Why are cybersecurity and functional monitoring for substations critical?

Cybersecurity and Functional Monitoring for Substations Webinar

OMICRON

Our Motivation

- We have been active in network communication in the power grid for 20 years
- Cybersecurity is a new problem for our well-known customers
- Current security solutions speak a foreign language for protection and control engineers

Our Goal

- IT security officers and substation engineers should be able to work together efficiently.
- Cybersecurity systems should be *usable* and *useful* for IT *and* OT officers.

How to secure your substation/SCADA network?

- **Identify** the status quo
  - Identify the risk for cyberattacks; identify assets and their vulnerabilities
- **Protect** against the highest risks
  - Technical measures, but also organizational measures
- **Detect** threats and prohibited activity
  - Allows you to minimize damage and learn for next time
- **Respond** to detected threats
  - E.g., investigate security alerts
- **Recover**
  - E.g., clear malware from Gateways, or patch/replace IEDs

NIST CSF:
Basis for many national security guidelines

How to Identify your risk?

- Most guidelines[1] recommend keeping
  "*a current list of installed components and their properties*".

Why?

- Security advisories about substation devices are published frequently

- My substations are at risk if
  - certain device types with
  - certain firmware version and
  - in certain network setup
- are used.

[1] For example: **ISO 27001** A.8.1.1 and **IEC 62443**-3-3 SR7.8 and NIST SP 800-53 rev. 5, CM-8(2)

Recent examples:

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

ICS Advisory (ICSA-21-082-02)

3.1 AFFECTED PRODUCTS

The following firmware versions of MU320E are affected:

- All firmware versions prior to v04A00.1

ICS Advisory (ICSA-21-131-03)

3.1 AFFECTED PRODUCTS

The following Siemens Linux based products are affected:

- RUGGEDCOM RM1224: All versions between v5.0 and v6.4
- SCALANCE M-800: All versions between v5.0 and v6.4
- SCALANCE S615: All versions between v5.0 and v6.4
- SCALANCE SC-600: All versions prior to v2.1.3
- SCALANCE W1750D: v8.3.0.1, v8.6.0, and v8.7.0

ICS Advisory (ICSA-21-096-01)

4.1 AFFECTED PRODUCTS

- Relion 670 series Version 1.1, all revisions
- Relion 670 series Version 1.2.3, all revisions
- Relion 670 series Version 2.0, all revisions
- Relion 670/650 series Version 2.1, all revisions
- Relion 670/650 series Version 2.2.0, all revisions
- Relion 670/650/SAM600-IO series Version 2.2.1, all revisions
- Relion 670 series Version 2.2.2, all revisions
- Relion 670 series Version 2.2.3, all revisions
- Relion 650 series Version 1.1, all revisions
- Relion 650 series Version 1.2, all revisions
- Relion 650 series Version 1.3, all revisions
- RTU500 CMU firmware release 7.x
- RTU500 CMU firmware release 8.x
- RTU500 CMU firmware release 9.x
- RTU500 CMU firmware release 10.x
- RTU500 CMU firmware release 11.x
- RTU500 CMU firmware release 12.x

How to establish an asset inventory?

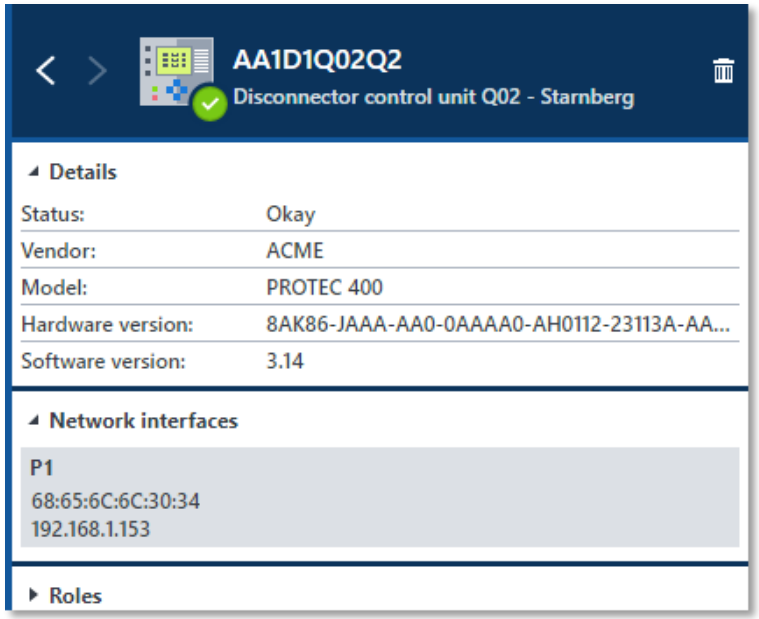
- **Manually**
  - Misses many “unexpected” devices
- **Passive** discovery
  - Only network card vendor, IP address and services used can be found out
  - Firmware version is not among them
- **Active** discovery using MMS
  - Firmware version
  - Type/model information
- **Using engineering file import** (SCL files)
  - Firmware version and HW config. directly entered by vendor engineering tool

IDENTIFY
CYBERSECURITY FRAMEWORK VERSION 1.1

OMICRON

Asset Inventory Discovery & Export

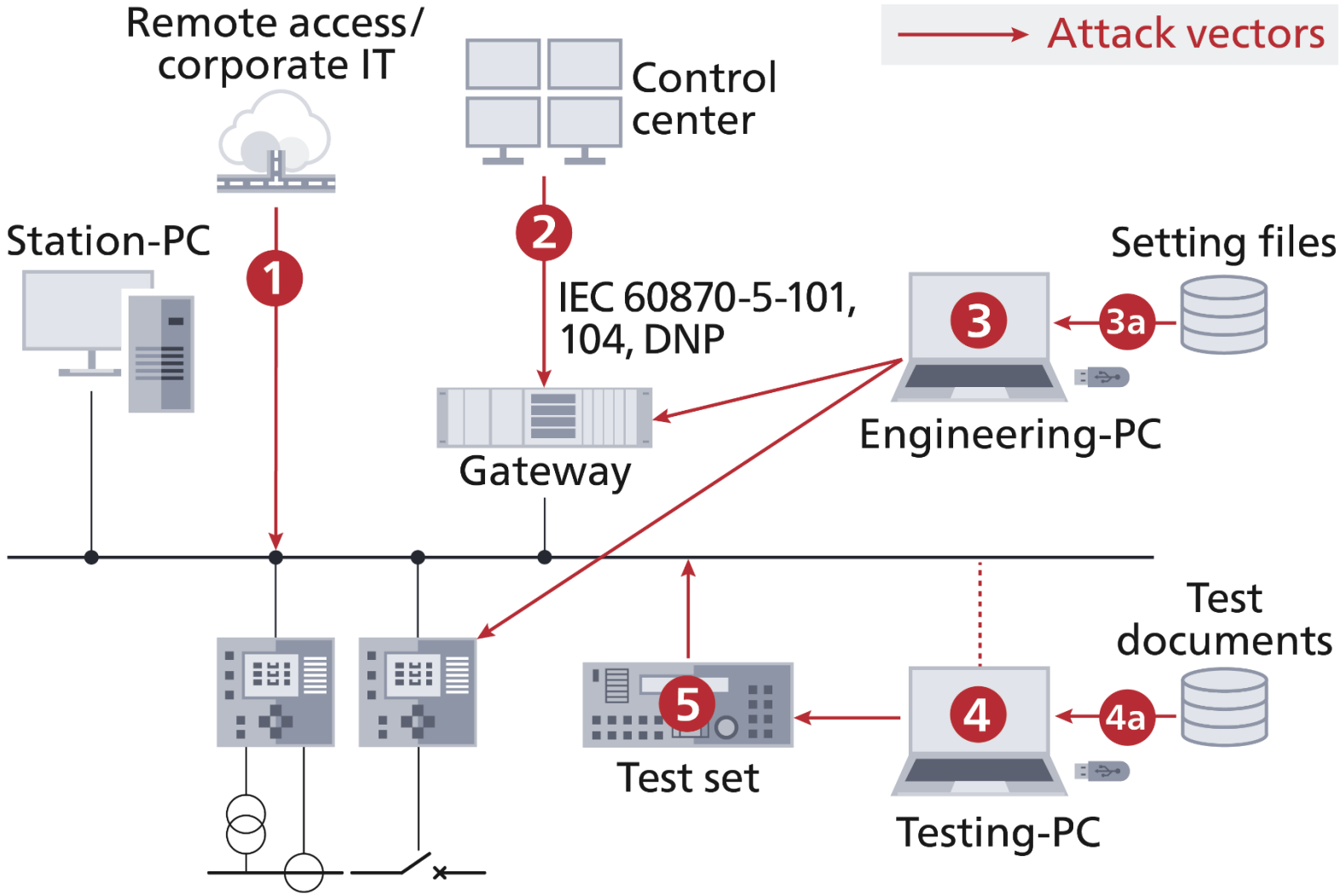
- Asset information collected from
  - Passive asset discovery
  - Engineering files – SCL
  - Active device interrogation (companion tool StationScout)



	A	B	C	D	E	F	G	H	I	J
1	Name	Description	Hardware version	Model	Serial	Softwa	Vendor	IP addresses	Origin	MAC addresses
2	AA1D1Q01Q1	Transformer infeed bay Q01	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.150	system_scd_v3.2	68:65:6C:6C:30:31
3	AA1D1Q02Q1	Bay control unit Q02 - Starnberg	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.152	system_scd_v3.3	68:65:6C:6C:30:33
4	AA1D1Q02Q2	Disconnector control unit Q02 - S	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.153	system_scd_v3.3	68:65:6C:6C:30:34
5	AA1D1Q03Q1	Bay control unit Q03 - Passau	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.154	system_scd_v3.3	68:65:6C:6C:30:35
6	AA1D1Q03Q2	Disconnector control unit Q03 - P	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.151	system_scd_v3.3	68:65:6C:6C:30:36
7	AA1D1Q04Q1	Transformer bay Q04	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.155	system_scd_v3.3	68:65:6C:6C:30:37
8	AA1D1Q05Q2	320kV measuring bay - Merging U		MU 300			ACME	192.168.1.157	system_scd_v3.3	68:65:6C:6C:30:39
9	AA1H1Q01Q1	Transformer 33kV bay Q01	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.160	system_scd_v3.3	68:65:6C:6C:30:32
10	AA1H1Q02Q1	Transformer 33kV bay Q02	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.161	system_scd_v3.3	68:65:6C:6C:31:30
11	BB_PROT	Busbar Protection	8AK86-JAAA-AA0-0AAAA0-AH0112-2311	PROTEC 400		3.14	ACME	192.168.1.173	system_scd_v3.3	68:65:6C:6C:30:30
12	HMI	IHMI		HMI 300			ACME	192.168.1.200	system_scd_v3.3	68:65:6C:6C:31:31
13	PCPQS1	Disturbance data collector		COLLEC 400			ACME	192.168.1.190	system_scd_v3.3	
14	RTU1	RTU for transformer bays		RTU 600			ACME	192.168.1.201	system_scd_v3.3	68:65:6C:6C:31:32
15	RTU2	RTU for feeder bays		RTU 600			ACME	192.168.1.202	system_scd_v3.3	68:65:6C:6C:31:33

OMICRON

How substations can be attacked (Attack Vectors)

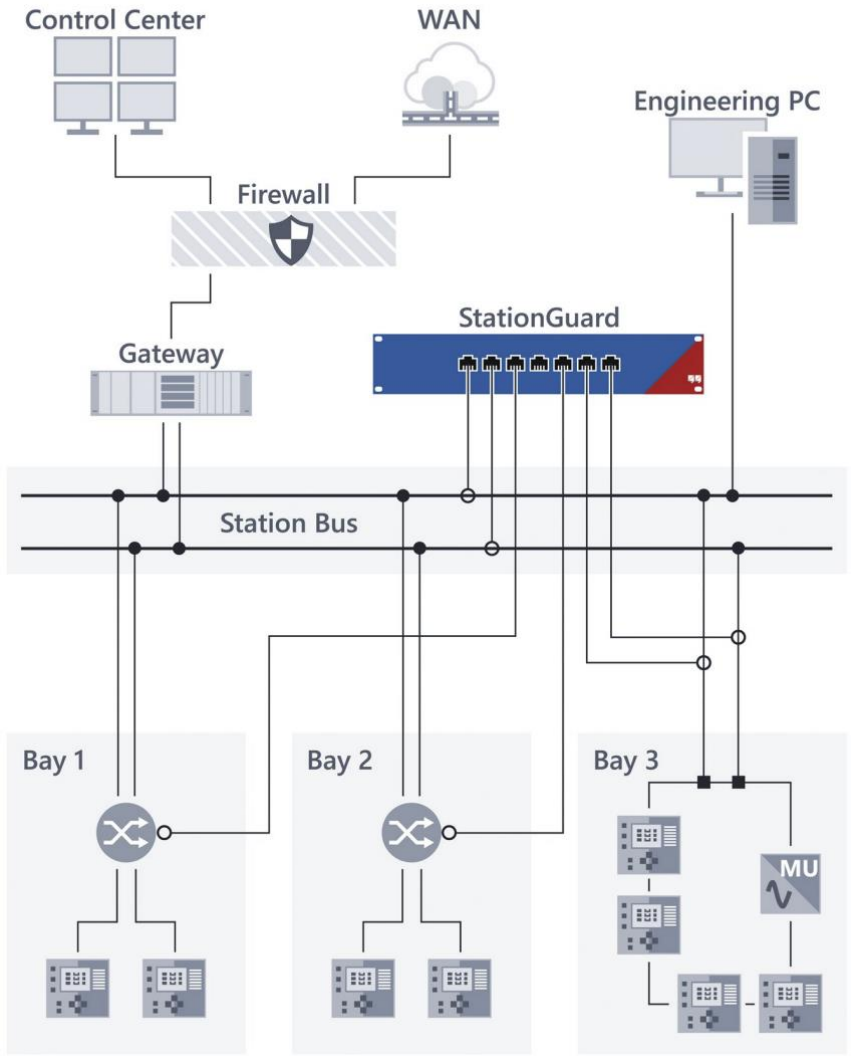


IDENTIFY
CYBERSECURITY
FRAMEWORK
VERSION 1.1

OMICRON

Countermeasure: Intrusion Detection Systems (IDS)

- History shows attacks often prepared **long before**
- Given enough time, attackers can always come through
- Detection allows to **respond** before damage is done
- Compromised devices **behave different** or fail

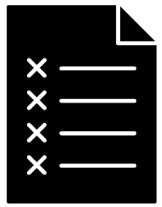


OMICRON

Problems of Current IDS

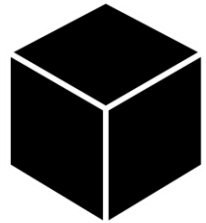
- **Signature**-based
  - PC virus scanner approach
  - Very few exploits/attacks known for our niche

Deny list



- **Baseline**-method, “learning-based”
  - Many false alarms: switching, maintenance, routine testing, ...
  - Complex alerts, because the IDS doesn’t understand the meaning of the messages

Black box



Difficult for to analyze,
even for experts

```
> ISO 8327-1 OSI Session Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8823 OSI Presentation Protocol
v MMS
  v confirmed-ResponsePDU
      invokeID: 36
    v confirmedServiceResponse: read (4)
      > read
```

OMICRON

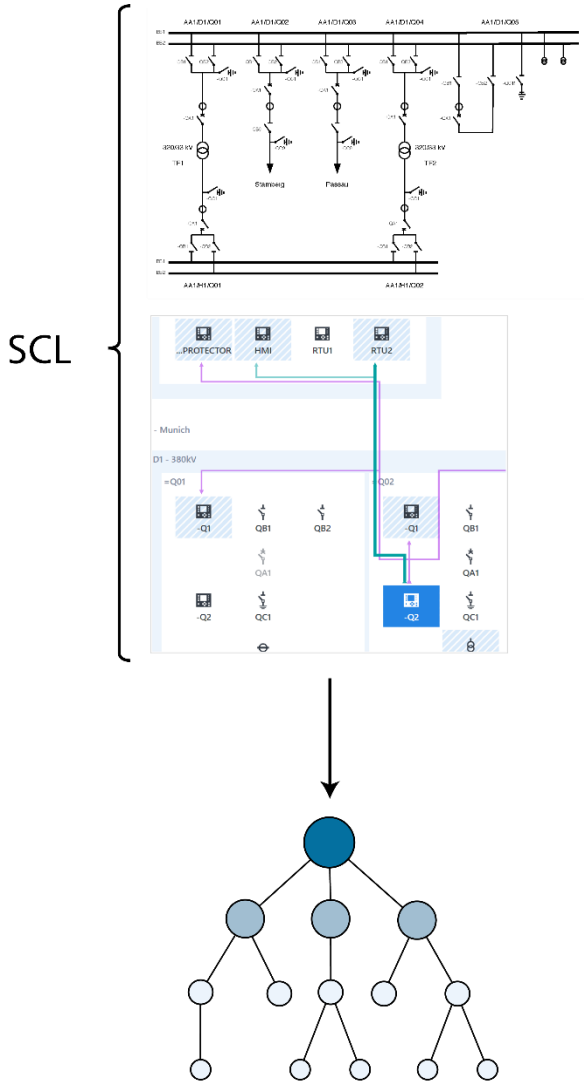
StationGuard Approach

StationGuard knows the substation

- Function of each device known from SCL or assigned roles
- Each packet evaluated against live system model
  - Allow list (whitelist) principle: alarm by default
- Maintenance and testing is part of system model

- Detailed verification of whole communication
- Detects not just cyber threats, but also malfunctions

Cyber Security Monitoring and Functional Monitoring



System model/allow list

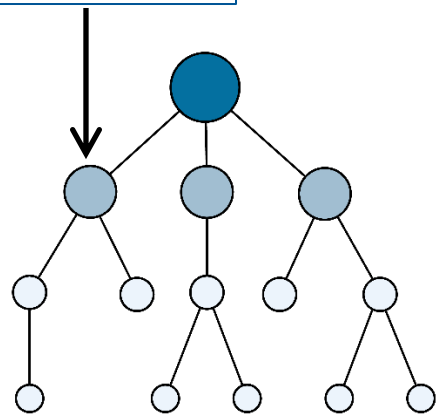
CYBERSECURITY FRAMEWORK VERSION 1.1
DETECT

OMICRON

What about other protocols?

- Modern substations: 98% of traffic is IEC 61850
  - Detailed system model approach possible
- Other protocols: DNP3, IEC-104, Modbus, FTP, HTTP ...
  - Deep packet inspection and application detection
- All connections must be allowed in the system model

Src./dest. MAC + src./dest. IP + VLAN + Port Number + **Application**



System model/ allow list

- Proprietary protocols protected by **Maintenance Mode**

OMICRON

Protocols with Deep Packet Inspection

OT Protocols

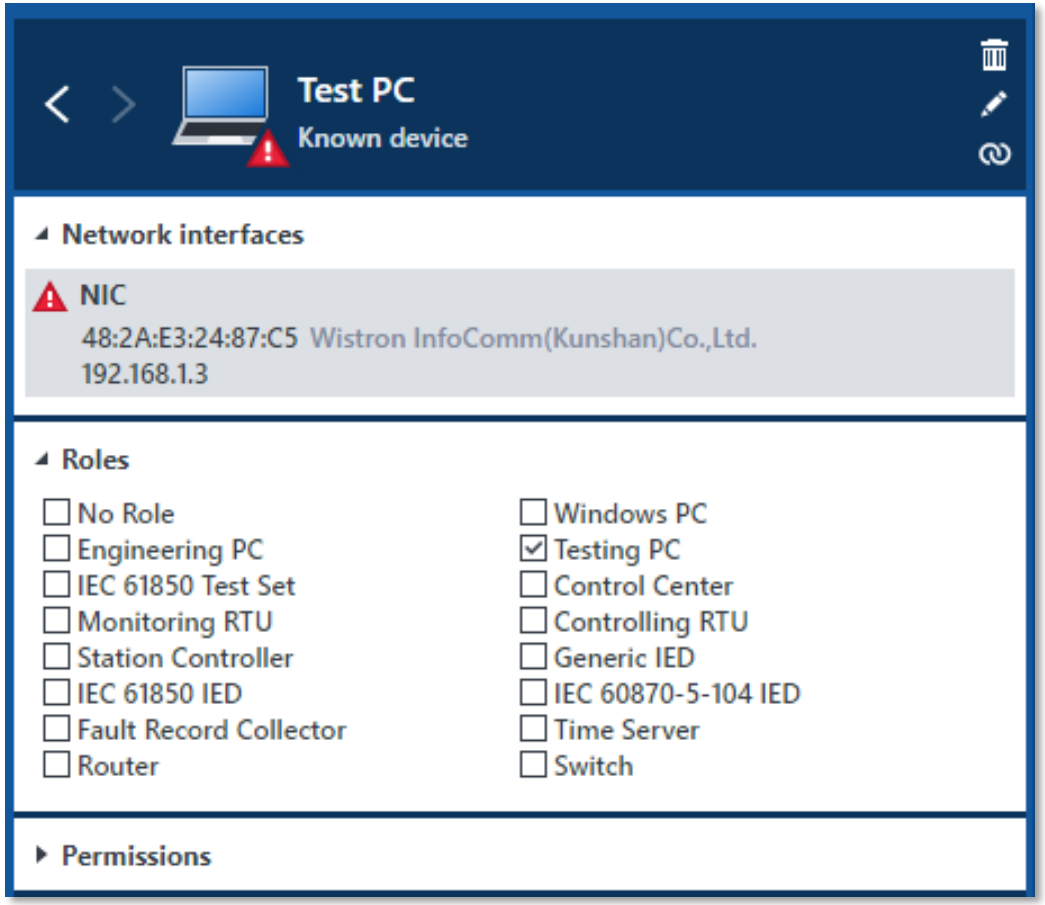
- IEC 61850
- IEC 62439-3 PRP and HSR (with RedBox)
- IEC 60870-5-104 (-101 and -103 over TCP/IP)
- DNP3
- Modbus TCP (and Modbus RTU over TCP/IP)
- IEC 62056 (DLMS/COSEM)
- IEEE C37.118 (Synchrophasor protocol)
- IEEE 1703-2012 / ANSI C12.22 (AMI protocol)
- IEC 60870-6 TASE.2/ICCP

IT Protocols (more than 300)

- FTP
- HTTP
- SSH, HTTPS (application detection without decryption)
- RDP
- NTP
- SNMP
- netbios (Windows file sharing)
- ARP, DHCP
- MySQL, MSSQL, PostgreSQL
- telnet
- ICMP, ICMPv6
- RIPv2
- SSDP
- MDNS
- ...

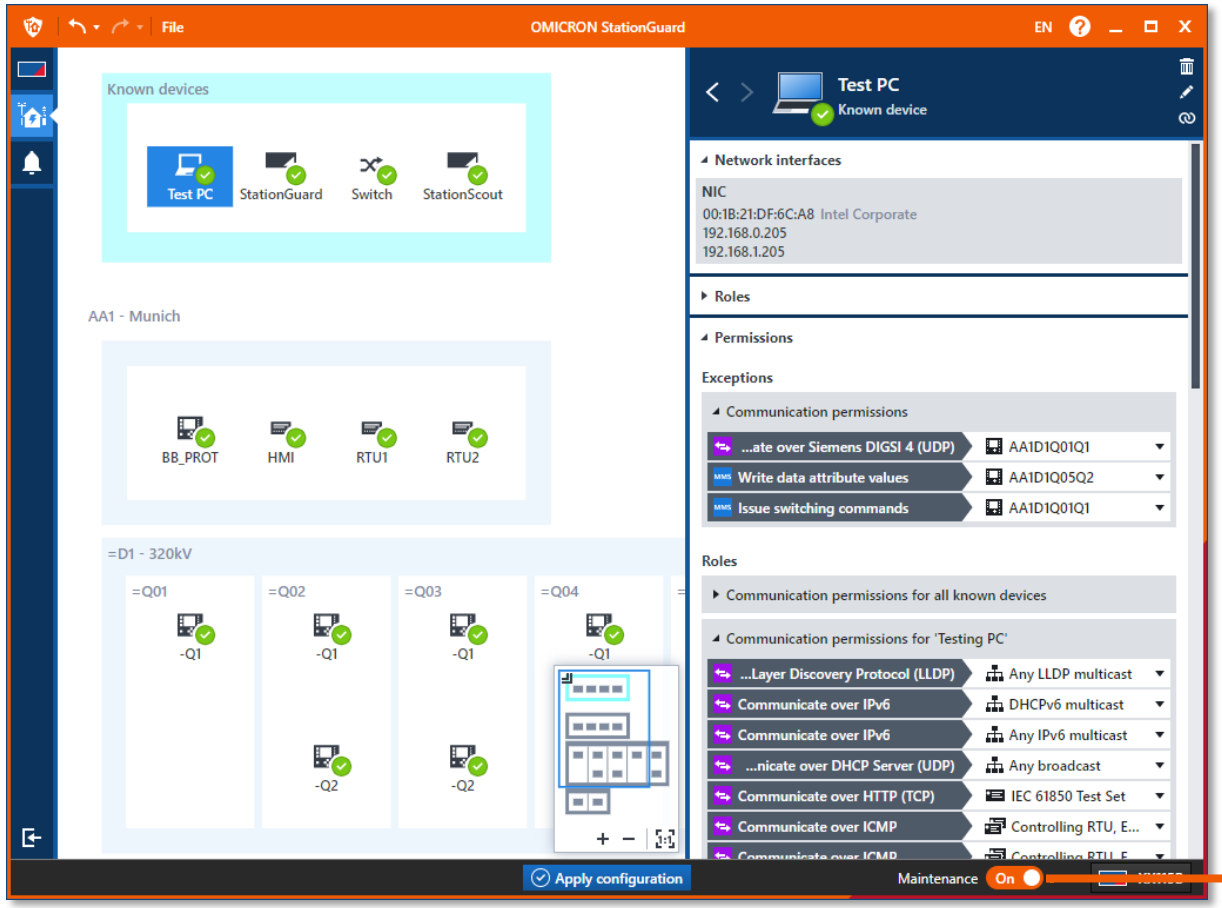
How do I configure StationGuard?

1. In case of IEC 61850 substations:
   - Import the SCL file(s)
2. Assign roles to remaining devices
   - RTUs
   - Engineering PCs, Switches, Time Server
   - …
3. Add additional permissions based on alerts
   - *"All **Engineering PCs** may use vendor protocol X, but only during maintenance."*



OMICRON

Built-in Support for Commissioning and Maintenance



Normal operation

- Engineering PCs must not use engineering protocols and web interfaces
- Remote access not allowed
- Activating IED Test Mode not allowed

Maintenance

- Engineering PCs may use certain engineering protocols and web interfaces
- Certain remote connections allowed
- Activating IED Test Mode allowed

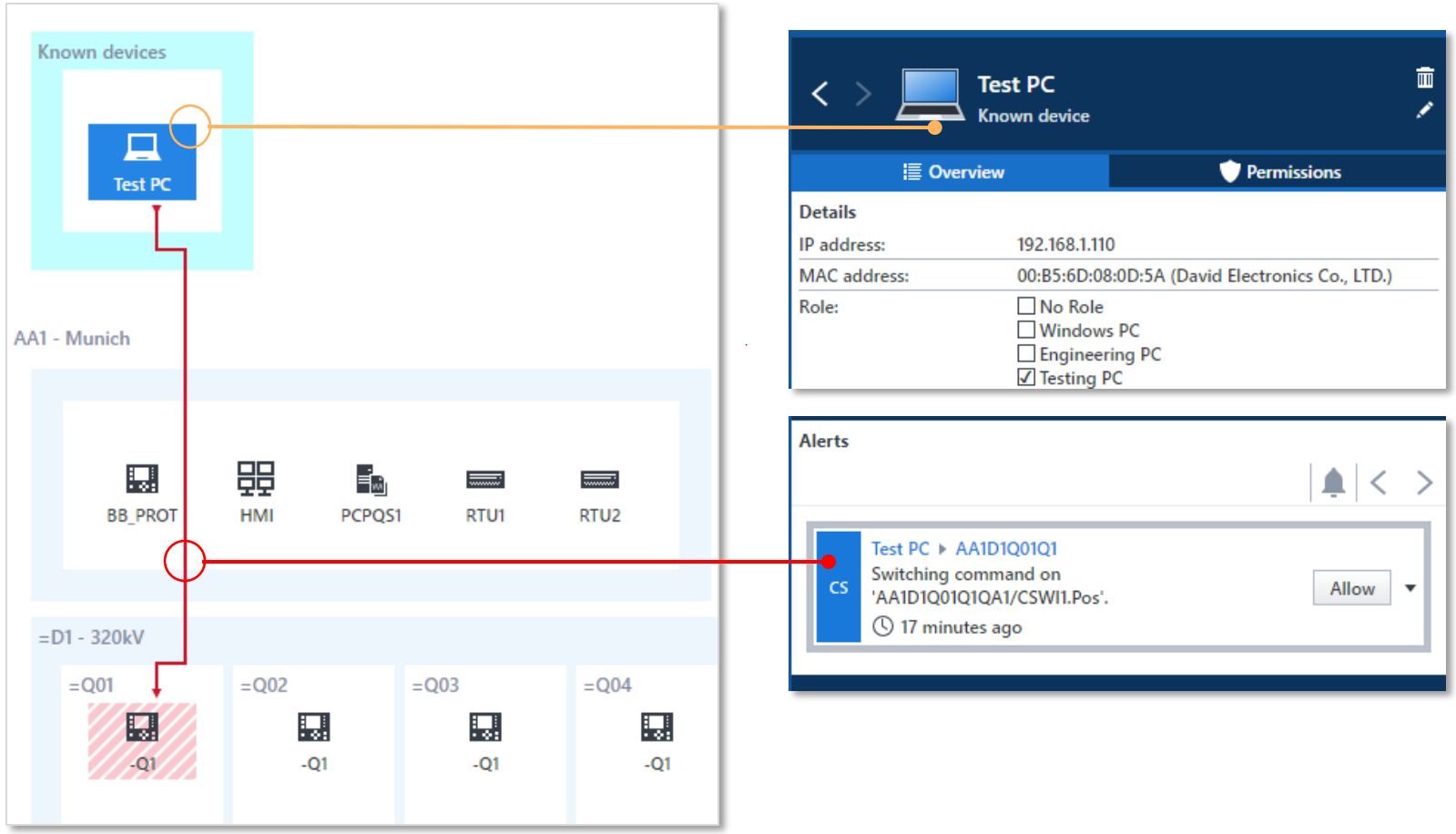
24/7 Functional Monitoring – Examples

- Detects device configuration changes
  Monitoring of configuration revision fields in messages
- Continuous GOOSE transmission time measurements
  Detecting failures in devices, network, or time synchronization
- Logging of critical events:
  - Control commands on switchgear, tap changers, etc.
  - Monitoring and logging of file transfers – including file names.

⚠	2020-10-31 10:42:15.255Z	G	AA1D1Q01Q1 ▸ GOOSE multicast Configuration revision (ConfRev) newer than expected in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:42:15.255Z	G	AA1D1Q01Q1 ▸ GOOSE multicast Wrong VLAN identifier in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:42:15.255Z	G	AA1D1Q01Q1 ▸ GOOSE multicast Wrong destination MAC address in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:40:25.165Z	G	AA1D1Q03Q1 ▸ GOOSE multicast Unknown GOOSE 'AA1D1Q03Q1Protection/LLN0GOgcb_2' found on network.
⚠	2020-10-31 10:09:52.866Z	CS	Test PC ▸ AA1D1Q01Q1 Switching command on 'AA1D1Q01Q1QA1/CSWI1.Pos'.
⚠	2020-10-31 09:32:43.987Z	G	AA1D1Q03Q1 ▸ GOOSE multicast IED indicates time synchronization failure (ClockNotSynchronized) in GOOSE 'AA1D1Q03Q1CONTROL/LLN0GOgcb

Security officers and engineers need to work together

- Protection and control engineers are needed in alert analysis
- User interface should allow engineers and security officers to analyze the cause **together**

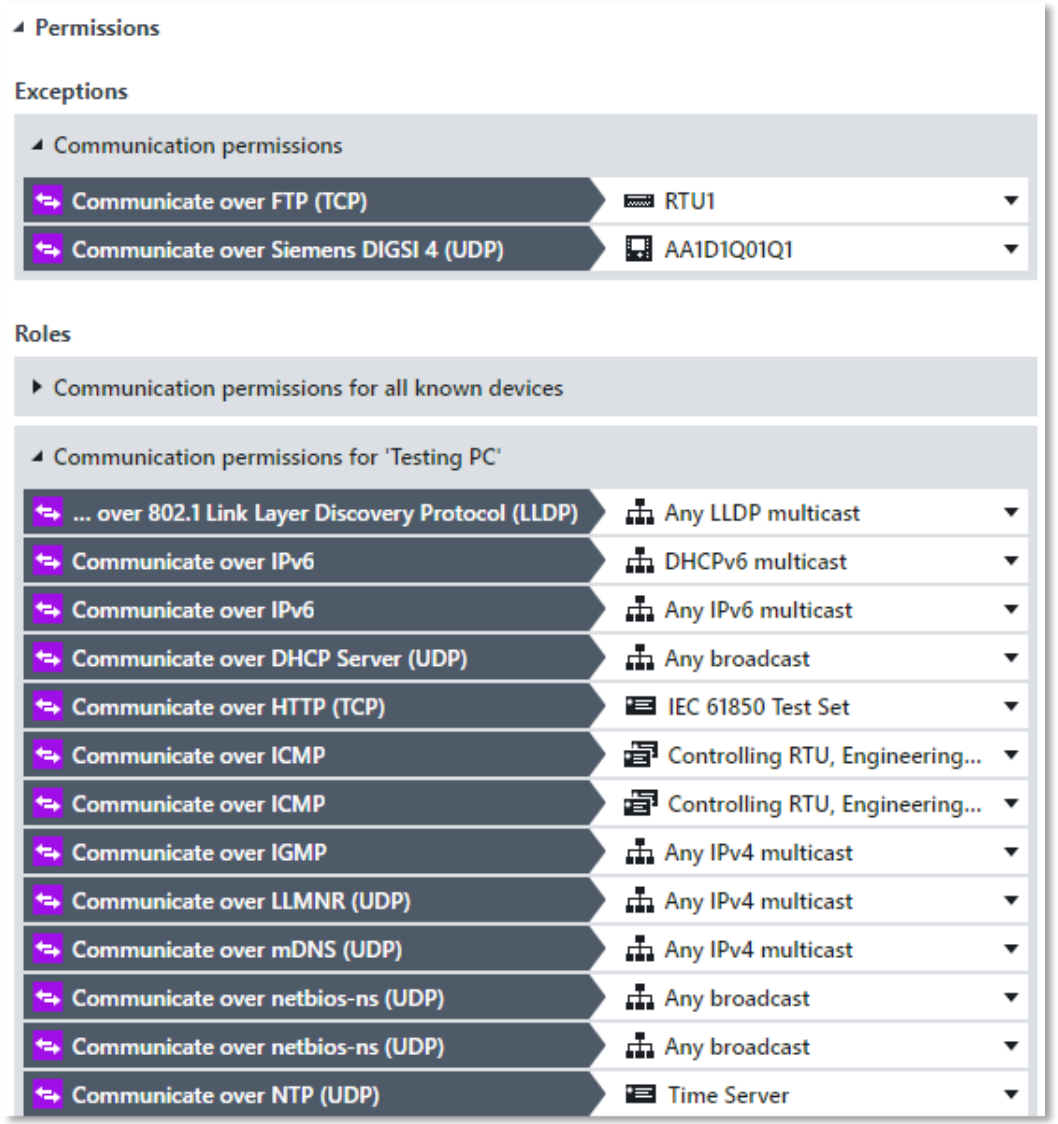


RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

OMICRON

Auditable Allow List

- Full control **who communicates** how and with whom
- Full control which laptops are used
- **Logging** of critical actions
- **Can be audited** by security experts without being on-site



OMICRON

StationGuard Platform Options

StationGuard on RBX1

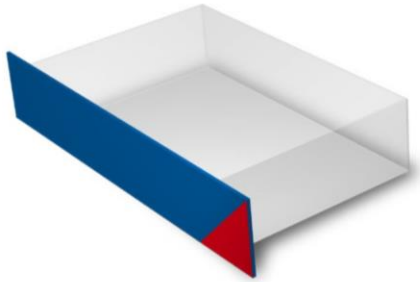
- Made for permanent installation in substations
- Ultra-high performance

StationGuard on MBX1

- Mobile applications, temporary usage
- Security assessments in substations
- Temporary monitoring during commissioning

StationGuard on virtual machine

- Installation on existing computing platforms [1]



[1] available Q3/Q4 2021

OMICRON

RBX1 Hardware Platform

- 8x Gigabit SFP fiber Ethernet ports
- Monitor 8+ separate networks simultaneously
- Binary I/Os for alarms and fault signal contact
- DC supply, redundant option
- Extreme cybersecurity hardening
- Rugged and fan-less design,
  IEC 61850-3 compliant

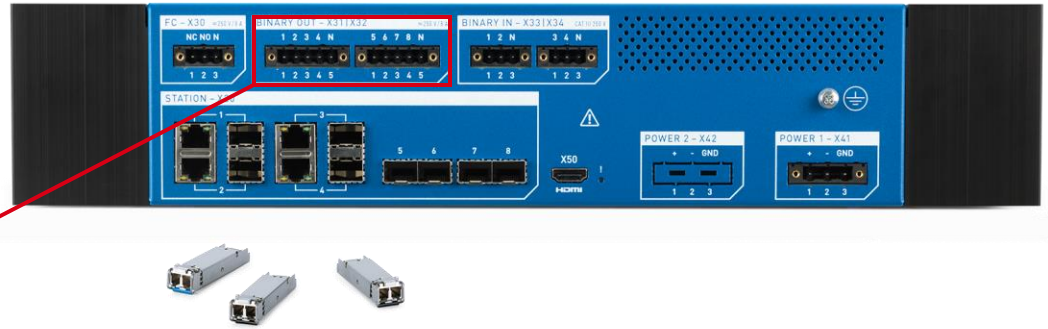
front view

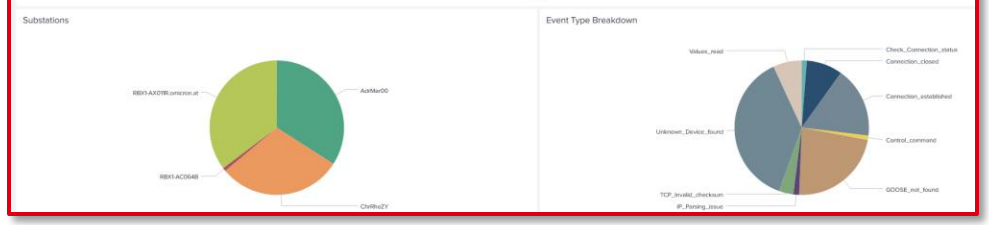
back view

OMICRON

How to integrate StationGuard?

- StationGuard Dashboard for central monitoring
  - Which substations show an alarm?
- Integration into SCADA signal list using binary outputs
  - Easy way to get IDS status into the control room
- Integration into SIEM Systems
  - Using Syslog and plug-ins
- Integration into ticket systems and CMDBs
  - Using Plug-Ins and export functions





SIEM integration example (Splunk App)

RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

OMICRON

Case study: Installation in legacy substations, 2018-2021

- Outdated/incomplete SCD?
  - **Generated the SCL** file from the live system
- Findings:
  - More **external connections** than expected
    - Different departments creating connections to substation equipment
  - NTP **time synchronization** issues
  - **MMS communication errors** between IEDs
    - Interoperability issues
    - Configuration errors

Conclusion

- Many ways to attack a substation
- Firewalls alone are not enough
- Security solutions must speak the language of protection and control engineers
- StationGuard is tailor-made for detecting intrusions in substations

Thank you for your attention!

www.stationguard.com

OMICRON