67th AMEU Convention

SUSTAINABLE CUSTOMER CENTRIC ELECTRICITY UTILITIES IN THE 4TH AND 5TH INDUSTRIAL REVOLUTION

Cyber Security Intrusion Detection for Station and Process Bus Applications in Substations:

Challenges, Experiences and Case Studies

Andreas Klien, OMICRON, Austria
Riaan Louw, Alectrix, South Africa

Hosted by

ETHEKWINI MUNICIPALITY

“There were, on average 1 611 attacks carried out against industrial facilities across Africa each week over the past six months, and about 11% of organisations were affected by [...] malware.”

CREAMER MEDIA'S ENGINEERING NEWS

Cybersecurity becoming part of industrial practices as digital applications and risks multiply

How to secure your substations?

- **Identify** the status quo
  - Identify your risk for cyberattacks: identify your vulnerabilities
- **Protect** against the highest risks
  - Technical and organizational measures
- **Detect** threats and prohibited activity
  - Allows to minimize damage and learn for next time
- **Respond** to detected threats
  - Investigate security alerts
- **Recover**
  - E.g., clear malware from Gateways

Source: nist.gov/cyberframework

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:

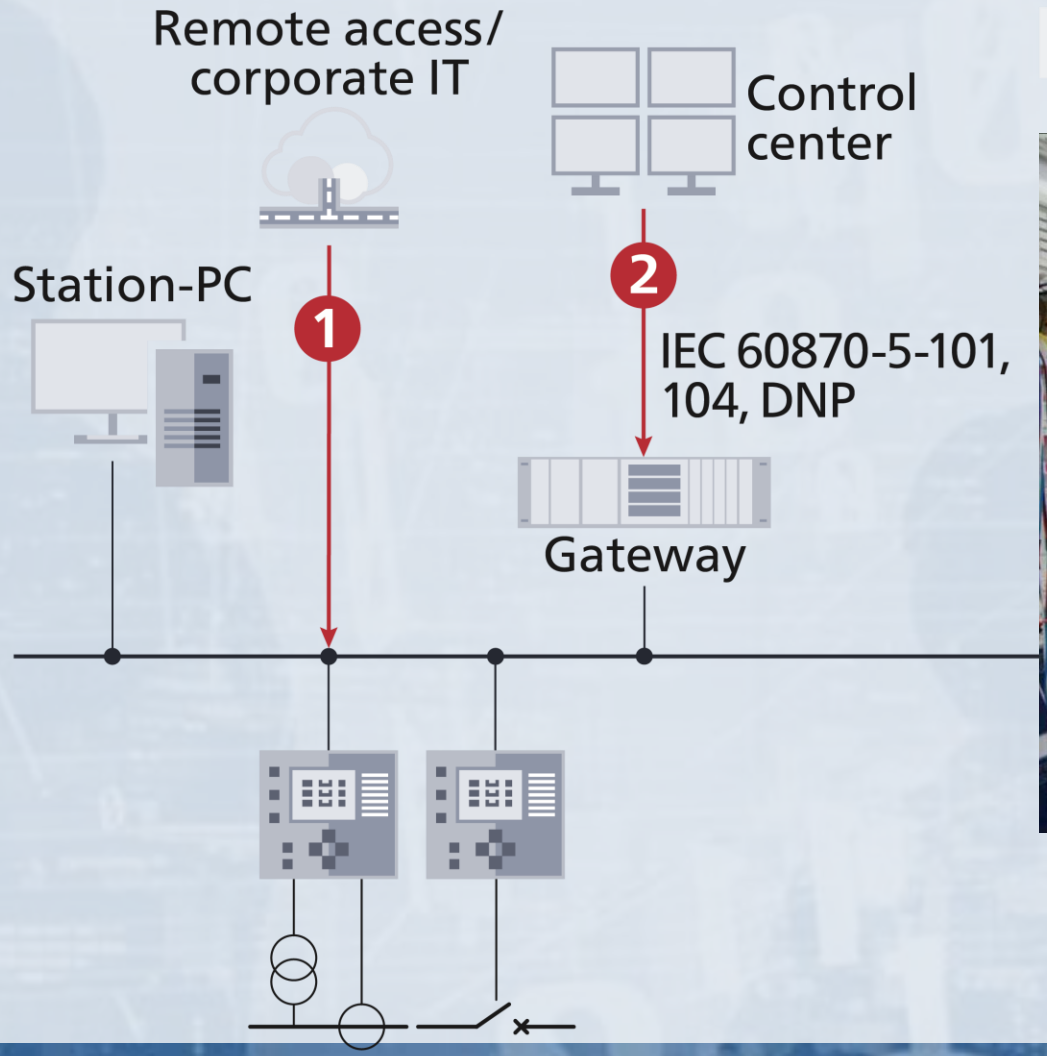
- RUGGEDCOM RM1224: All versions between v5.0 and v6.4
- SCALANCE M-800: All versions between v5.0 and v6.4
- SCALANCE S615: All versions between v5.0 and v6.4
- SCALANCE SC-600: All versions prior to v2.1.3
- SCALANCE W1750D: v8.3.0.1, v8.6.0, and v8.7.0

ICS Advisory (ICSA-21-096-01)

4.1 AFFECTED PRODUCTS

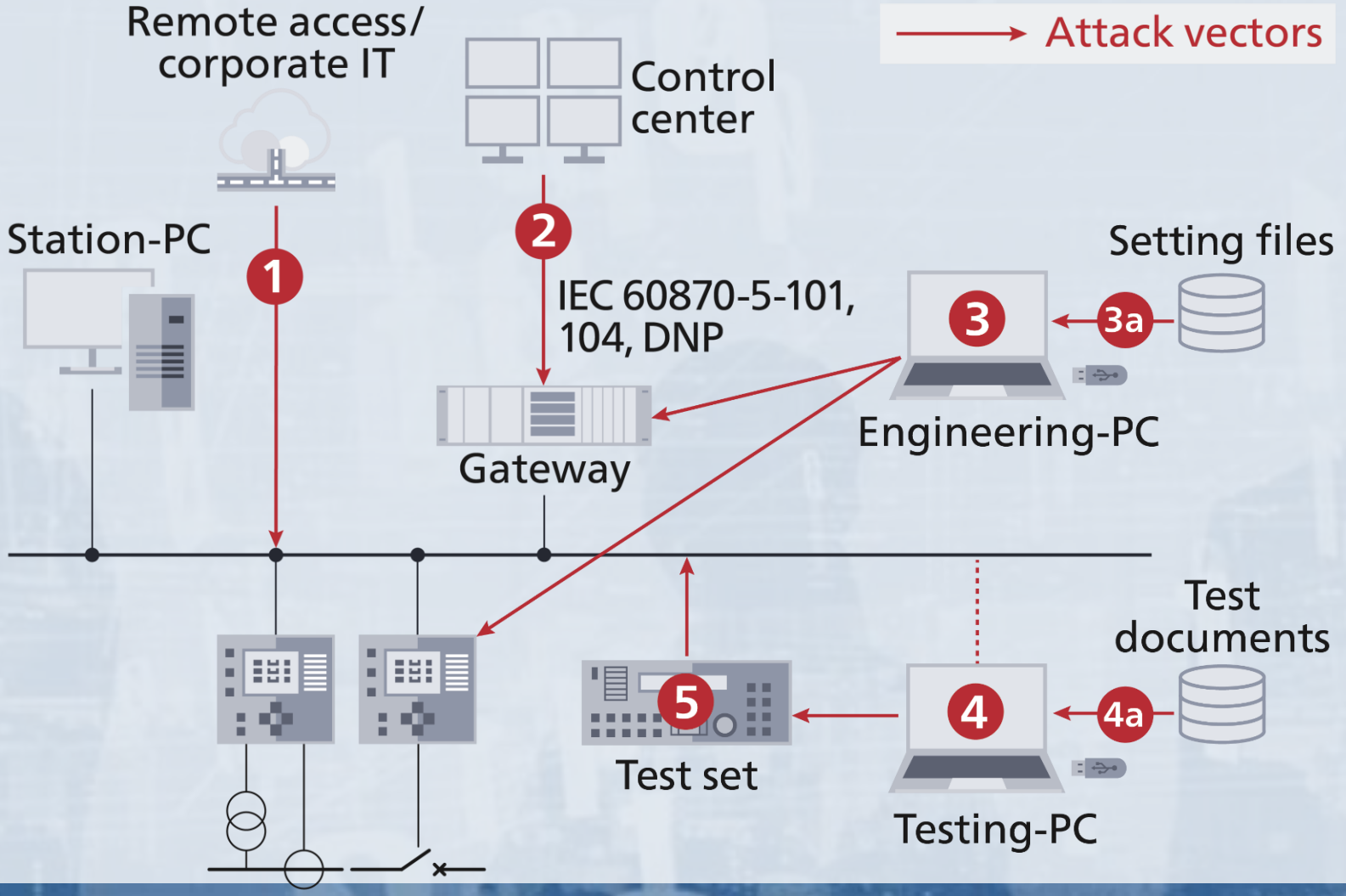
- Relion 670 series Version 1.1, all revisions
- Relion 670 series Version 1.2.3, all revisions
- Relion 670 series Version 2.0, all revisions
- Relion 670/650 series Version 2.1, all revisions
- Relion 670/650 series Version 2.2.0, all revisions
- Relion 670/650/SAM600-IO series Version 2.2.1, all revisions
- Relion 670 series Version 2.2.2, all revisions
- Relion 670 series Version 2.2.3, all revisions

Identifying the attack points of substations



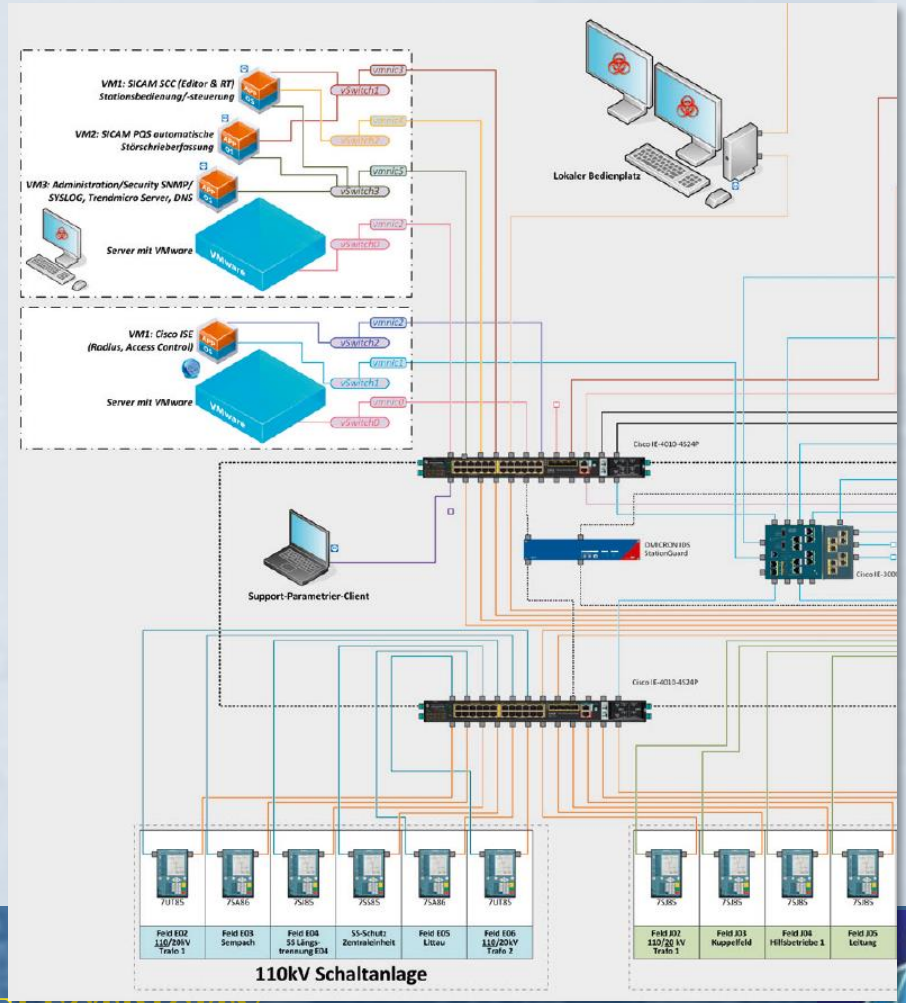
Attack vectors

Identifying the attack points of substations



Secure substations do exist! – A Case Study

- Example by Swiss distribution and generation utility CKW
- Sophisticated security architecture
  - Secure remote (and local) access
  - Multiple firewall zones on station bus (ACL)
  - Switch port security
  - Role-based access control
- Defense in depth:
  - Intrusion detection in all substations
- Commissioning of first substation started 2019
  [See paper here.]



Source: Centralschweizer Kraftwerke AG (CKW), Switzerland

Problems of current IDS when applied in the power grid

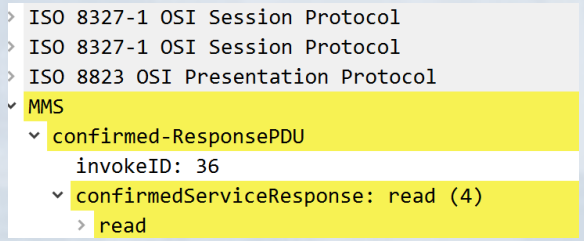
- **Signature**-based
  - PC virus scanner approach
  - Very few exploits/attacks known for our niche

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

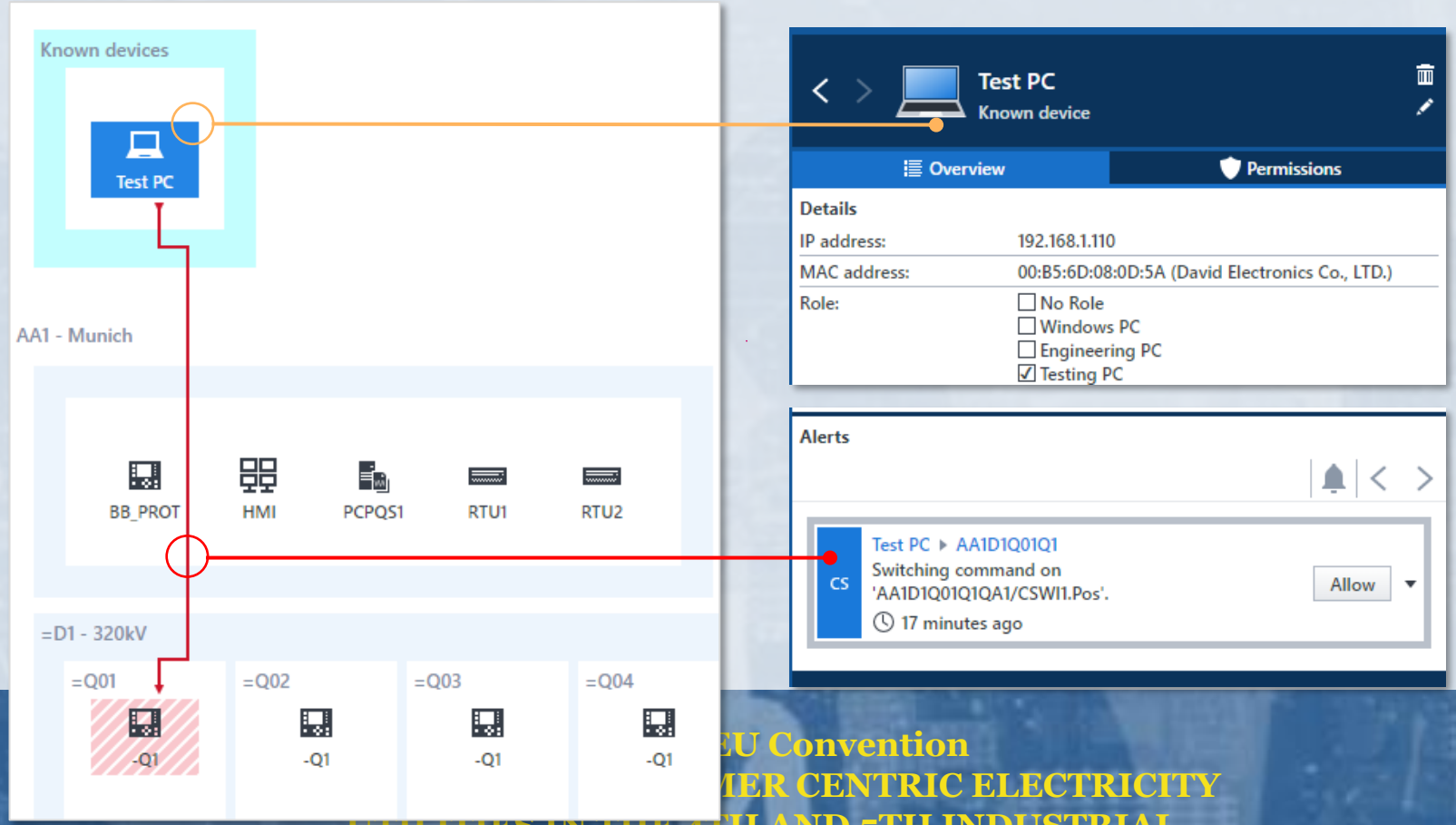
Black box

Difficult for to analyze,
even for experts



OT-Engineers Need to Participate in Security Processes

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



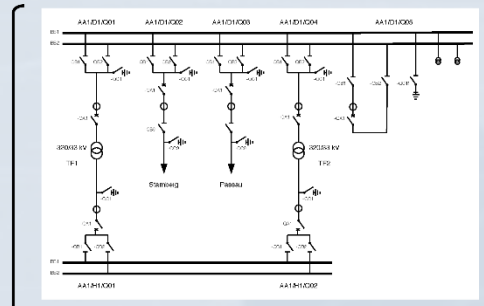
Intrusion Detection in the Power Grid

StationGuard knows the substation

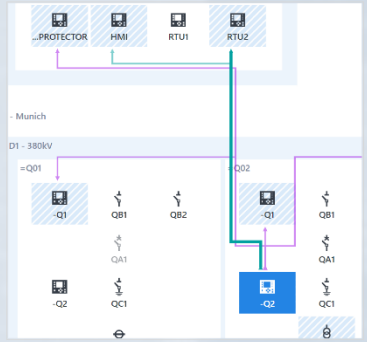
- Function of each device known from engineering files (SCL)
- Each packet evaluated against live system model
  - Allow list (whitelist) principle: alarm by default
- Maintenance and testing is part of system model

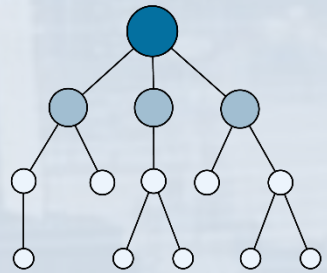
- Detailed <u>verification</u> of whole communication
- Detects not just cyber threats, but also malfunctions

Functional security monitoring



SCL

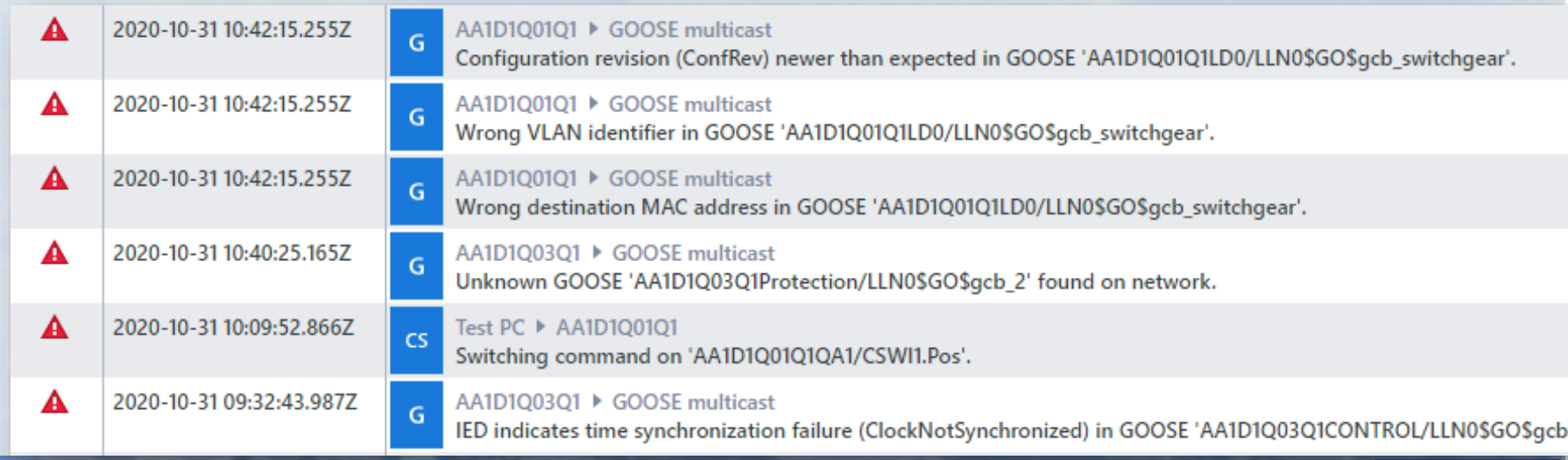




System model/allow list

Additional benefits: Functional Monitoring

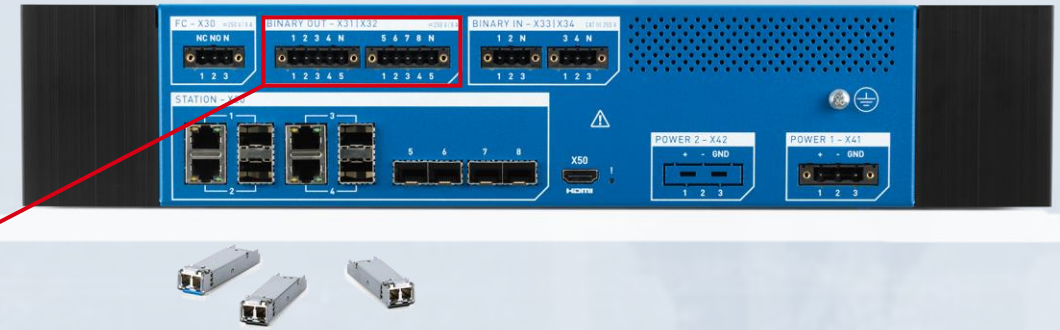
- Detecting IED configuration changes and configuration issues
- Continuous GOOSE transmission time measurements
  - Detecting IED, network, and time sync. failures
- Logging of critical events:
  - Control commands:
    - Successful / Failed
  - File transfers incl. file names

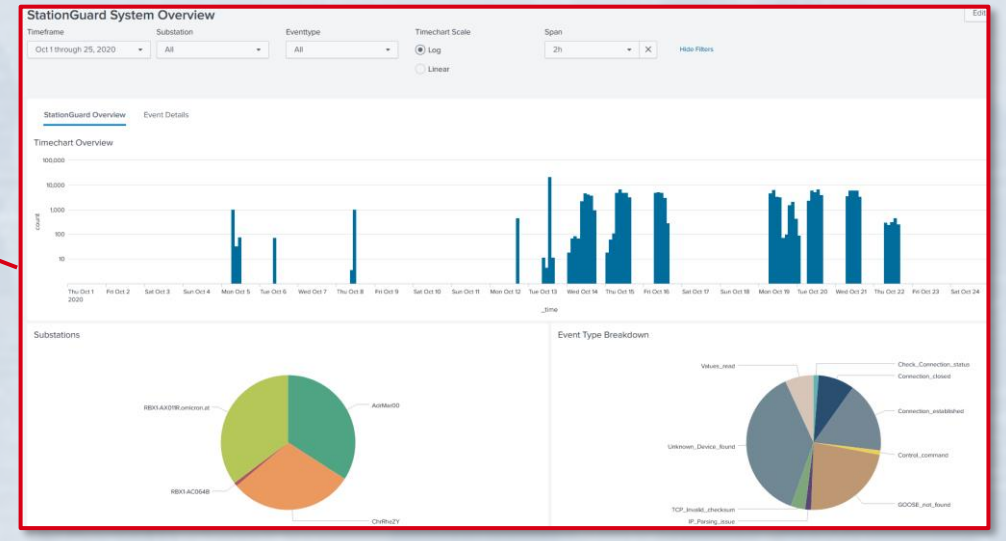


⚠	2020-10-31 10:42:15.255Z	G	AA1D1Q01Q1 ▸ GOOSE multicast Configuration revision (ConfRev) newer than expected in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:42:15.255Z	G	AA1D1Q01Q1 ▸ GOOSE multicast Wrong VLAN identifier in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2020-10-31 10:42:15.255Z	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

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)

Common findings in legacy substations

- IEDs with known vulnerabilities (no surprise)
- More external connections than expected
  - Each connection represents an attack vector
  - E.g., “The network guys” managing the switches
- Gateways with outdated Windows OS
- Functional Issues
  - RSTP reconfiguration every 10 seconds!
  - NTP time synchronization issues
  - Configuration errors in RTU Report config.

Conclusion

- Many attack vectors bypass the firewall
- Intrusion Detection Systems (IDS) can help in many phases of the security processes
- Tailor-made IDS for the power grid are available

  www.stationguard.com

- **Thank you for your attention!**