
CONFERENCE
OMAINTEC
2024
EXHIBITION
THE 21ST INTERNATIONAL
OPERATIONS & MAINTENANCE
CONFERENCE IN THE ARAB COUNTRIES
Improving Operational efficiency and OT Security for Power Grids
Protect Your Grid
by OMICRON
#OmaintecConf
An Initiative by
OMAINTEC
المجلس العربي للتشغيل والصيانة
Arab Operations & Maintenance Council
Organized by
EXICON.
International Group
مجموعة أكزيكون الدولية

Who We Are

Amro Mohamed
Regional Cybersecurity Sales Manager – MEA Region
amro.mohamed@omicronenergy.com

Arulraj Irudayasamy
Regional Cybersecurity and SAS Application Specialist – MEA Region
arulraj.irudayasamy@omicronenergy.com

About OMICRON

- OMICRON serves the electrical power industry with **innovative products and services** for **testing, diagnostics and monitoring** of assets worldwide.
- We help to make the generation, transmission and distribution of electricity **safe and reliable**.
- Over **1,100 employees** from **45 different countries** and **25 offices worldwide.**
- Customers in **171 countries worldwide**

Short Agenda

Patching an Industrial Asset: A Dilemma or An Opportunity

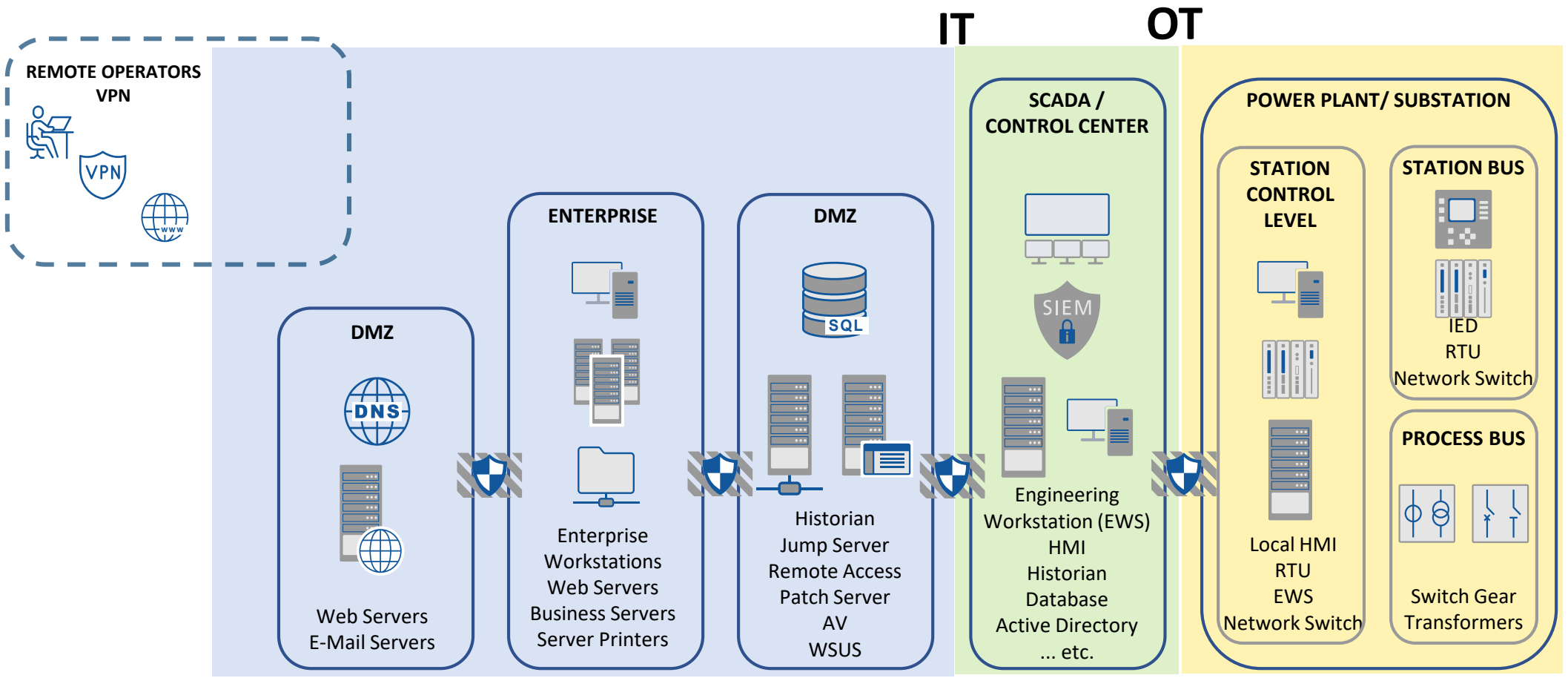
OASIS CSAF 2.0: A New Standard for Vulnerability Matching and Management

Asset Inventory Management in the Age of Modern and Digital Substations: The Importance of IEC61850

OMICRON's StationGuard: A Solution for Vulnerability and Asset Inventory Management based on CSAF and IEC61850

StationGuard: A Practical Demonstration of Cybersecurity in Power Grids

IT/OT Convergence: The Key to Digital Transformation



#OmaintecConf

The Rise of Industrial Cyber threats in 2023

ICS/OT

670 ICS Vulnerabilities Disclosed by CISA in First Half of 2023: Analysis

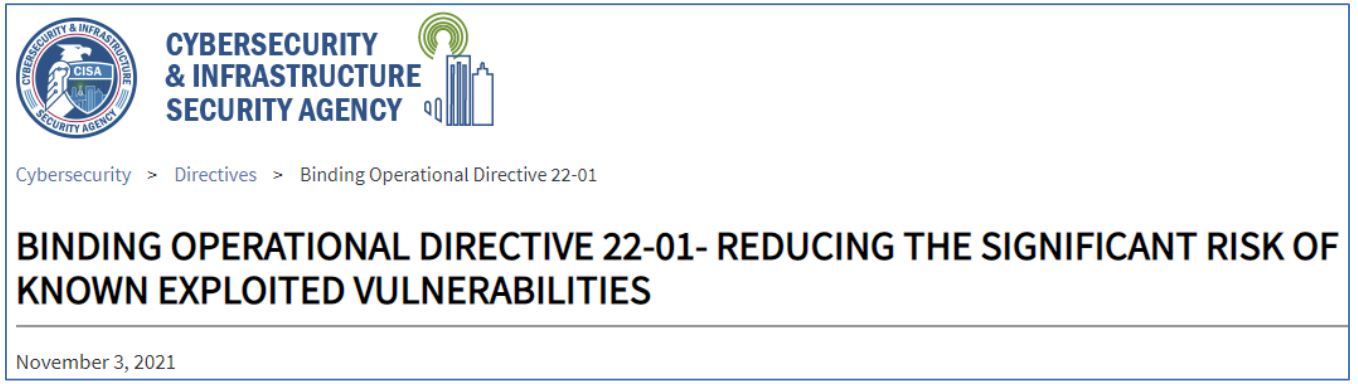
CISA disclosed 670 ICS vulnerabilities in the first half of 2023, but roughly one-third have no patches or mitigations from the vendor.

Source: SecurityWeek

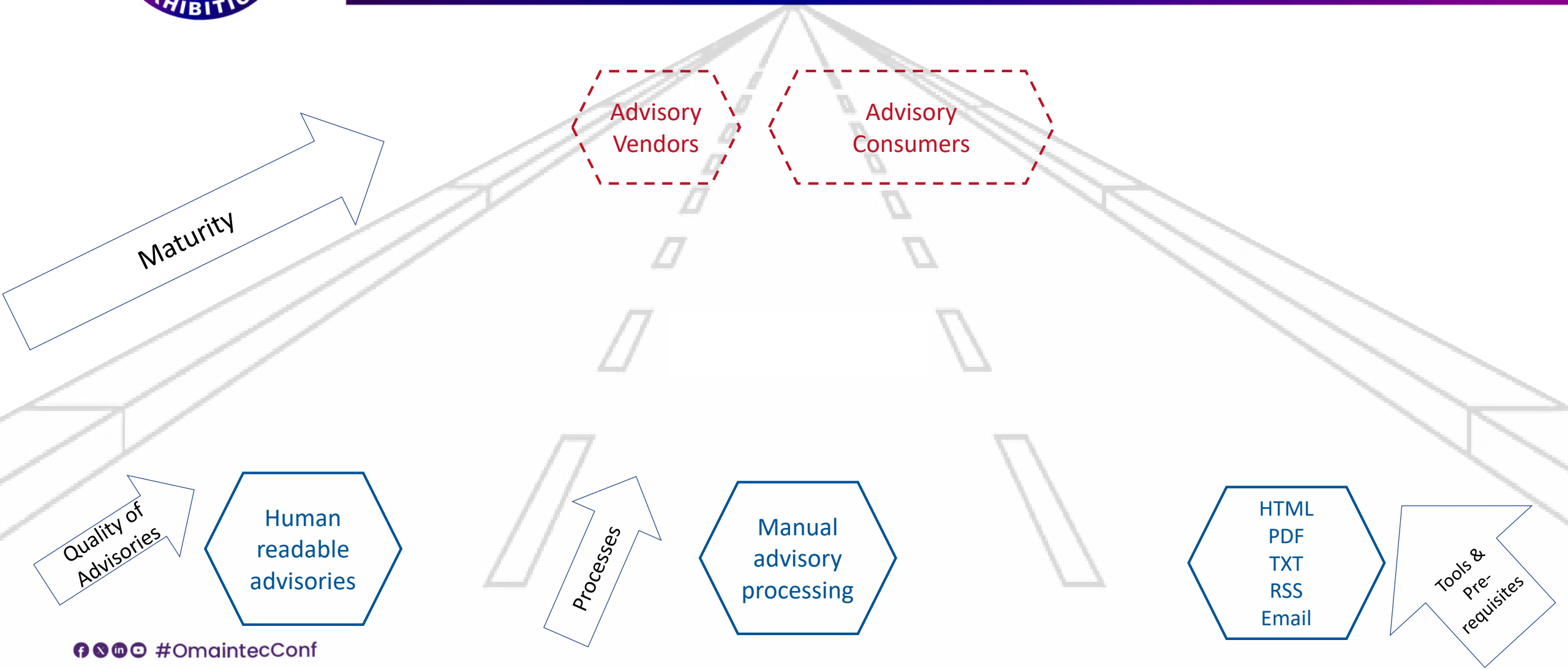
Start Patching!

"Why are there still thousands of protection and control devices

- with **firmware** that is years old,
- with **vulnerabilities** that are years old,
- and even with known **exploits**?"



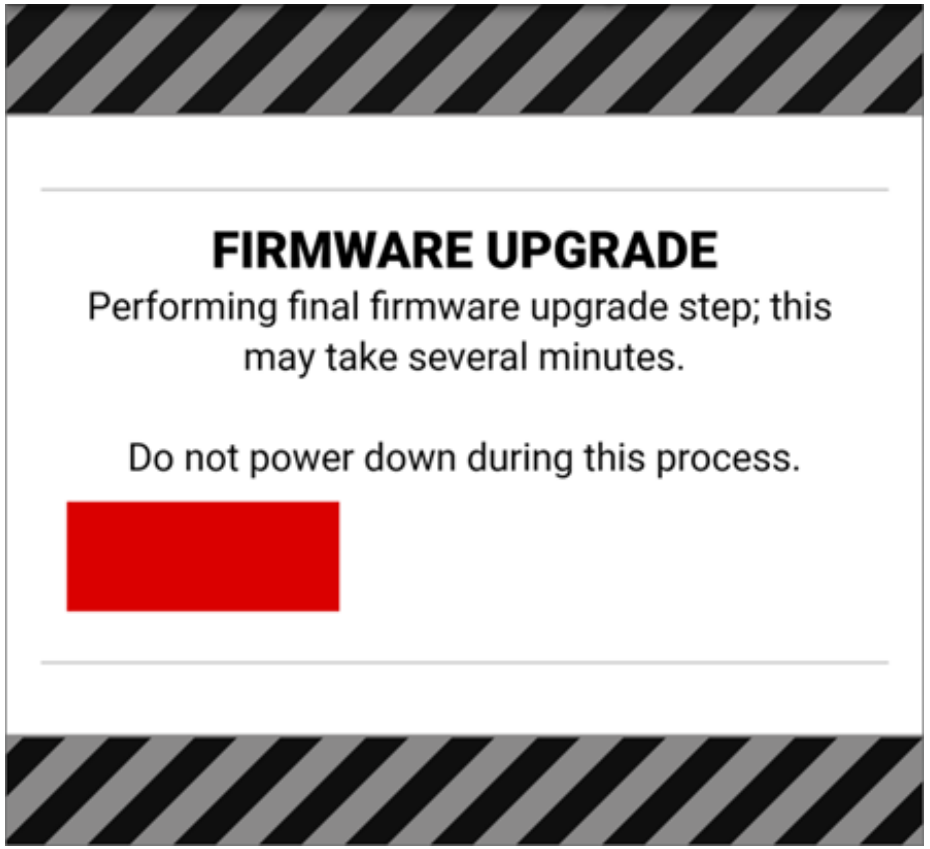
Security Advisories Information Flow & Maturity



Reason 1: Shutdowns

- Patching Requires Power Lines and Generators to Be De-energized.

- The Cycle of Patching: Shutdown Approval Delays and New Patches.



Reason 2 : It’s a Software!

The risk of applying a patch can be **higher than not applying it.**

- **Patching is not a Bug-Free Solution.**
- **Patches are Not Consistent across Hardware Revisions.**
- **Patches May Affect Your PLC Logic Negatively.**


WIRED

LILY HAY NEWMAN SECURITY AUG 11, 2022 1:20 PM

Sloppy Software Patches Are a ‘Disturbing Trend’

The Zero Day Initiative has found a concerning uptick in security updates that fail to fix vulnerabilities.

How do i test Automation and Logic functions?

Risk Management Instead of Blind Patching

1. What are the security vulnerabilities of my OT vendors?
2. Which OT devices are affected?
3. How big is the risk?
4. What are the remediation/mitigation options?
5. What are the intermediate options until we can patch it?

What is a Security Advisory?

- Security advisories about utility automation devices are published frequently
- My substations are at risk if
  - certain device types with
  - certain firmware version and
  - in certain network setup

  are used.

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

Challenge with Security Advisories

- Security advisories are usually sent as PDFs by e-mail from each manufacturer separately.
- Per manufacturer **60-200 advisories per year**.
- Approx. **10-20 device types** affected per advisory.
- You find statements like these in the PDFs:

> *"Affected are medium voltage drives manufactured since 2015 and prior to 2022"*

> *"Affected are all versions between V2.5 (including) and V2.7 (excluding)"*

> *"Affected are* ACME 14 *installations installed from material dated earlier than 2020-09-15"*

OMAINTEC CONFERENCE EXHIBITION 2024

OASIS CSAF 2.0: A New Standard for Vulnerability Matching and Management

#OmaintecConf

Common Security Advisory Format (CSAF)

Source: Oasis Open

The OASIS Common Security Advisory Framework (CSAF)

- Machine-readable, standardized format for security advisories
- Several big vendors already publish with CSAF
- Great improvement over PDFs sent out via email!

https://csaf.io

But there is still some work to do:

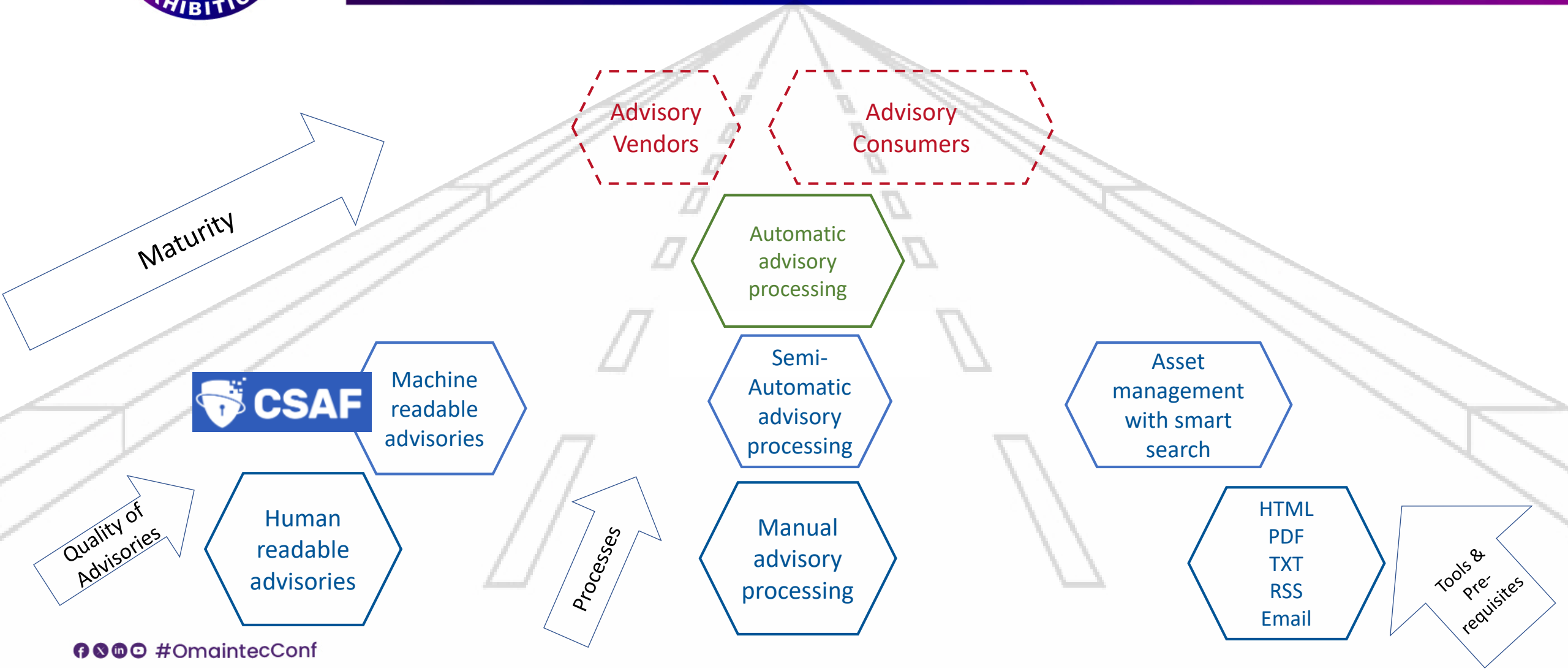
Examples for CSAF field
product_version_range

"Medium voltage drives manufactured since 2015 and prior to 2022"

"All versions between V2.5 (including) and V2.7 (excluding)"

"ACME 14 *installations installed from material dated earlier than 2020-09-15"*

Security Advisories Information Flow & Maturity



Our Compliance with CSAF for Vulnerability Disclosures

OMICRON

Products Applications Training Support

ID	Title	Affected Products	CVE ID	CVSS Score	Last update	Download
OSA-8	Linux Kernel Vulnerability in IGB Driver affecting StationGuard and StationScout	StationGuard Image 2.10.0073, 2.20.0080, 2.21.0081, StationScout StationScout Image 2.10.0059, 2.20.0063, 2.21.0064	CVE-2023-45871	9.8	2023-11-22	PDF TXT CSAF
OSA-7	3rd Party Vulnerabilities affecting StationGuard and StationScout	StationGuard < 2.30, StationScout < 2.30	CVE-2023-23919 CVE-2023-30589	7.5 8.2	2023-11-22	PDF TXT CSAF
OSA-6	Incorrect Authorization Vulnerability in StationScout and StationGuard	StationGuard StationGuard Image 1.10.0056 - 2.20.0080, StationScout StationScout Image 1.30.0040 - 2.20.0063	CVE-2023-28611	10	2023-11-22	PDF TXT CSAF
OSA-5	Vulnerability in Update Process of StationScout and StationGuard < 2.21	StationGuard StationGuard Image all before 2.20.0080, StationScout StationScout Image all before 2.20.0063	CVE-2023-28610	10	2023-11-22	PDF TXT CSAF

Anatomy of CSAF JSON file

Document Section


```
{
    "document": {
        "category": "csaf_security_advisory",
        "csaf_version": "2.0",
        "distribution": {
            "text": "Public",
            "tlp": {
                "label": "WHITE"
            }
        },
        "lang": "en-US",
        "notes": [
            {
                "category": "summary",
                "text": "Linux Kernel vulnerability CVE-2023-45871 allows an attacker to cause memory corruption in the network driver of the *BX device by sending special crafted network traffic. The behaviour of the system caused by memory corruption is highly unpredictable: the device is either restarted, processes crash, or a manual reboot is required.",
                "title": "Summary"
            },
            {
                "category": "details",
                "text": "OMICRON has released StationGuard 2.30 (with device image version 2.30.0092) and StationScout 2.30 (with device image version 2.30.0066) which address the issue and fix the vulnerability. It is strongly recommended that customers currently using the affected versions install the latest update available on the customer portal (registration required) as soon as possible to ensure the security of their system.\n  \nMore information about StationGuard and StationScout, including the link to download them, can be found on\n  \nhttps://www.omicronenergy.com/en/products/stationguard/ \n  \nand \n \nhttps://www.omicronenergy.com/en/products/stationscout/",
                "title": "Mitigation"
            },
            {
                "category": "general",
                "text": "OMICRON is an international company serving the electrical power industry with innovative testing, diagnostic and cybersecurity solutions. The application of OMICRON products allows users to assess and monitor the condition of assets in their electrical energy systems with complete confidence. Services offered in the area of consulting, commissioning, testing, diagnosis and training make the product range complete. Customers in more than 160 countries rely on the company’s ability to supply leading edge technology of excellent quality. Service centers on all continents provide a broad base of knowledge and extraordinary customer support. All of this together with our strong network of sales partners is what has made our company a market leader in the electrical power industry.",
                "title": "About OMICRON electronics"
            }
        ],
        "publisher": {
            "category": "vendor",
            "contact_details": "security@omicronenergy.com",
            "name": "OMICRON Product Security Team",
            "namespace": "https://www.omicronenergy.com/security/"
```

Anatomy of CSAF JSON file

Product Section


```
"product_tree": {
    "branches": [
        {
            "branches": [
                {
                    "branches": [
                        {
                            "branches": [
                                {
                                    "category": "product_version",
                                    "name": "2.10.0059",
                                    "product": {
                                        "name": "StationScout Image 2.10.0059",
                                        "product_id": "PUC-SSI210"
                                    }
                                },
                                {
                                    "category": "product_version",
                                    "name": "2.20.0063",
                                    "product": {
                                        "name": "StationScout Image 2.20.0063",
                                        "product_id": "PUC-SSI220"
                                    }
                                },
                                {
                                    "category": "product_version",
                                    "name": "2.21.0064",
                                    "product": {
                                        "name": "StationScout Image 2.21.0064",
                                        "product_id": "PUC-SSI221"
                                    }
                                },
                                {
                                    "category": "product_version",
                                    "name": "2.30.0066",
                                    "product": {
                                        "name": "StationScout Image 2.30.0066",
                                        "product_id": "PUC-SSI230"
                                    }
                                }
                            ],
                            "category": "product_name",
                            "name": "StationScout Image"
                        },
```

Anatomy of CSAF JSON file

Vulnerability Section

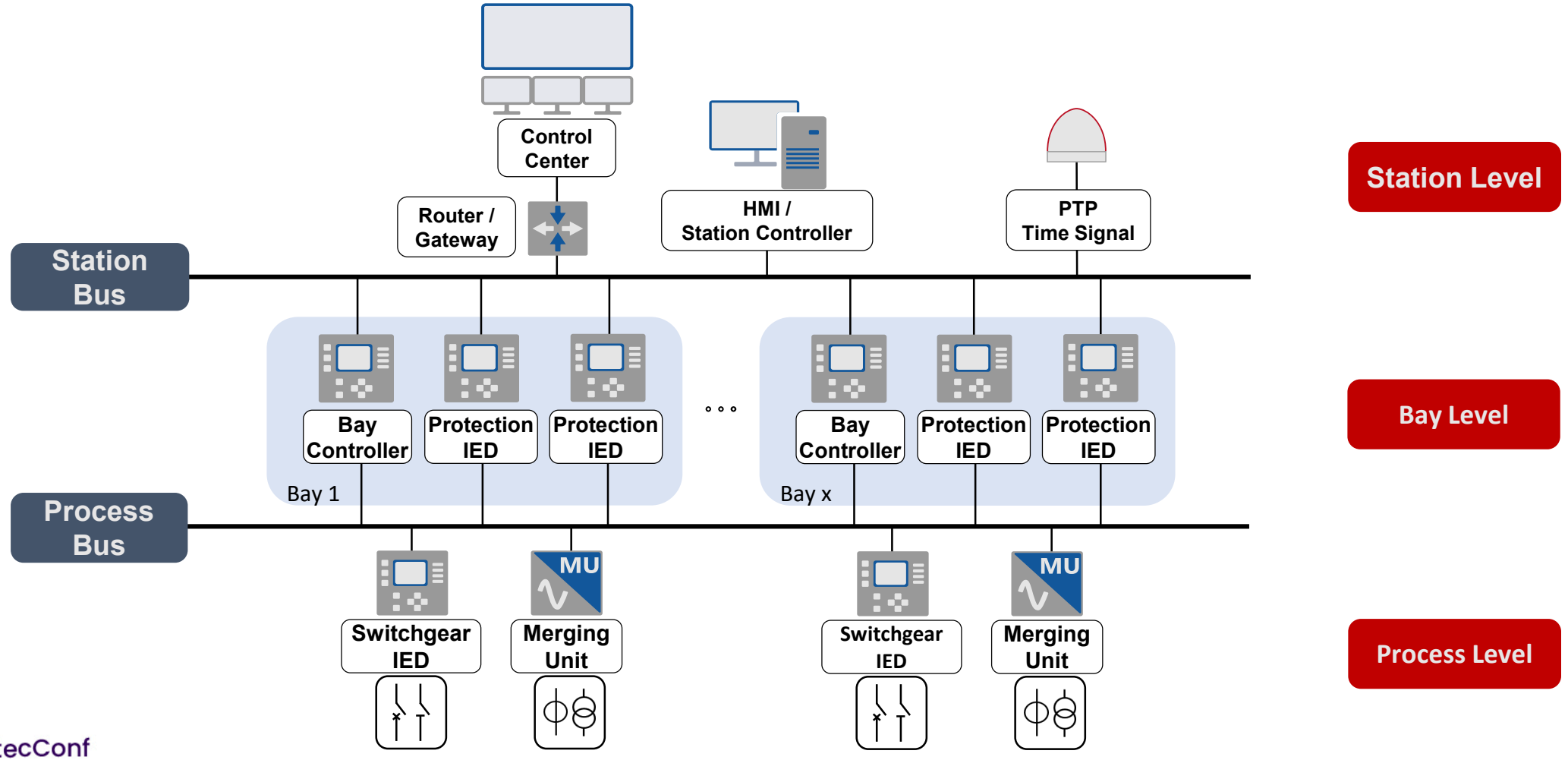

```
"vulnerabilities": [
    {
        "cve": "CVE-2023-45871",
        "cwe": {
            "id": "CWE-120",
            "name": "Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')"
        },
        "discovery_date": "2023-08-28T10:00:00.000Z",
        "involvements": [
            {
                "date": "2023-07-31T00:00:00.000Z",
                "party": "discoverer",
                "status": "completed",
                "summary": "Vulnerability discovered and reported by OMICRON electronics"
            }
        ],
        "notes": [
            {
                "category": "summary",
                "text": "An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel before 6.5.3. A buffer size may not be adequate for frames larger than the MTU.",
                "title": "Summary"
            }
        ],
        "product_status": {
            "first_fixed": [
                "PUC-SGI230",
                "PUC-SSI230"
            ],
            "known_affected": [
                "PUC-SGI210",
                "PUC-SGI220",
                "PUC-SGI221",
                "PUC-SSI210",
                "PUC-SSI220",
                "PUC-SSI221"
            ]
        },
        "references": [
            {
                "category": "external",
                "summary": "CVE-2023-45871",
                "url": "https://www.cve.org/CVERecord?id=CVE-2023-45871"
            },
            {
                "category": "external",
                "summary": "Linux Kernel Vulnerability in IGB Driver affecting StationGuard and StationScout",
                "url": "https://www.omicronenergy.com/fileadmin/user_upload/website/files/product-security/osa-8.pdf"
```

OMAINTEC CONFERENCE 2024 EXHIBITION

Asset Inventory Management in the Age of Modern and Digital Substations: The Importance of IEC61850

#OmaintecConf

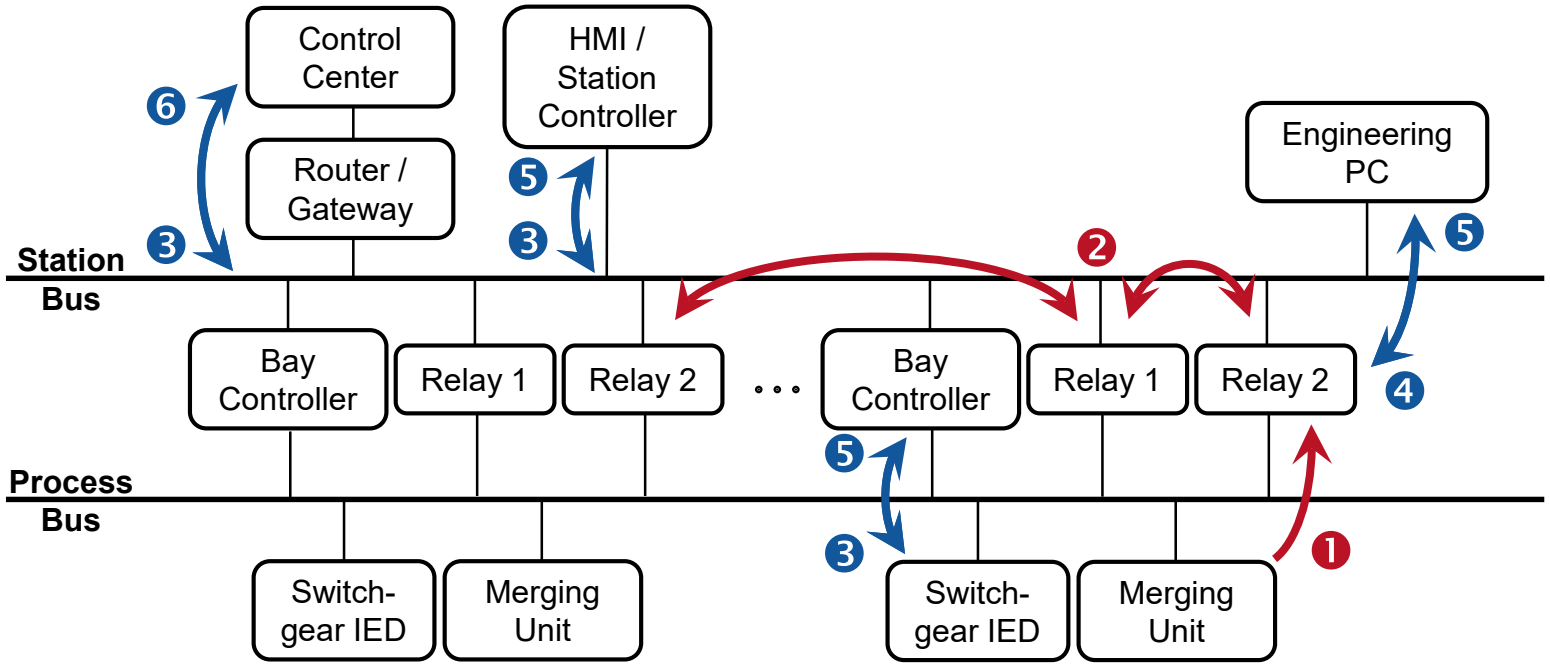
Typical Substation Communication Architecture



IEC 61850 Scope: More than just Communication

WHAT is communicated?	**Data Model**	Common Vocabulary
HOW is communicated?	**Services**	Grammar / Structure
BY WHAT is communicated?	**Mapping**	Channel / Medium Translation to Network
Engineering SCL	**System Configuration**	**File Format** / Configuration Tools
Testing	**Testing**	Conformance / Performance / **Functional**

Different Requirements for Communication in Substation



Realtime Services

1 CT/VT data: Sampled Values
2 fast IO data exchange: GOOSE

Client / Server Services

3 control
4 configuration
5 supervision
6 control-center: SCADA

Anatomy of an IEC 61850 SCD file

Header

Substation

Communication

IEDs

Data Type Templates

```
1    <?xml version='1.0' encoding='UTF-8'?>
2    <SCL xmlns="http://www.iec.ch/61850/2003/SCL" xmlns:sxy="http://www.iec.ch/61850/2003/SCLcoordinates" xmlns:xs
3      <Header id="Munich IOP SSD extended by hand" nameStructure="IEDName" revision="R0.0" toolID="emacs" version=
4      <Substation desc="Munich" name="AA1" sxy:x="1" sxy:y="5">
816    <Communication>
817
818    <IED name="BB_PROT" desc="Fallback protetion mechanism for Busbars" type="CoolDev12" manufacturer="Zewa">
934
935    <IED name="AA1D1Q01Q1" desc="Transformer infeed bay Q01" type="PROTEC 400" manufacturer="ACME">
1152
1153   <IED name="AA1D1Q01Q2" desc="Transfomer bay Q01" type="PROTEC 400" manufacturer="ACME">
1215
1216   <IED name="AA1H1Q01Q1" desc="Tranformer 33kV bay Q01" type="PROTEC 400" manufacturer="ACME">
1374
1375   <IED name="AA1D1Q02Q1" desc="Controller for breaker and bay Q02 infeed - Starnberg" type="PROTEC 400" manufa
1518
1519   <IED name="AA1D1Q02Q2" desc="Control disconnector to Starnberg - Q02" type="PROTEC 400" manufacturer="ACME">
1607
1608   <IED name="AA1D1Q03Q1" desc="Bay Q03 - Passau" type="PROTEC 400" manufacturer="ACME">
1820
1821   <IED name="AA1D1Q04Q1" desc="Transformer bay Q04" type="PROTEC 400" manufacturer="ACME">
1946
1947   <IED name="AA1D1Q05Q1" desc="380kV BC Protection &amp;amp; Control IED" type="ISIO 200 Circuit Breaker and Disco
2323
2324   <IED name="AA1D1Q05Q2" desc="380kV Bus1 &amp;amp; Bus2 Monitoring - Merging Unit" type="PROTEC 400" manufacturer
2398
2399   <IED name="AA1H1Q02Q1" desc="Tranformer 33kV bay Q02" type="MU 300" manufacturer="ACME">
2513
2514   <IED name="HMI" desc="IHMI" type="HMI 300" manufacturer="ACME" configVersion="HMI_300_0815">
2515   <IED name="RTU1" desc="RTU for transformer lines" type="RTU 600" manufacturer="ACME" configVersion="RTU_600_
2516   <IED name="RTU2" desc="Feeder RTU" type="RTU 600" manufacturer="ACME" configVersion="RTU_600_0815">
2517   <IED name="PCPQS1" desc="Disturbance record collector" type="COLLEC 400" manufacturer="ACME" configVersion="
2518   <DataTypeTemplates>
3550   </SCL>
```

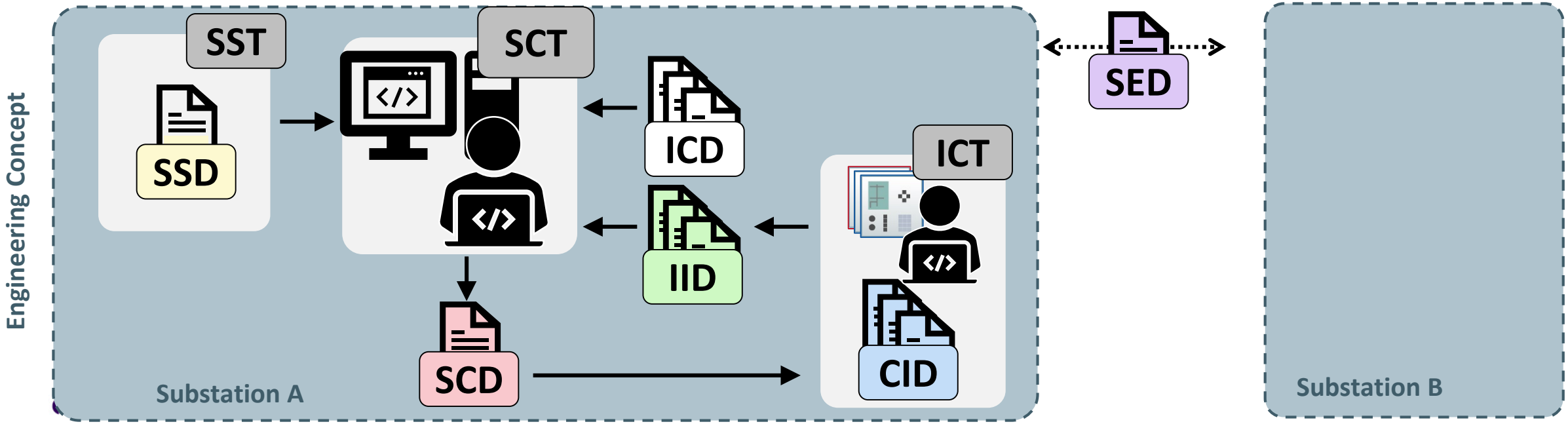
SCL Engineering Concept based on IEC 61850

IEC 61850 SCL Files

- **SSD** System Specification Description
- **ICD** IED Capability Description
- **SCD** System Configuration Description
- **CID** Configured IED Description
- **IID** Instantiated IED Description
- **SED** System Exchange Description

Tools

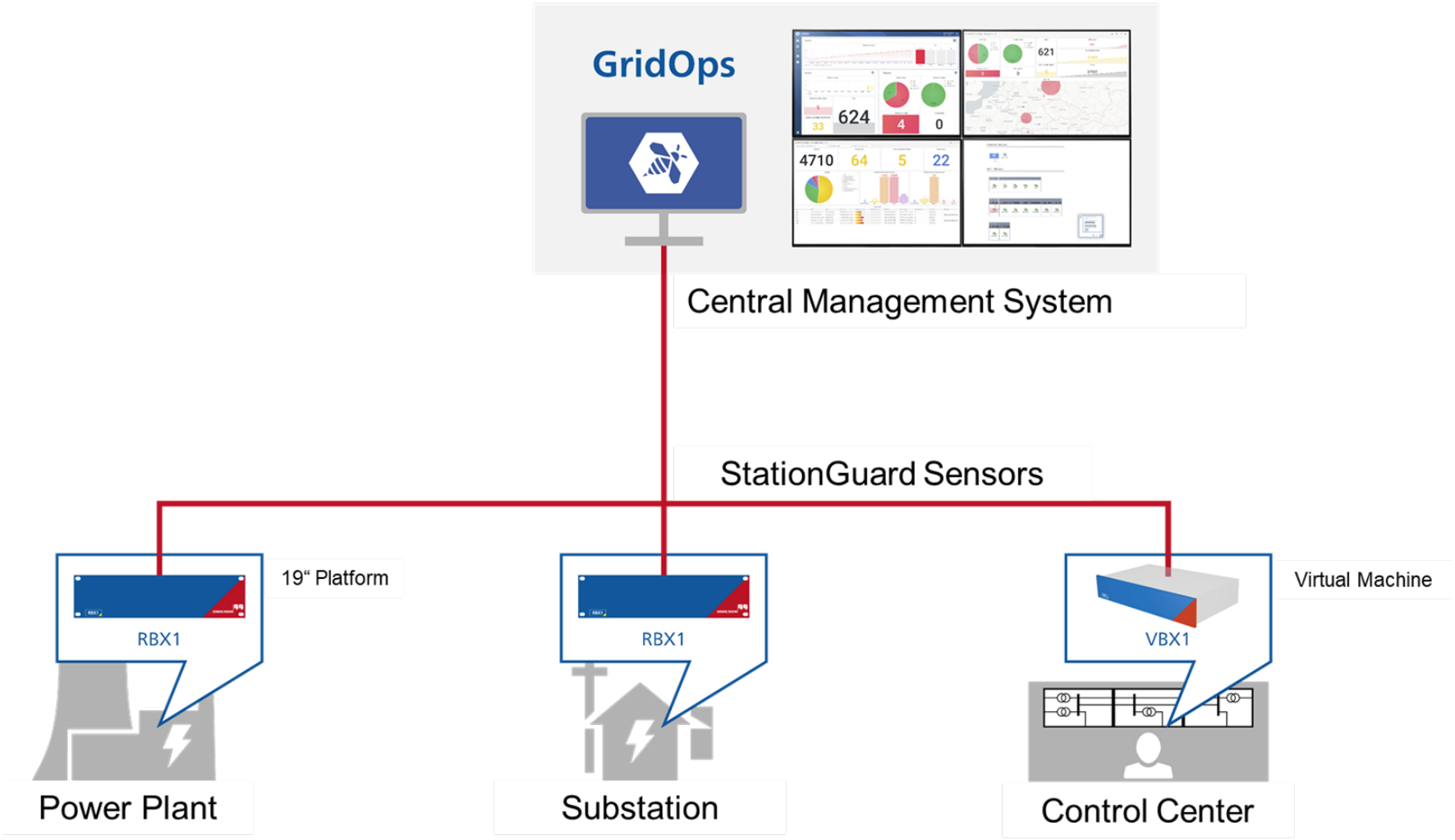
- **SST** System Specification Tool
- **ICT** IED Configuration Tool
- **SCT** System Configuration Tool



OMICRON’s StationGuard: A Solution for Vulnerability and Asset Inventory Management based on CSAF and IEC61850

OMICRON's Industrial Cybersecurity Solution

- **Tailor-made for utility automation and control systems**
- **Speaks the language of protection and control engineers**
- **Identifies malfunctions in the system**



How StationGuard Protects Critical Infrastructure

Visibility

- Makes communication and cyber risks visible

Asset inventory

- Works with the most precise and detailed list of assets

Vulnerability management

- Provides over- and insight into your device vulnerabilities

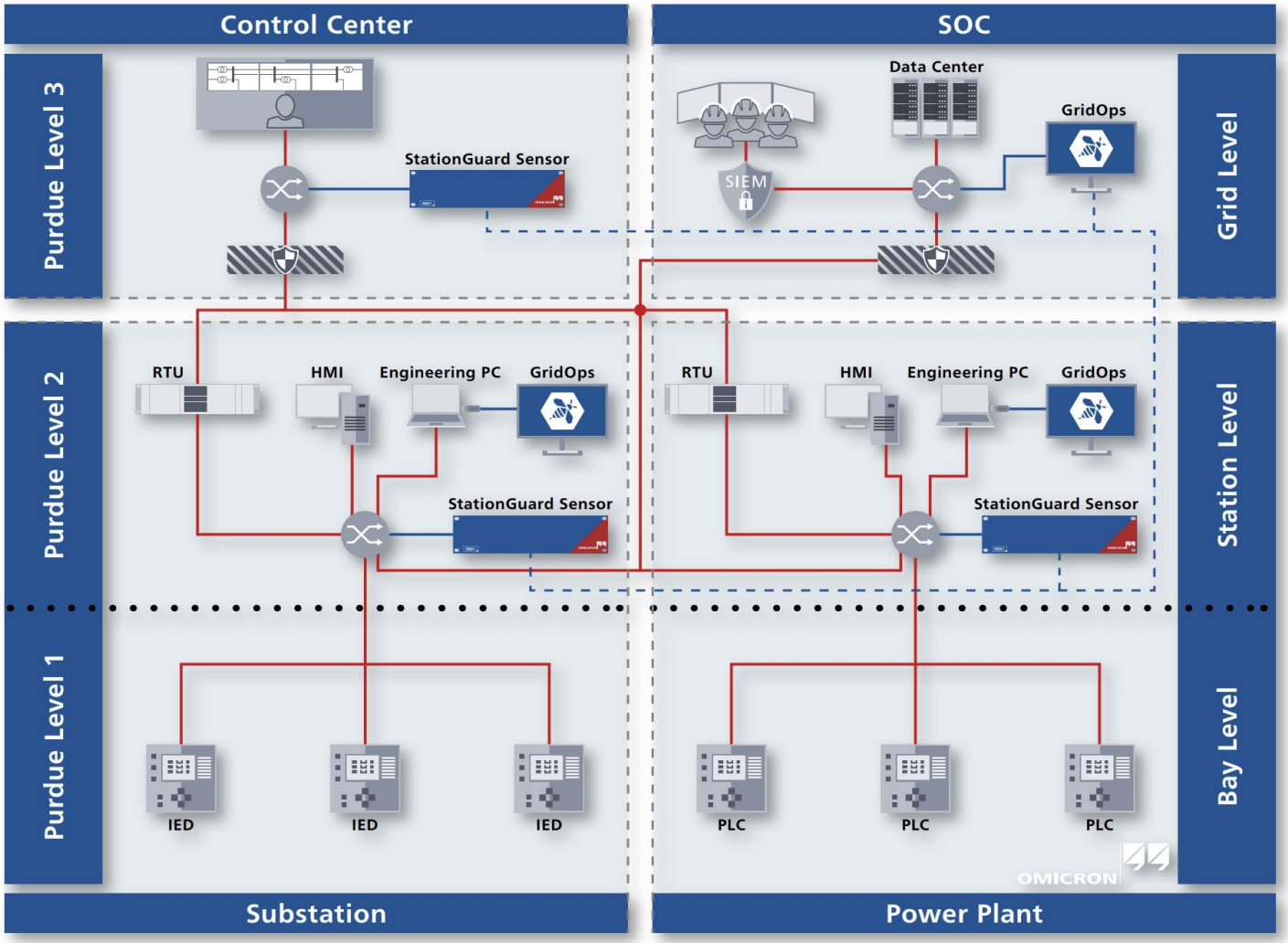
Intrusion detection

- Built-in ICS knowledge enables fewer false alarms, easier analysis, and faster response

Functional monitoring

- Detect malfunctions and configuration errors

How to integrate StationGuard?

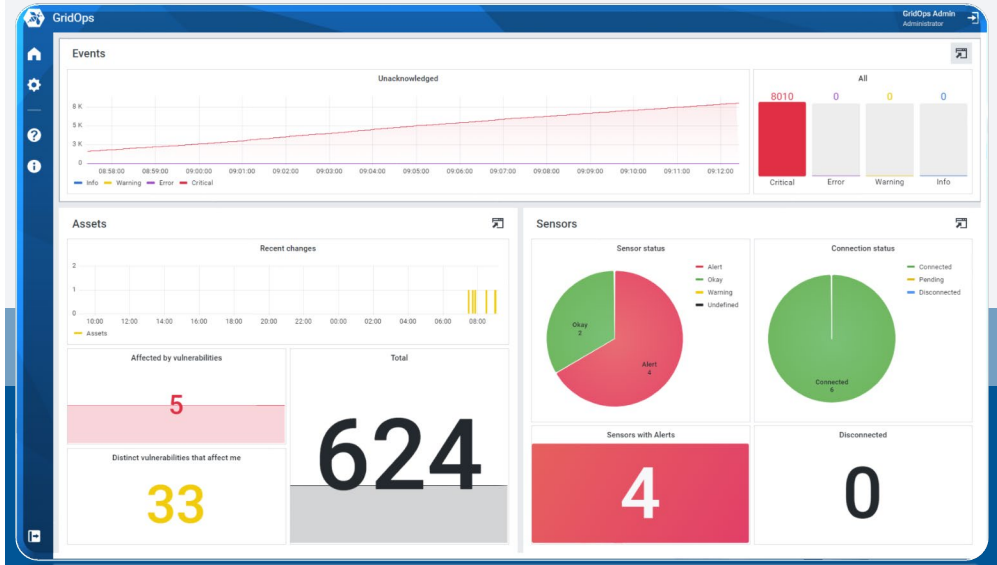


StationGuard Deployment Diagram

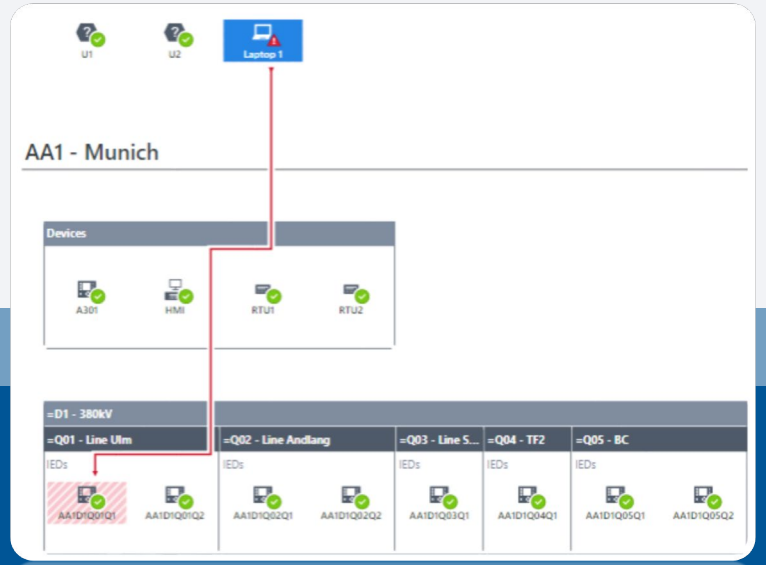
- Central management system: GridOps
  - Which plants show an alarm?
  - Asset inventory and vulnerability management
- StationGuard Sensors can be used in
  - Control centers
  - Power plants
  - Substations

How StationGuard is securing the Critical Infrastructure

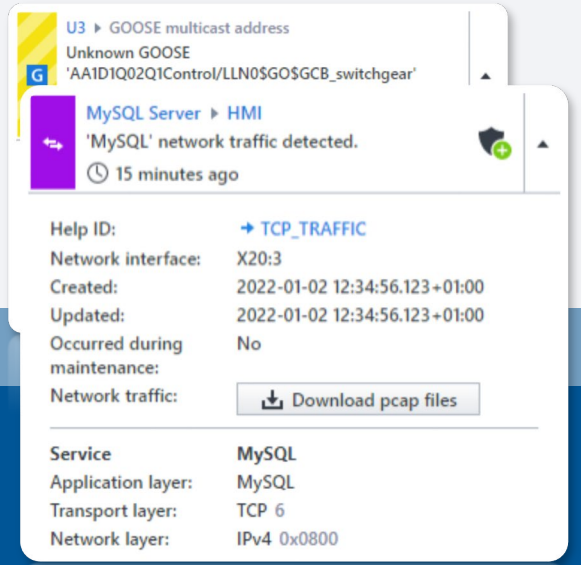
Grid level
Multiple dashboards to provide overview on the status of all your networks



Plant level
Intuitive network visualization



Communication
Visualize assets and their communication



Zero Line Diagram to Purdue Model Mapping

Control center level
= Purdue level 3

Control center

MUC-SCADA | MUC-Control | NU-SCADA | NU-Control

Station control level
= Purdue level 2

AA1 - Munich

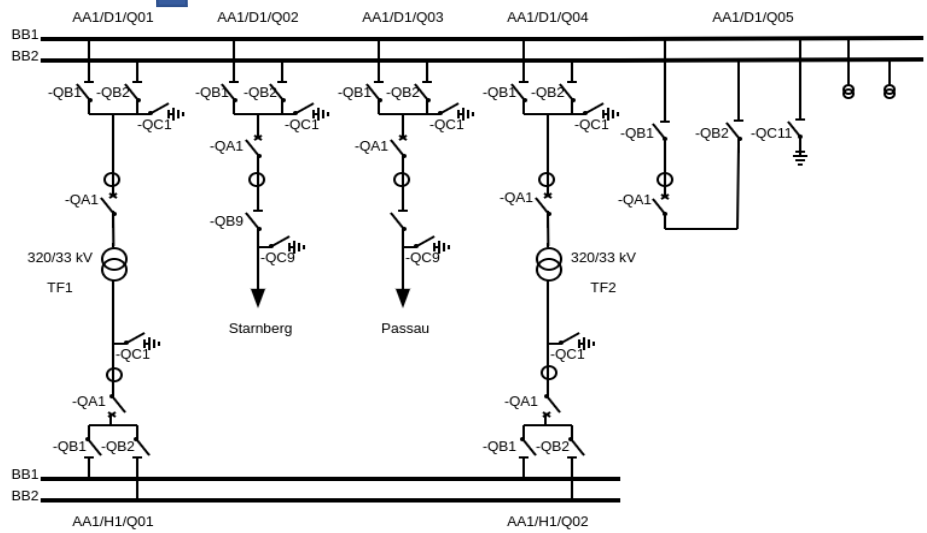
Devices
BB_PROT
HMI
PCPQS1
RTU1
RTU2

Bays and voltage levels
= Purdue level 1

=D1 - 320kV				
=Q01 - TF1	=Q02 - Line S...	=Q03 - Line p...	=Q04 - TF2	=Q05 - ISIO 2...
IEDs	IEDs	IEDs	IEDs	IEDs
AA1D1Q01Q1	AA1D1Q02Q1	AA1D1Q03Q1	AA1D1Q04Q1	AA1D1Q05Q1

=H1 - 33kV	
=Q01 - TF1LV	=Q02 - TF2LV
IEDs	IEDs
AA1D1H01Q1	AA1D1H02Q1

.scd, iid,
.icd, .cid,



#OmaintecConf

StationGuard knows the Substation

From '20230131_NUCBX1_without_AA1D1Q03Q1_report_arrows.scd'

IEC 61850 MMS permissions

MMS Accept connection	HMI
MMS Accept connection	RTU1
MMS Allow usage of any report	HMI
MMS Allow usage of any report	RTU1
MMS Transmit report on request	HMI
MMS Transmit report on request	RTU1
R Send report	HMI
R Send report	RTU1

IEC 61850 GOOSE permissions

G Send 'LD0/LLN0.gcb_protection'	01:0C:CD:01:00:0A
G Send 'LD0/LLN0.gcb_switchgear'	01:0C:CD:01:00:0A

Permissions

Exceptions

Communication permissions

Communicate over FTP (TCP)	RTU1
Communicate over Siemens DIGSI 4 (UDP)	AA1D1Q01Q1

Roles

Communication permissions for all known devices

Communication permissions for 'Testing PC'

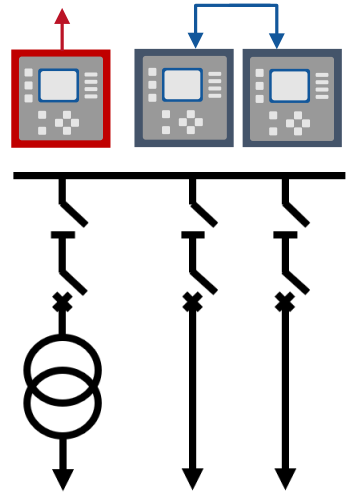
... over 802.1 Link Layer Discovery Protocol (LLDP)	Any LLDP multicast
Communicate over IPv6	DHCPv6 multicast
Communicate over IPv6	Any IPv6 multicast
Communicate over DHCP Server (UDP)	Any broadcast
Communicate over HTTP (TCP)	IEC 61850 Test Set
Communicate over ICMP	Controlling RTU, Engineering...
Communicate over ICMP	Controlling RTU, Engineering...
Communicate over IGMP	Any IPv4 multicast
Communicate over LLMNR (UDP)	Any IPv4 multicast
Communicate over mDNS (UDP)	Any IPv4 multicast
Communicate over netbios-ns (UDP)	Any broadcast
Communicate over netbios-ns (UDP)	Any broadcast
Communicate over NTP (UDP)	Time Server

AA1D1Q02Q2

Disconnector control unit Q02 - Starnberg

Details

Status:	OK
Vendor:	ACME
Model:	PROTEC 400
Hardware version:	8AK86-AAAA-AA0-0AAAA0-AB0123-32123A-AAA000...
Software version:	v0.123



#OmaintecConf

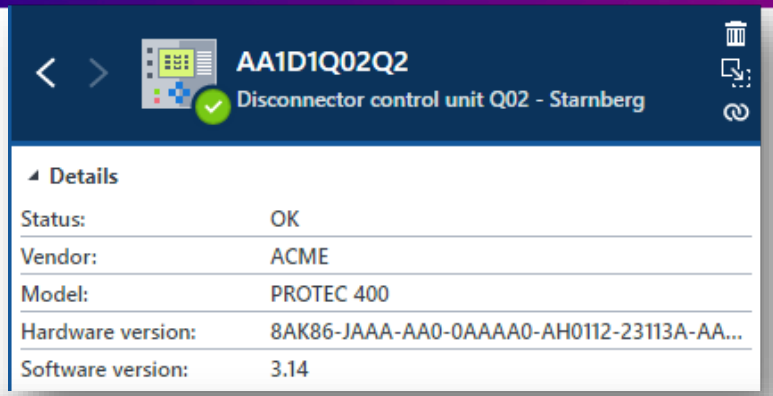
Automatic Asset Creation with StationGuard

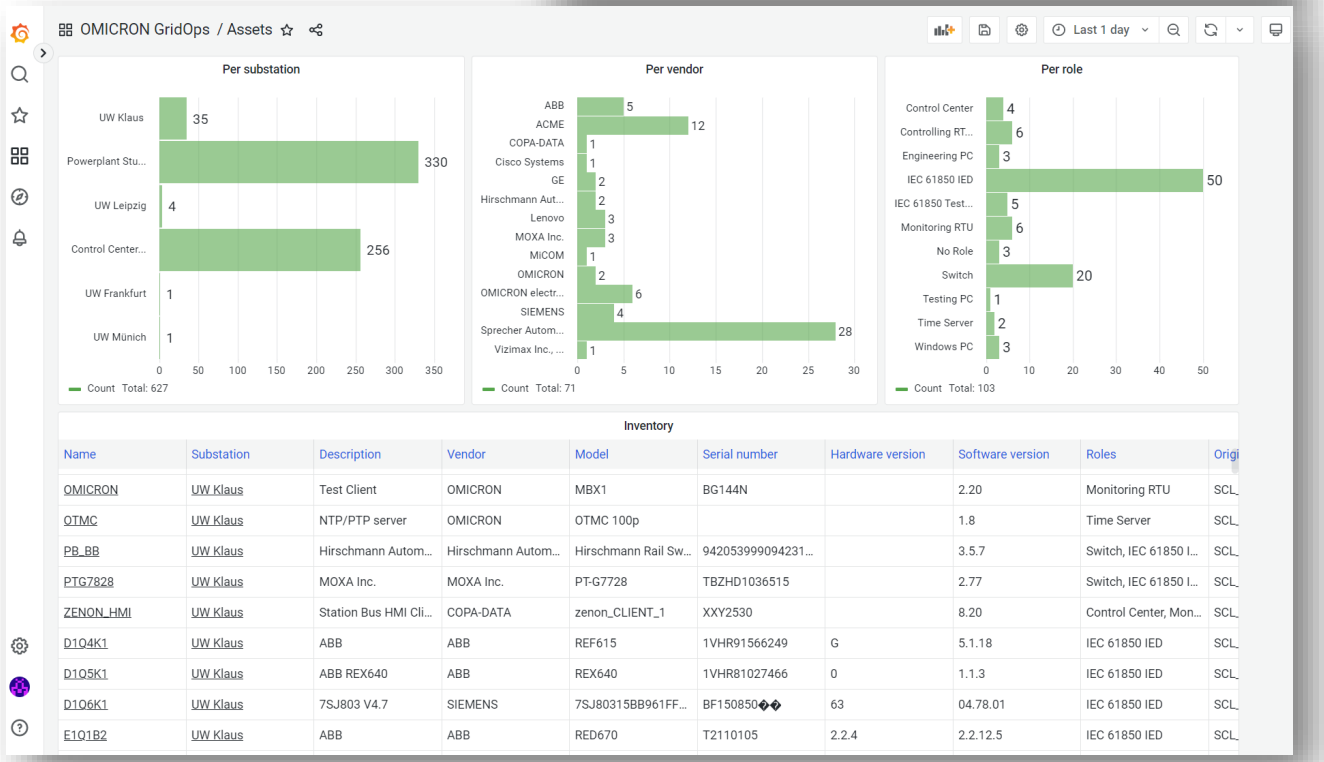
StationGuard collects asset information from

- **Passive discovery** from network
- Engineering files: **IEC61850 SCL** and **CSV**
- Active Device interrogation (IEC61850 **MMS**)

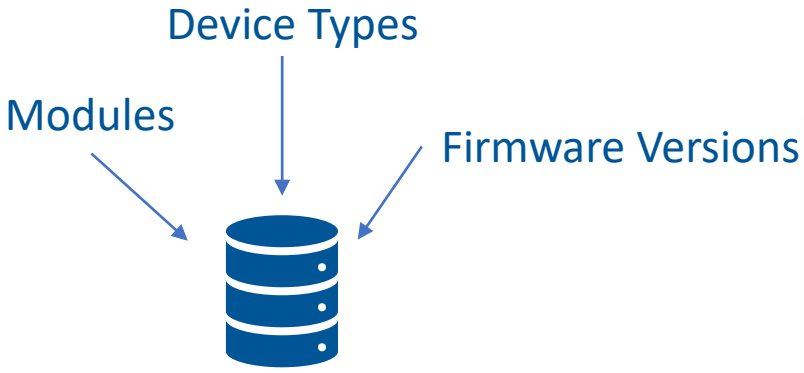
Export and import to synchronize with other systems

- ERP Systems
- OT Processes: OMICRON ADMO

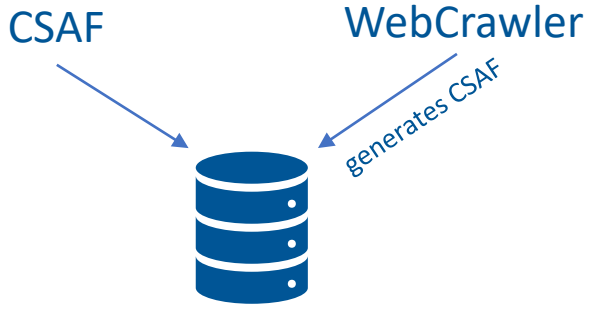




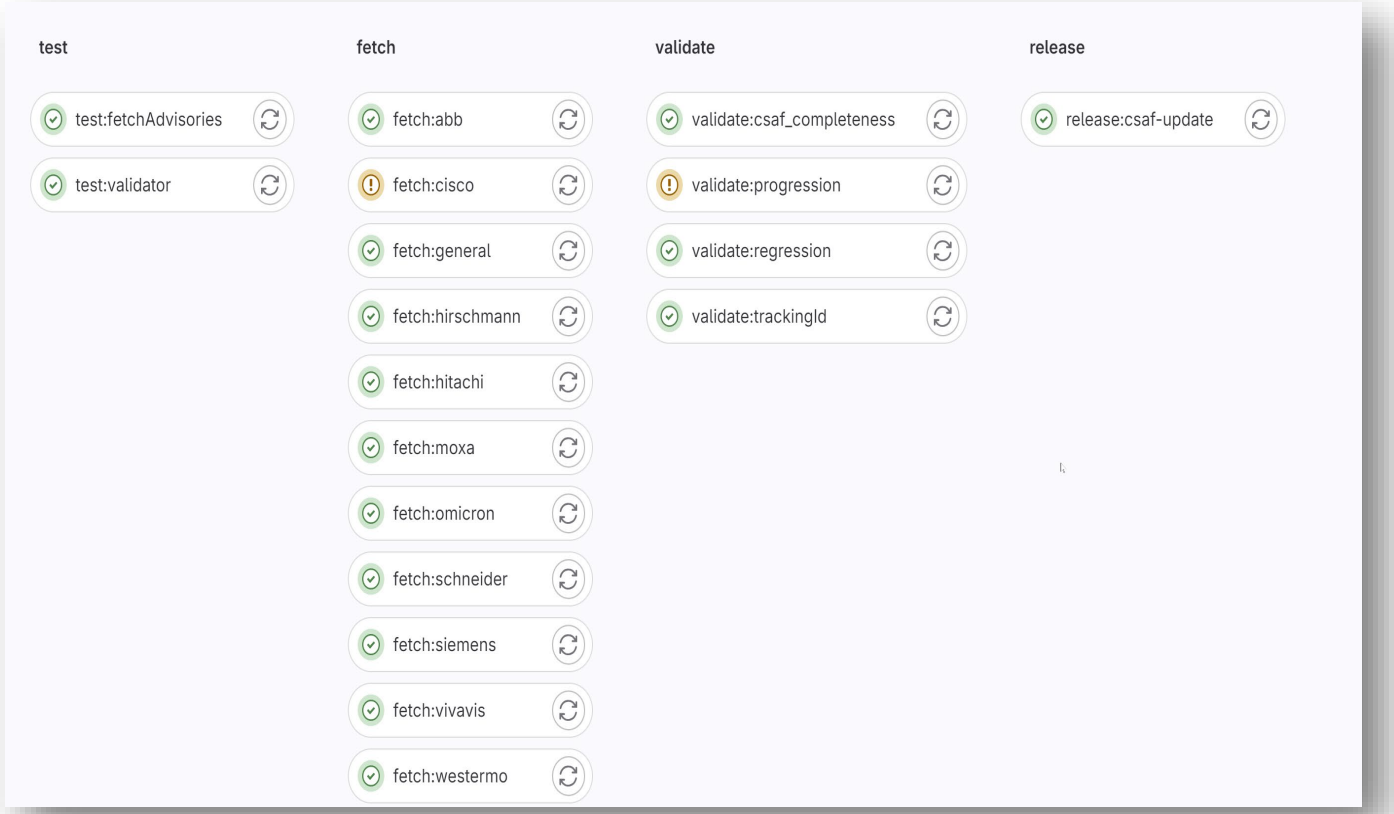
Vulnerability and IED Type Database: How We Construct It



Device Type Database



Vulnerability Database

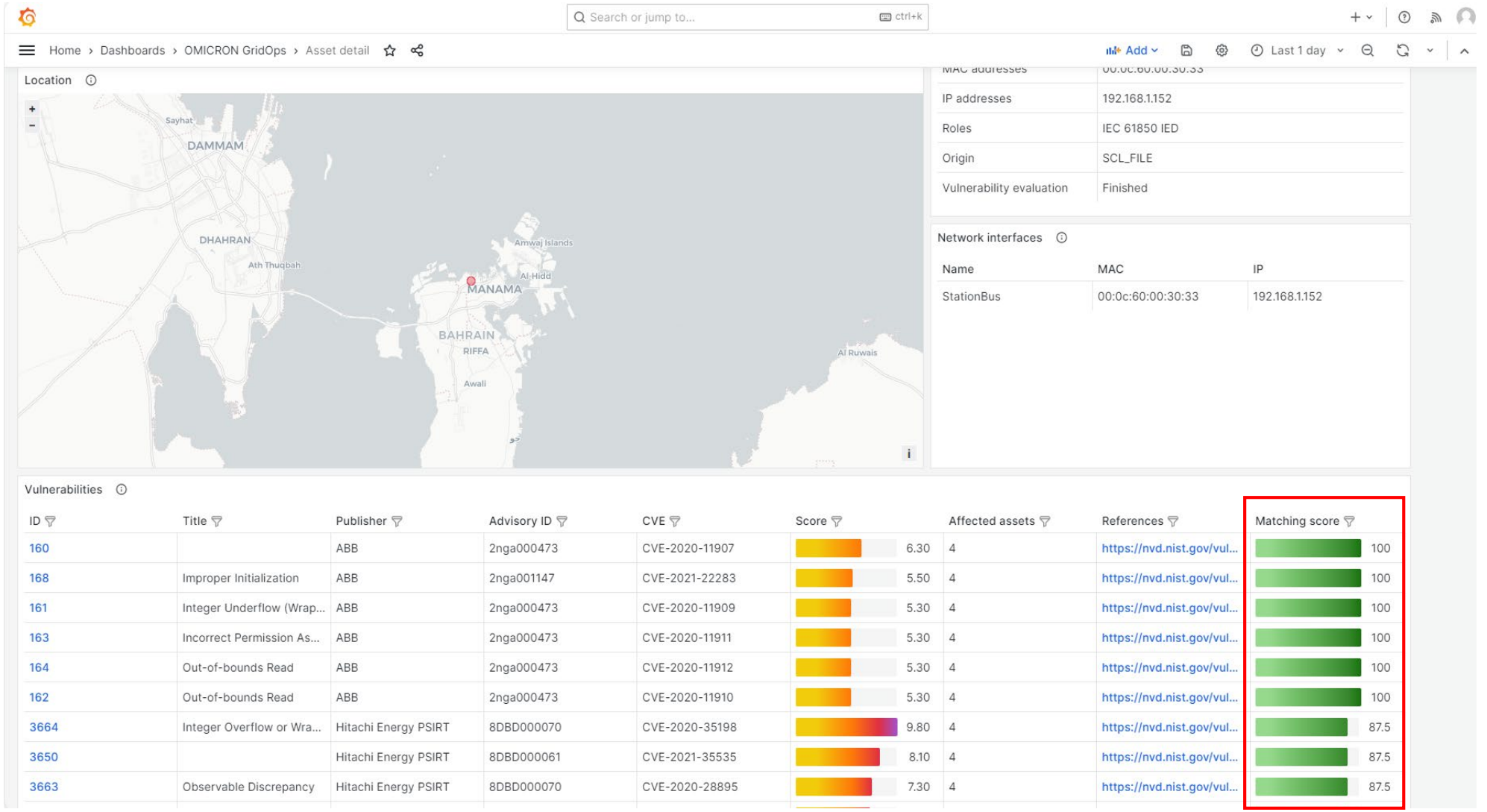


CSAF Crawler Pipeline

Vulnerability Matching Problem: How We Approach It

- OMICRON Vulnerability Database: A Rich Source of Device Meta Information.

- Only the pertinent vulnerabilities are displayed automatically.



ID	Title	Publisher	Advisory ID	CVE	Score	Affected assets	References	Matching score
160		ABB	2nga000473	CVE-2020-11907	6.30	4	https://nvd.nist.gov/vul...	100
168	Improper Initialization	ABB	2nga001147	CVE-2021-22283	5.50	4	https://nvd.nist.gov/vul...	100
161	Integer Underflow (Wrap...	ABB	2nga000473	CVE-2020-11909	5.30	4	https://nvd.nist.gov/vul...	100
163	Incorrect Permission As...	ABB	2nga000473	CVE-2020-11911	5.30	4	https://nvd.nist.gov/vul...	100
164	Out-of-bounds Read	ABB	2nga000473	CVE-2020-11912	5.30	4	https://nvd.nist.gov/vul...	100
162	Out-of-bounds Read	ABB	2nga000473	CVE-2020-11910	5.30	4	https://nvd.nist.gov/vul...	100
3664	Integer Overflow or Wra...	Hitachi Energy PSIRT	8DBD000070	CVE-2020-35198	9.80	4	https://nvd.nist.gov/vul...	87.5
3650		Hitachi Energy PSIRT	8DBD000061	CVE-2021-35535	8.10	4	https://nvd.nist.gov/vul...	87.5
3663	Observable Discrepancy	Hitachi Energy PSIRT	8DBD000070	CVE-2020-28895	7.30	4	https://nvd.nist.gov/vul...	87.5

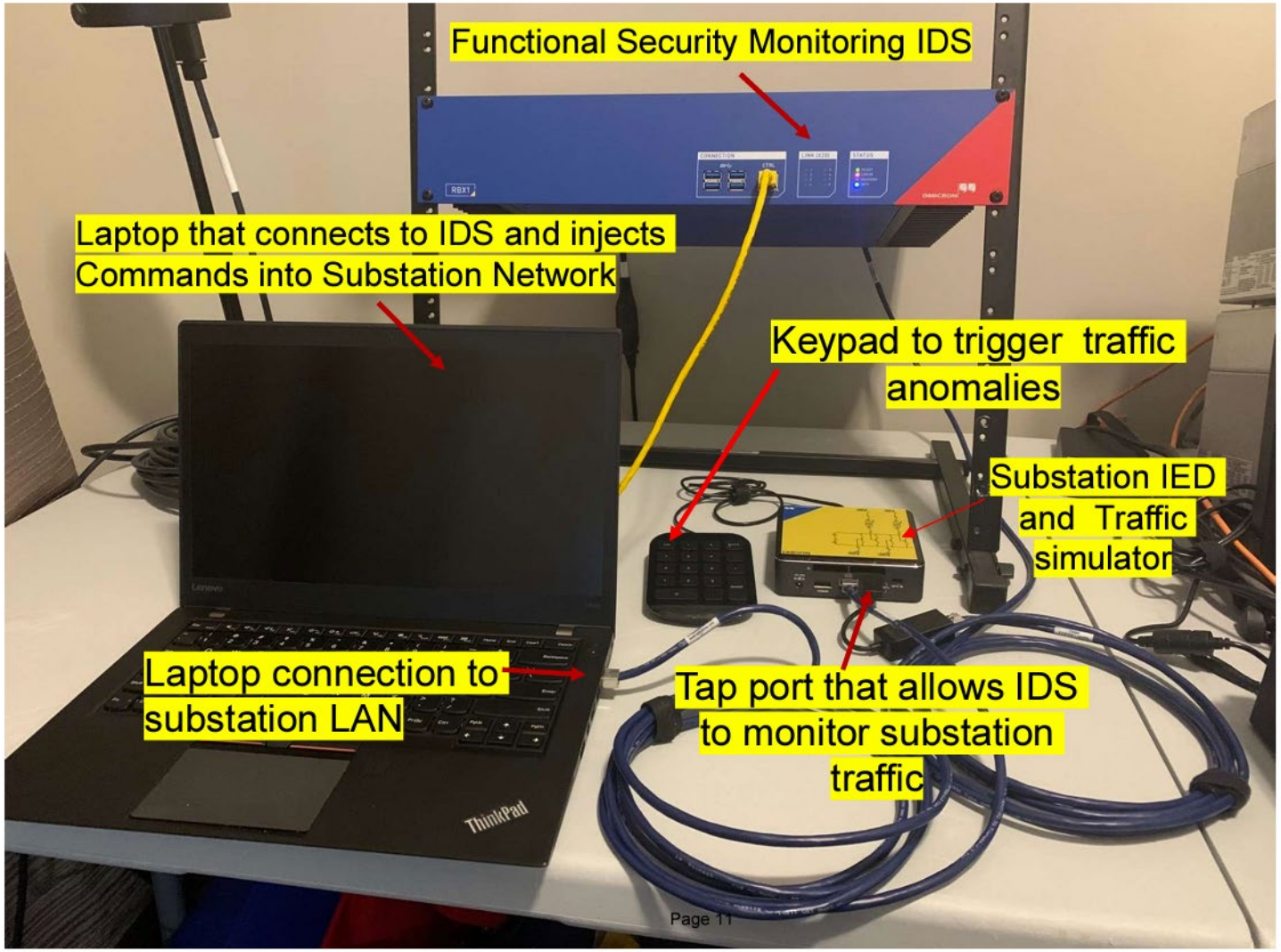
Benefits of 24/7 Functional Monitoring

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

Severity	Date and time	Message
⚠	2022-06-02 18:10:57.835+03:00	G AA1D1Q03Q2 ▸ GOOSE multicast address Restart of GOOSE 'AA1D1Q03Q2CONTROL/LLN0GOQC9' detected.
⚠	2022-06-02 18:10:57.835+03:00	G AA1D1Q03Q2 ▸ GOOSE multicast address Restart of GOOSE 'AA1D1Q03Q2CONTROL/LLN0GOQB9' detected.
⚠	2022-06-02 18:10:57.825+03:00	G AA1D1Q03Q1 ▸ GOOSE multicast address Restart of GOOSE 'AA1D1Q03Q1CONTROL/LLN0GOgcb' detected.
⚠	2022-06-02 18:10:57.825+03:00	G AA1D1Q03Q1 ▸ GOOSE multicast address IED indicates time synchronization failure (ClockNotSynchronized) in GOOSE 'AA1D1Q03Q1CONTROL/LLN0GOgcb'.
⚠	2022-06-02 18:10:17.818+03:00	G AA1D1Q01Q1 ▸ GOOSE multicast address Restart of GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear' detected.
⚠	2022-06-02 18:10:17.818+03:00	G AA1D1Q01Q1 ▸ GOOSE multicast address Unexpected VLAN identifier in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2022-06-02 18:10:17.818+03:00	G AA1D1Q01Q1 ▸ GOOSE multicast address Configuration revision (ConfRev) newer than expected in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.
⚠	2022-06-02 18:10:17.818+03:00	G AA1D1Q01Q1 ▸ GOOSE multicast address Wrong destination MAC address in GOOSE 'AA1D1Q01Q1LD0/LLN0GOgcb_switchgear'.

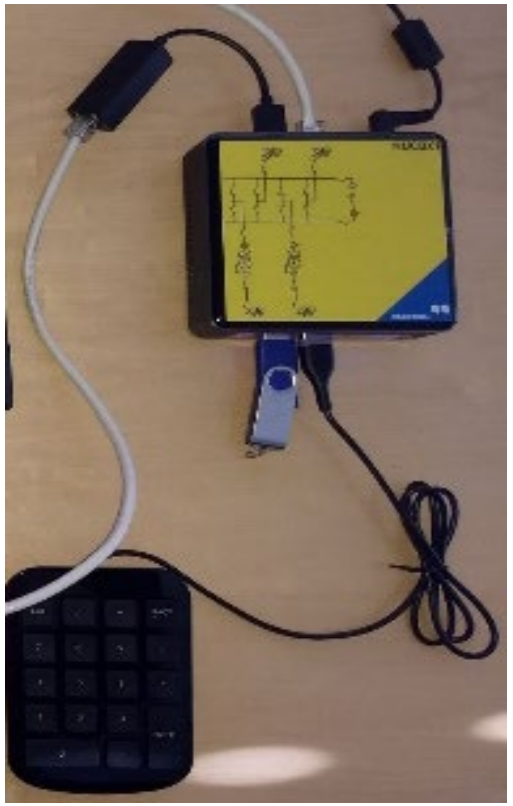

CONFERENCE
OMAINTEC
2024
EXHIBITION
StationGuard in Action
#OmaintecConf

Live Demo – Physical Connectivity



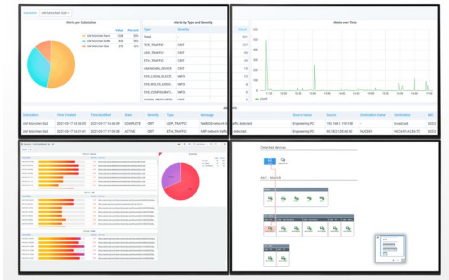
Live Demo – Network Architecture

Substation Simulator



StationGuard Desktop

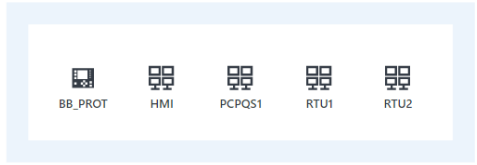
GridOps

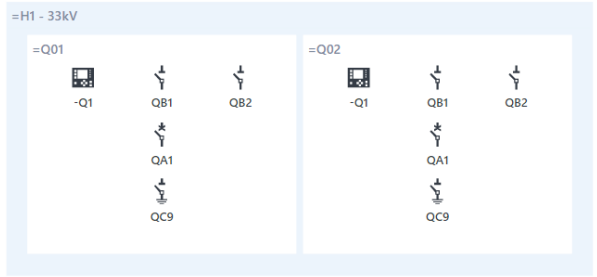


Switch Port

StationGuard

Mirror Port





#OmaintecConf

OMAINTEC CONFERENCE EXHIBITION 2024

THE 21ST INTERNATIONAL OPERATIONS & MAINTENANCE CONFERENCE IN THE ARAB COUNTRIES

THANK YOU!

Protect Your Grid by OMICRON

#OmaintecConf

An Initiative by

OMAINTEC
المجلس العربي للتشغيل والصيانة
Arab Operations & Maintenance Council

Organized by

EXICON.
International Group
مجموعة أكزيكون الدولية