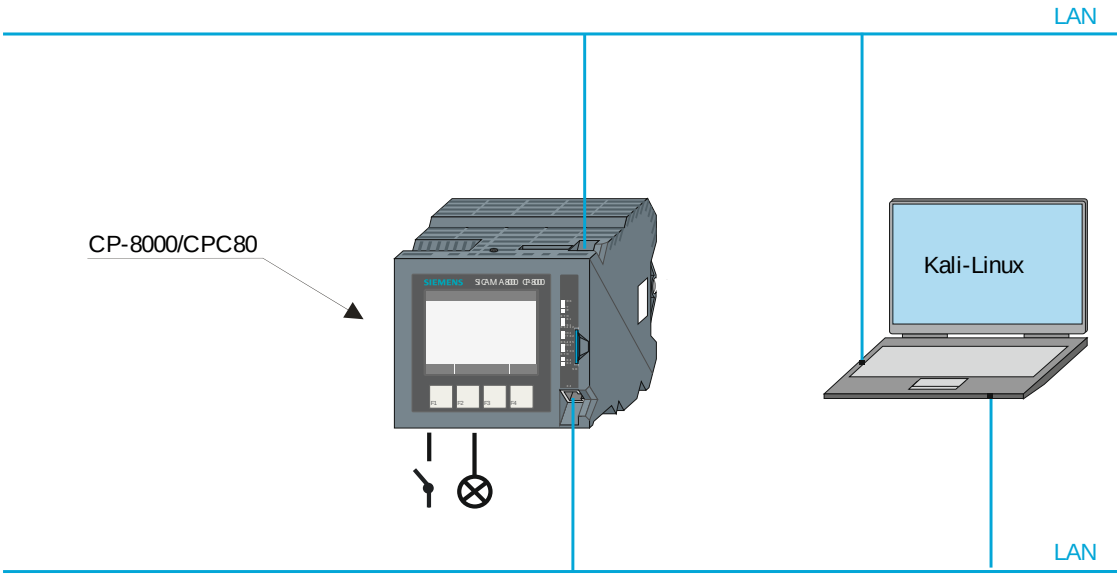
4.1.4 Protocol Elements on SICAM BC

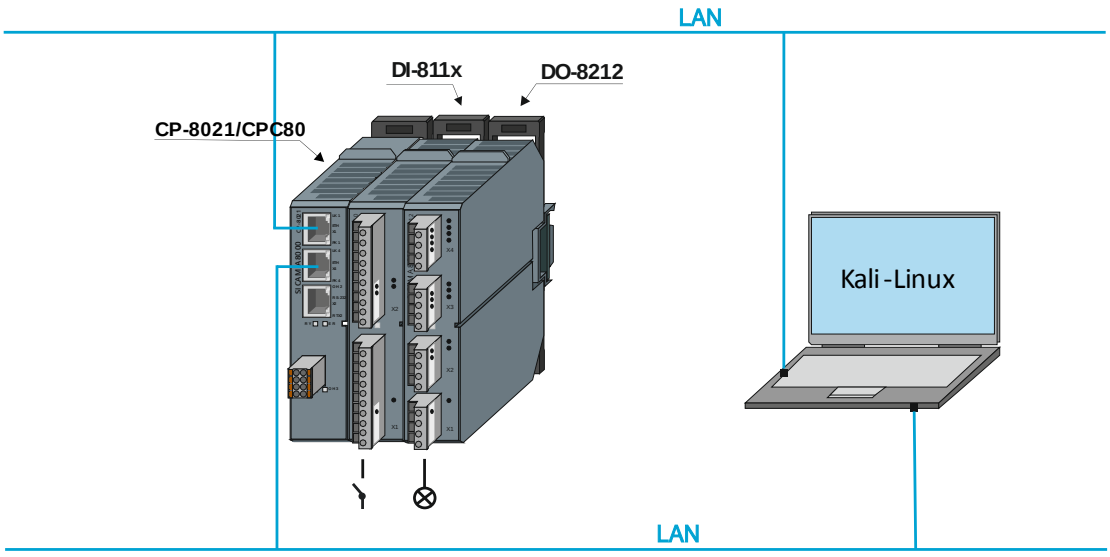


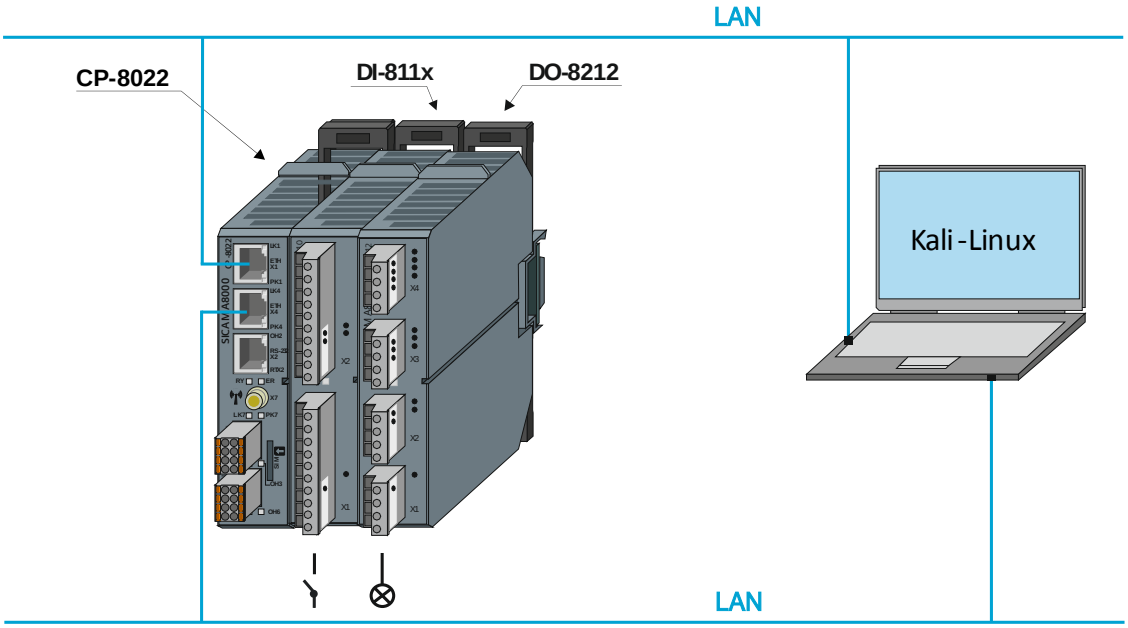
SM-2558 at SICAM BC is not tested separately, the SICAM AK 3 tests meet this requirements.

4.1.5 Protocol Elements on SICAM A8000 Series CP-8000/21/22

At SICAM A8000 Series CP-8000/21/22 a digital input and a digital output is configured.







Security Testing is done at all CP-8000/21/22 LAN interfaces.

Protocols integrated in BSE Firmware

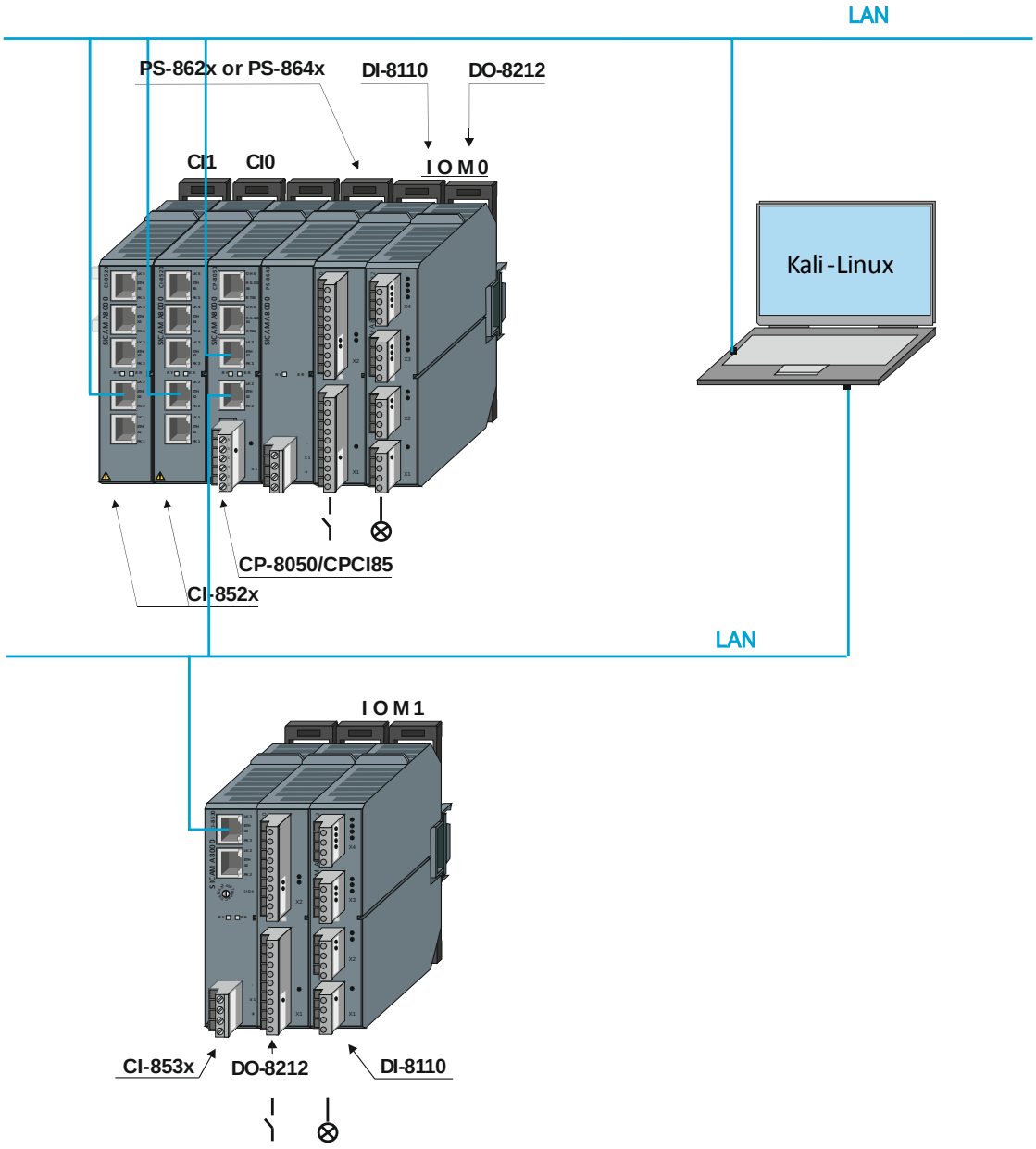
Integrated in	Service	Mausezahn	nmap	NESSUS	Fuzzing
CP-8000/CPC80 CP-8021/CPC80 CP-8022/CPC80	NTP-Server	x	x	x	-
	SNMP	x	x	x	-
	IPSec VPN, IKE	x	x	x	-
	Syslog-Client	x	x	x	-
	RADIUS authentication protocol	x	x	x	-
Application SWEB00 and/or	https – SICAM WEB	x	x	x	-
Application TBII-remote operation	https – TBII-remote operation	x	x	x	-

Local Protocol Elements

Designation	Service	Mausezahn	nmap	NESSUS	Fuzzing
ET84	IEC 60870-5-104	x	x	x	x
ET85	IEC 61850 Ed. 2	x	x	x	-
DNPiT1	DNP3 TCP/IP Slave	x	x	x	-

4.1.6 Protocol Elements on SICAM A8000 Series CP-8050

At SICAM A8000 Series CP-8050 a local digital input and digital output as well as an Ethernet based IO digital input and digital output is configured.



IEC 60870-5-104- server will be configured once at CP-8050 X3, once at CI0 and once at CI1. All three interfaces are testet as well as the Ethernet Based IO Interface.

Security Testing is done at all CP-8050 LAN interfaces.

Protocols integrated in BSE Firmware

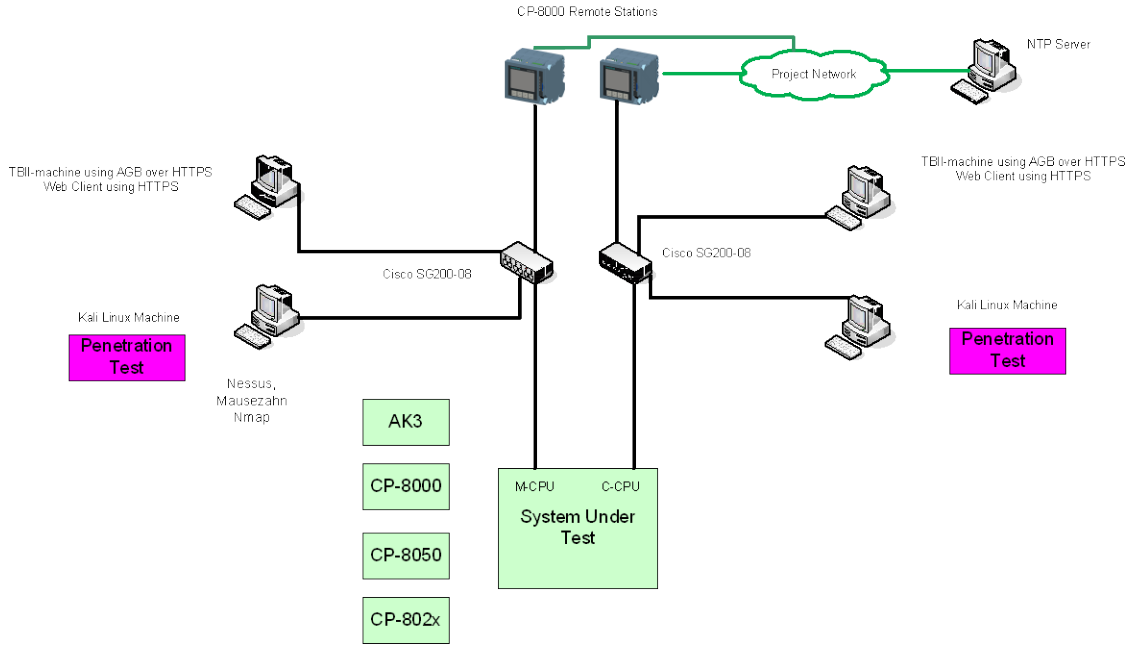
Integrated in	Service	Mausezahn	nmap	NESSUS	Fuzzing
CP-8050/CPCI85	NTP-Server	x	x	x	-
	SNMP	x	x	x	-
	IPSec VPN, IKE	x	x	x	-
	Syslog-Client	x	x	x	-
	RADIUS authentication protocol	x	x	x	-
Application SWEB00 and/or	https – SICAM WEB	x	x	x	-
Application TBII-remote operation	https – TBII-remote operation	x	x	x	-

Local Protocol Elements

Designation	Service	Mausezahn	nmap	NESSUS	Fuzzing
ETI4	IEC 60870-5-104	x	x	x	x
ETI5	IEC 61850 Ed. 2 http(s), Web.Server (WEB-page)	x	x	x	-

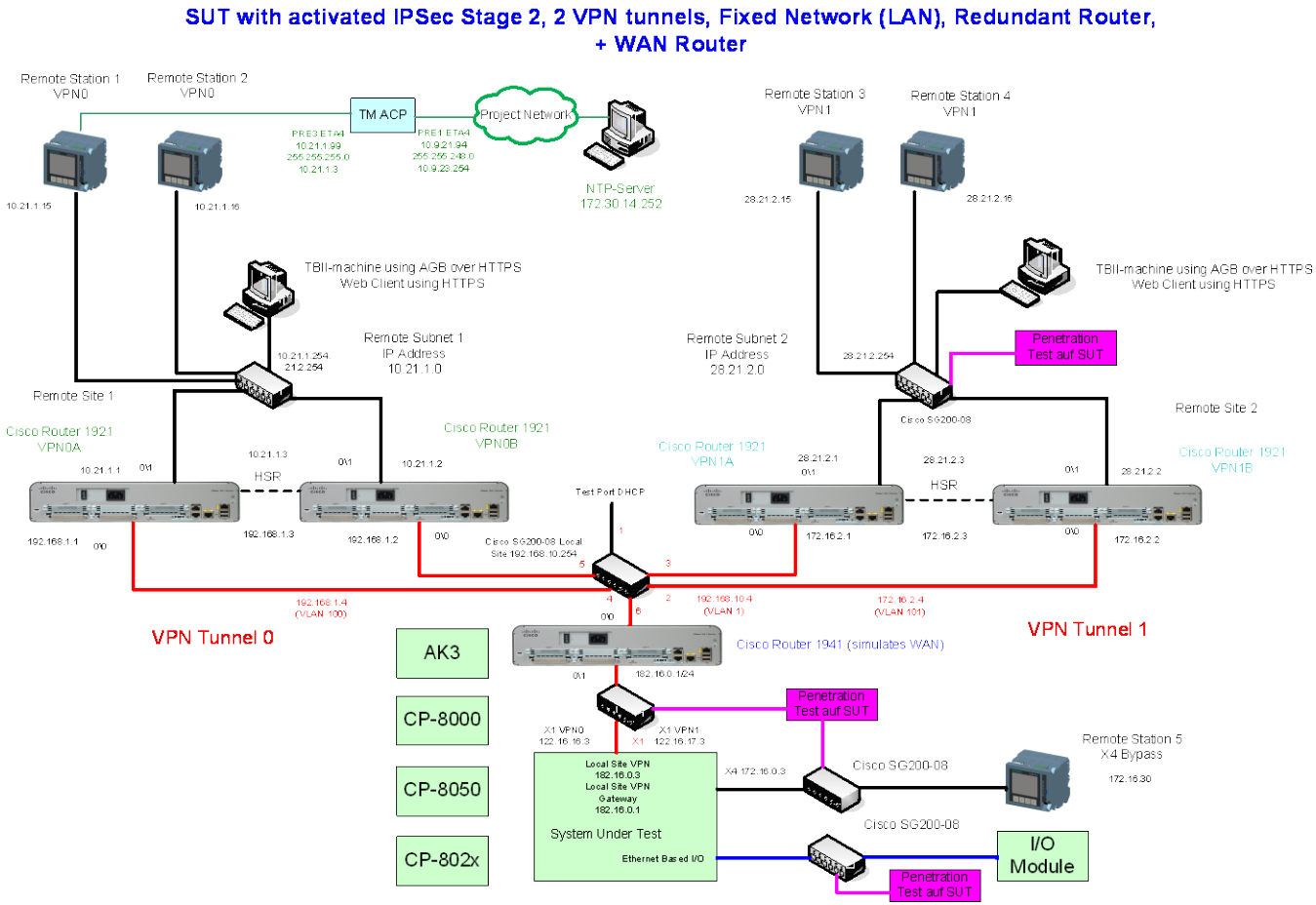
4.1.7 Test Configuration without IPSec

Topology Penetrationtest SICAM RTUs



4.1.8 Test Configuration with IPSec

Topology Penetrationtest SICAM RTUs



4.1.8.1 Test Configuration Parameters

Simply equip a new AU, and configure parameters as listed below. All available Services (listener ports) must be enabled.

Service/Function	Add. Info	SICAM AK 3									CP-8000 CP-802x				CP-8050			
		CPCX26	PCCX26	ET24	ET25	ETA4	ETA5	MBSiA0	MBCiA0	DNPiA1	CPC80	ET85	ET84	DNPiT1	CPCI85	ETI4	ETI5	DNPiT1
One Click to Connect	enabled	-	-	-	-	-	-	-	-	-	-	-	-	-	x	-	-	-
Security	https	x	x	-	-	x	x	x	x	x	x	-	-	-	x	-	-	-
TOOLBOX II remote operation	enabled	x	x	-	-	x	x	x	-	x	x	-	-	-	x	-	-	-
SICAM WEB (SWEB00)	enabled	-	-	-	-	-	-	-	-	-	x	x	-	-	x	x	-	-
Web-Server (WEB-page)	enabled (only if available)	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-	-
NTP Server	enabled	x	x	-	-	x	x	-	-	-	x	-	-	-	x	-	-	-
SNMP	enabled	x	-	-	-	-	-	-	-	-	x	-	-	-	x	-	-	-
IEC 60870-5-104 Server	configured, Connection to IEC 60870-5-104 Client	-	-	x	-	x	-	-	-	-	-	-	x	-	-	-	x	-
IEC 61850 Ed. 2 Server	configured, Connection to IEC 61850 Client	-	-	-	x	-	x	-	-	-	-	x	-	-	-	x	-	-
MODBUS TCP/IP Master	configured, Connection to MODBUS TCP/IP Master	-	-	-	-	-	-	-	x *)	-	-	-	-	-	-	-	-	-
MODBUS TCP/IP Slave	configured, Connection to MODBUS TCP/IP Slave	-	-	-	-	-	-	x	-	-	-	-	-	-	-	-	-	-
DNP3 TCP/IP Slave	configured, Connection to DNP3 TCP/IP Master	-	-	-	-	-	-	-	-	x	-	-	-	x	-	-	-	x
IPSec VPN	enabled	x	x	-	-	x	-	-	-	-	x	-	-	-	x	-	-	-
RADIUS authentication protocol	enabled	-	-	-	-	-	-	-	-	-	x	-	-	-	x	-	-	-
Syslog client	enabled	x	x	-	-	x	-	-	-	-	x	-	-	-	x	-	-	-

*) only client service, but basic test must be done

4.2 Test Description

4.2.1 Stress Test

Stress test is done using MZ Mausezahn.

During test the tested device must not fail ! When Test is finished, the Services still must work.

Note

Several times the communication fails.
this is valid, if the communication works well when the test was finished (10 minutes wait time).

4.2.1.1 MZ Mausezahn Test

A randomized MZ test is performed using a bandwidth rate of SPEED=("xMbit"), see list below. The configured speed will be measured using iptraf.

The scanned TCP ports are: PORTS=("80" "102" "443" "123" “500” "2001" "2404" “4500”).

4.2.1.1.1 Test Data Rate

MZ Mausezahn test bandwidth rates, specified for the different tested hardware:

Hardware	Firmware	SPEED (data loss allowed)
CP-2016	CPCX26 (w/o IPSec)	100 Mbit
	CPCX26 (with IPSec)	100 Mbit
CP-2019	PCCX26 (w/o IPSec)	100 Mbit
	PCCX26 (with IPSec)	100 Mbit
SM-2558	ETA4 (w/o IPSec)	100 Mbit
	ETA4 (with IPSec)	100 Mbit
	ETA5	100 Mbit
	MBSiA0	100 Mbit
	MBCiA0	100 Mbit
	DNPiA1	100 Mbit
CP-8000/21/22	CPC80 (w/o IPSec)	100 Mbit
	CPC80 (with IPSec)	100 Mbit
CP-8050	CPCI85 (w/o IPSec)	100 Mbit
	CPCI85 (with IPSec)	100 Mbit

4.2.1.1.2 Security Test Precondition

Equip a DUT as described in chapter 4.1.8.1.

Set up one connection per 104 / 61850, connect with TBII remote operation, and disconnect.

4.2.1.1.3 Stress Test (data loss allowed, but system must recover)

At diagnosis (TOOLBOX II) all errors are reset.

Communicating with a communication partner (test system).

This test will be performed about 1 hour. When the test has ended (MZ stopped), 10 minutes later the system must recover. Then the DUT communicates with a communication partner.

The diagnosis (TOOLBOX II) shows that there was no board failure.

4.2.1.1.4 MZ Mausezahn Test Script

The MZ test script “SICAMRTUsMZtest.sh” is used. The MZ test script is provided on request, it is part of the master test report.

Note

Adapt the test bandwidth rates SPEED=("xMbit") at MZ script, according to specified data rate (see 4.2.1.1.1)

4.2.2 Port Scan

Port Scan is done with different Tools.

During test the communication must be configured, but not connected. The test system is switched off.

During test the tested device must not fail!

Note

Several times the tested device recognizes a IP-connection setup by a unknown communication partner. This is valid.

4.2.2.1 Hint

For the purpose of system hardening verification, the Port Scan will also be done with deactivated firewall.

4.2.2.2 Available Ports

Protocol or System -Element		Protocol	Port
CP-2016/CPCX26		https	TCP port 443
		NTP Server	UDP port 123
		SNMP SNMP Trap	UDP port 161 UDP port 162
		IKE (IPSec VPN)	UDP port 500 UDP port 4500
		Syslog Client	UDP port 514
	ET24	IEC 60870-5-104	TCP port 2404
	ET25	IEC 61850 Ed. 2	TCP port 102
	SM-2558/ETAx	see below	see above
CP-2019/PCCX26		https	TCP port 443
		NTP Server	UDP port 123
		IKE (IPSec VPN)	UDP port 500 UDP port 4500
		Syslog Client	UDP port 514
	ET24	IEC 60870-5-104	TCP port 2404
	ET25	IEC 61850 Ed. 2	TCP port 102
	SM-2558/ETAx	see below	see above
SM-2558/ETA4		IEC 60870-5-104	TCP port 2404
		https	TCP port 443
		NTP Server	UDP port 123
		IKE (IPSec VPN)	UDP port 500 UDP port 4500
		Syslog Client	UDP port 514
SM-2558/ETA5		IEC 61850 Ed. 2	TCP port 102
		https	TCP port 443
		NTP Server	UDP port 123
SM-2558/MBSiA0		MODBUS TCP/IP Slave	TCP port 502
		https	TCP port 443
		NTP Client	UDP port 123
SM-2558/MBCiA0		MODBUS TCP/IP Master	TCP port 502
SM-2558/DNPiA1		DNP3 TCP/IP Slave	TCP port 20000
		https	TCP port 443
		NTP Client	UDP port 123

CP-8000/21/22	Protocol	Port
CP-8000/21/22/CPC80	NTP Server	UDP port 123
	SNMP SNMP Trap	UDP port 161 UDP port 162
	IKE (IPSec VPN)	UDP port 500 UDP port 4500
	Syslog Client	UDP port 514
	RADIUS	TCP port 1812
Application SWEB00 and/or Application TBII-remote operation	https	TCP port 443
Application/ET8x:		
ET84	IEC 60870-5-104	TCP port 2404
ET85	IEC 61850 Ed. 2	TCP port 102
DNPiT1	DNP3	TCP port 20000

CP-8050	Protocol	Port
CP-8050/CPCI85	DNS Server	UDP port 53 *1)
	DHCP Server	UDP port 67 *2)
	NTP Server	UDP port 123
	SNMP SNMP Trap	UDP port 161 UDP port 162
	IKE (IPSec VPN)	UDP port 500 UDP port 4500
	Syslog Client	UDP port 514
	RADIUS	TCP port 1812
Application SWEB00 and/or Application TBII-remote operation	https	TCP port 443
Application/ET8x:		
CI-8520	IEC 60870-5-104	TCP port 2404
CI-8520	IEC 61850 Ed. 2	TCP port 102
DNPiT1	DNP3	TCP port 20000

*1) The feature *One Cick to Connect* will not be tested. This feature is designed for first commissioning.

It is recommended to disable this feature in case of deployment of the device in exposed environment.

*2) DHCP enabling under
System settings | Network settings | Interface | DHCP server enable

Only the ports of configured services are allowed to be open.

The port matrix is described in the security SICAM TOOLBOX II ADMINISTRATOR Security-Manual /2/.

4.2.2.3 Security Test Precondition

Equip a DUT as described in chapter 4.1.8.1.

Set up one connection (SERVER) per 104 / 61850, but do not set up a communication partner.

4.2.2.4 NMAP

A port scan will be done for TCP only:

TCP port scan:

nmap -A -p 1-65535 dest-ip

UDP port scan:

Nmap is not used for UDP scan, but nessus vulnerability scan will be done for these ports (configured at nessus manually):

DNS-Server
DHCP-Server
NTP-Server
SNMP
IPSec 500+4500

Note for UDP:

"Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible." (https://docs.tenable.com/nessus/6_5/Content/_New_Topics/Discovery.htm)

For the purpose of system hardening verification, the vulnerability scan will also be done with deactivated firewall for full TCP and UDP port range.

4.2.2.5 Nessus

Nessus is a vulnerability scanner, but it is also used for port scan.

The port scan is the first test step of a Nessus scan, see also 4.2.3.1

4.2.2.6 TOOLBOX II Remote Operation

Connect to the DUT using SICAM TOOLBOX II remote operation.

First connect to the AU and set a Connection Password at AU, then disconnect. Secondly connect again to the DUT using SICAM TOOLBOX II remote operation. The DUT requests a “Connection Password”, without the “Connection Password” SICAM TOOLBOX II remote operation can not setup a connection to AU.

The function „Connection Password“ is not available for SICAM A8000 Series CP-8050. The connection to the device is supervised by „Role-Based-Access“ (RBAC).

4.2.3 Vulnerability Scan

The vulnerability scan is done using NESSUS; NESSUS is used in a Kali Linux machine.

4.2.3.1 Nessus Scan

The first test step of a Nessus scan is a port scan.

The test is performed once.

During test the communication must be configured, but not connected. The test system is switched off.

During test the tested device must not fail !

Note

Several times the tested device recognizes an IP-connection by an unknown communication partner. This is valid.

4.2.3.1.1 Security Test Precondition

Equip a DUT as described in chapter 4.1.8.1.

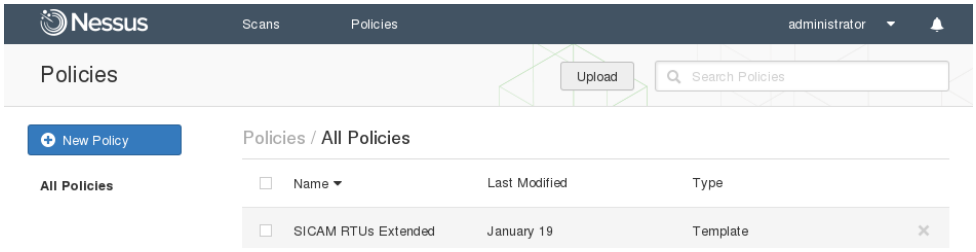
Set up one connection (SERVER) per 104 / 61850. The test system is switched off.

4.2.3.1.2 Hint

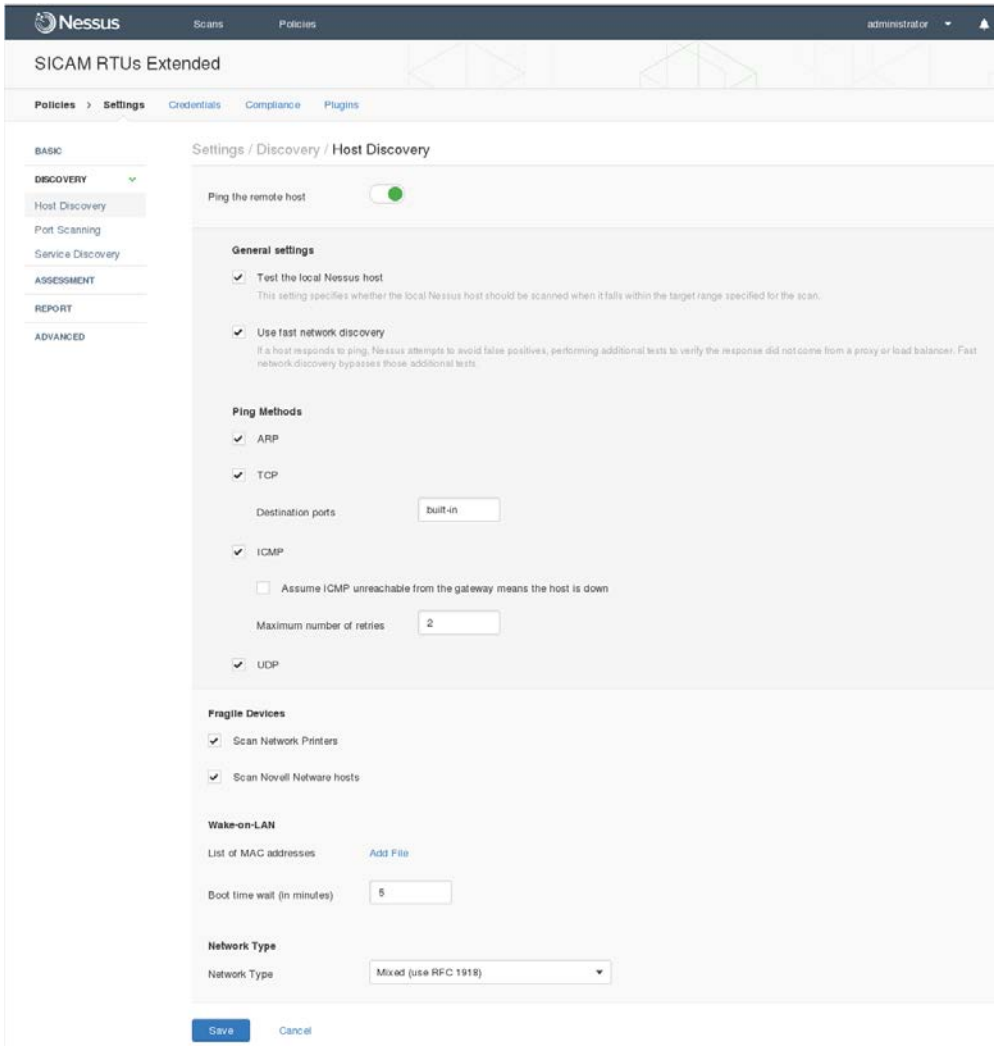
For the purpose of system hardening verification, the vulnerability scan will also be done with deactivated firewall for full TCP qand UDP port range.

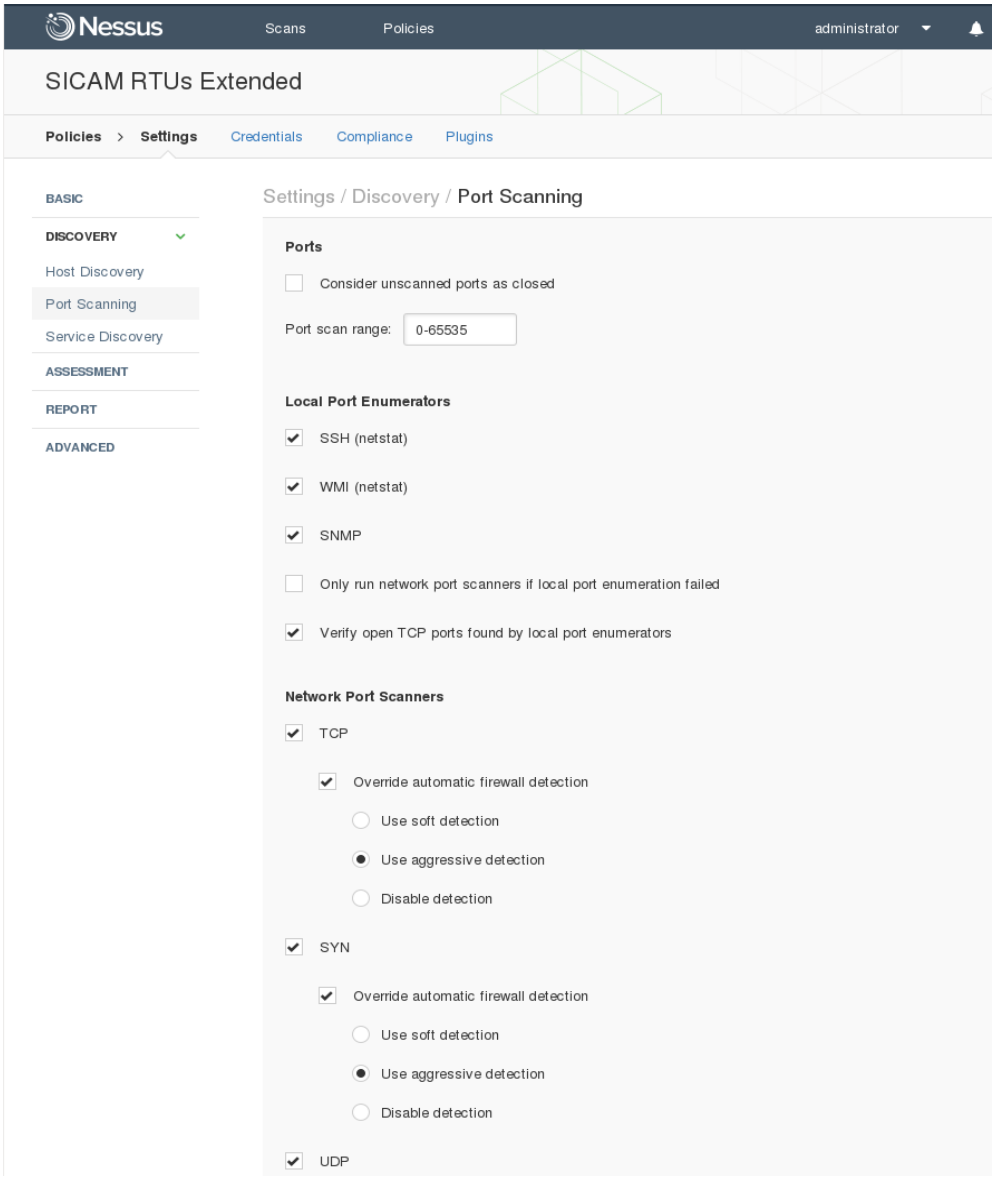
4.2.3.1.3 Configuration of Nessus

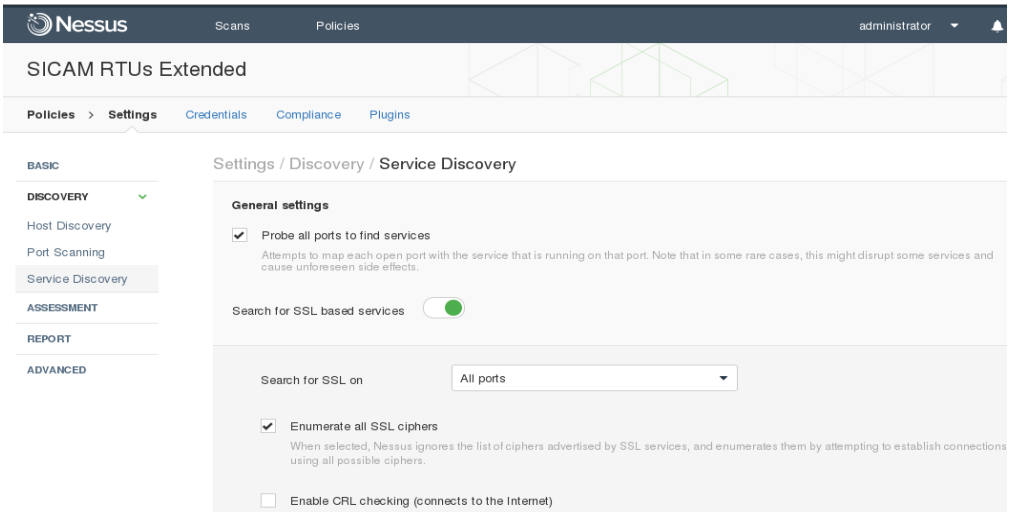
First step is to upload the scan policy:



Secondly configure the Policy / Discovery Settings:

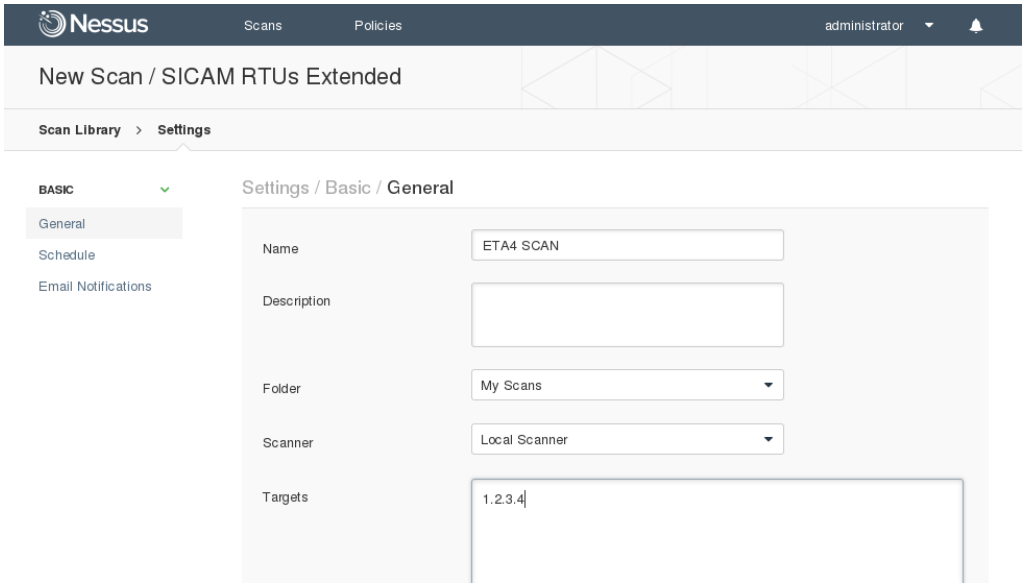




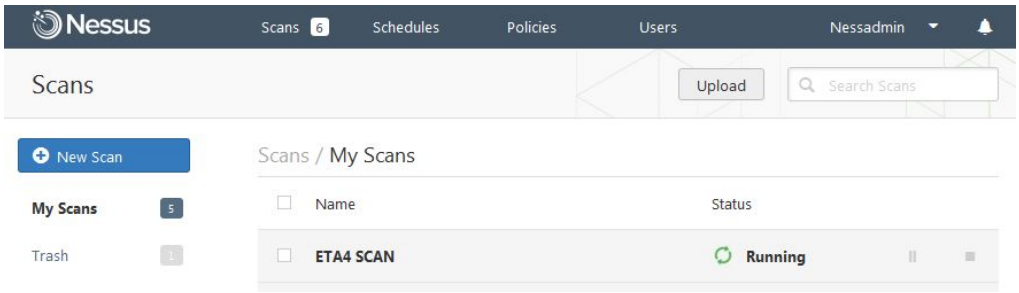


Hint:
If the NESSUS scan is done several times, the port scan can be temporary disabled.

Then a new Scan is configured:



Simply Start the Scan:



4.2.3.1.4 Scan Policy

The vulnerability scan is performed, using the the “SICAM_RTUs.nessus” scan policy. The policy is provided in request, it is part of the master test report.

4.2.4 Protocol fuzzing

Protocol fuzzing is done using Aegis™.

4.2.4.1 Aegis™ Protocol Fuzzer

4.2.4.1.1 Security Test Precondition

Equip a DUT as described in chapter 4.1.8.1.

SICAM device is controlled (server) remote station, Aegis™ Protocol Fuzzer is controlling (client)

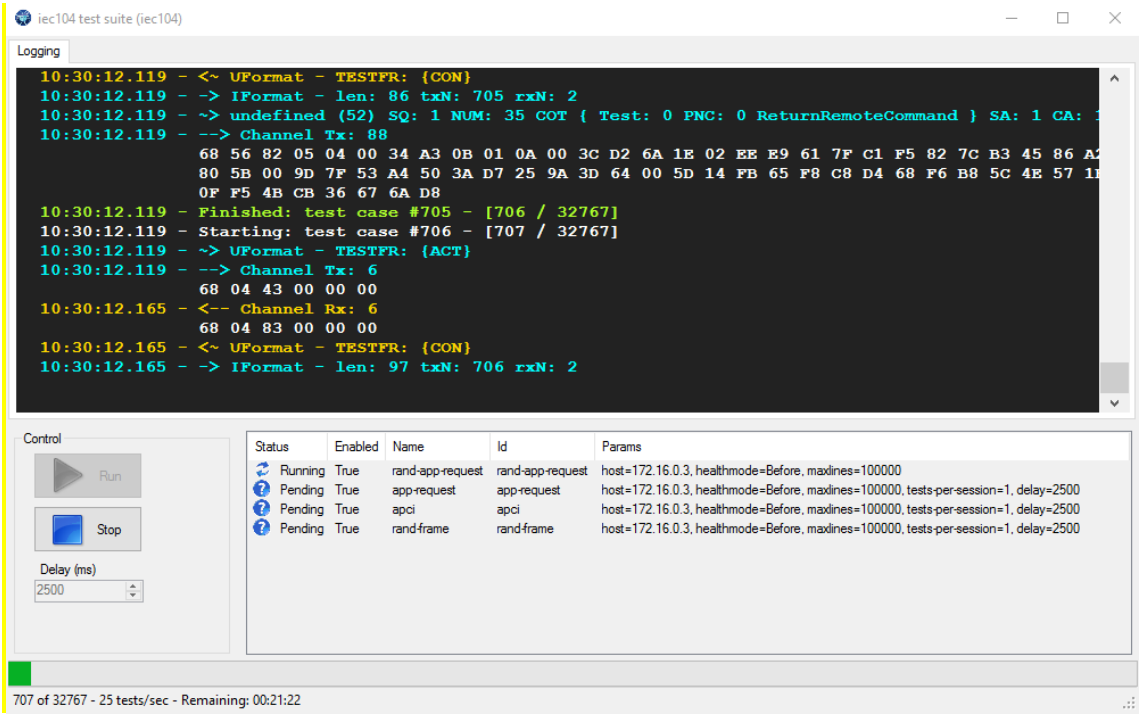
4.2.4.1.2 Configuration of Aegis™ Protocol Fuzzer

Parameterize 104 communication of sicam device to controlled (server) remote station.

Ip address = ip-address of machine running aegis studio

- Start aegis studio
- Load test configuration
- File | load → aegis_sicam1703_controlled.xml
- Select test suite | options
  edit tcp host (=ip address of sicam device)
- Select test suite | open
- Edit delay (ms): 2500

RUN:
all available predefined test procedures are executed.



Expected result:

Communication errors after the tests are finished.

Note

Only 104 communication of sicam device to controlled (server) remote station is part of this test.

4.2.4.1.3 Scan Policy

The fuzzing is performed, using the the “aegis_sicam1703_controlled.xml” policy. The policy is provided in request, this is part of the master test report.

5 Glossary

104	IEC 60870-5-104
61850	IEC 61850 Edition 1
61850 Ed. 2	IEC 61850 Edition 2
AU	Automation Unit
BSE	Basic System Element
C	BSE, Additional CPU
CPU-Type	type of processing unit
DUT	Device Under Test
FW	Firmware
HW	Hardware
IKE	Internet Key Exchange
IPSEC	Internet Protocol Security (IPsec)
HTTP	Hypertext Transfer Protocol
HTTPs	HTTP Secure
MZ	Mausezahn – Traffic generator
M	BSE, Main CPU
NTP	Network Time Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TBII	SICAM TOOLBOX II Engineering Tool
TBII-remote	TBII remote operation
TLS	Transport Layer Security
Virtual	Firmware equipable, no special hardware necessary
WEB	WEB-browser: we talk about WWW, the world wide web
ZSE	Additional System Element

6 References

/1/ **BSI-Studie "Durchführungskonzept für Penetrationstests**“
https://www.bsi.bund.de/DE/Publikationen/Studien/pentest/index_htm.html

/2/ SICAM RTUs – SICAM TOOLBOX II
ADMINISTRATOR Security-Manual (DC0-115-2)

--- end of document ---