IEC 61850 and Cybersecurity : Testing Solutions review

Hennie Pretorius

March 2024

OMICRON Academy

IEC 61850

What is 61850 ?

defines **communication protocols to provide communication between different** equipment located in a substation

standard series and associated extensions is **a leading standard technology. Governing the interoperability in the Power Utility automation**

IEC 61850 is an international standard defining communication protocols for intelligent electronic devices at electrical substations. It is a part of the International Electrotechnical Commission's Technical Committee 57 reference architecture for electric power systems. Wikipedia

The concept of virtualization

REAL WORLD

real function

circuit breaker

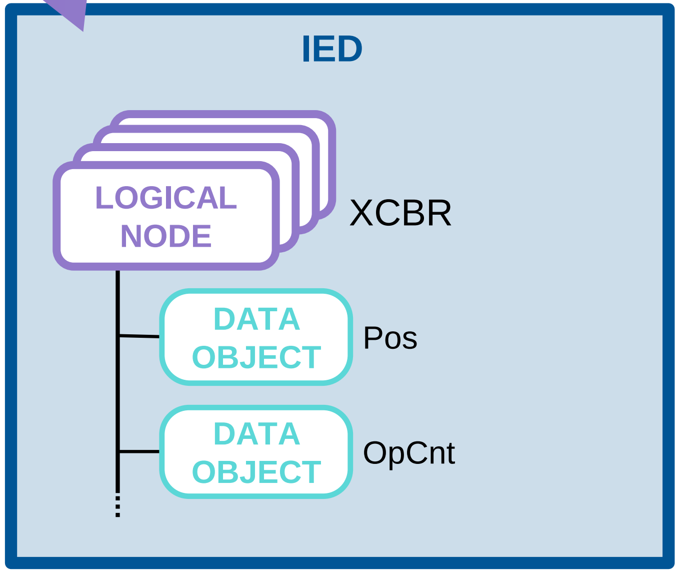
virtualization

VIRTUAL WORLD

modelled as

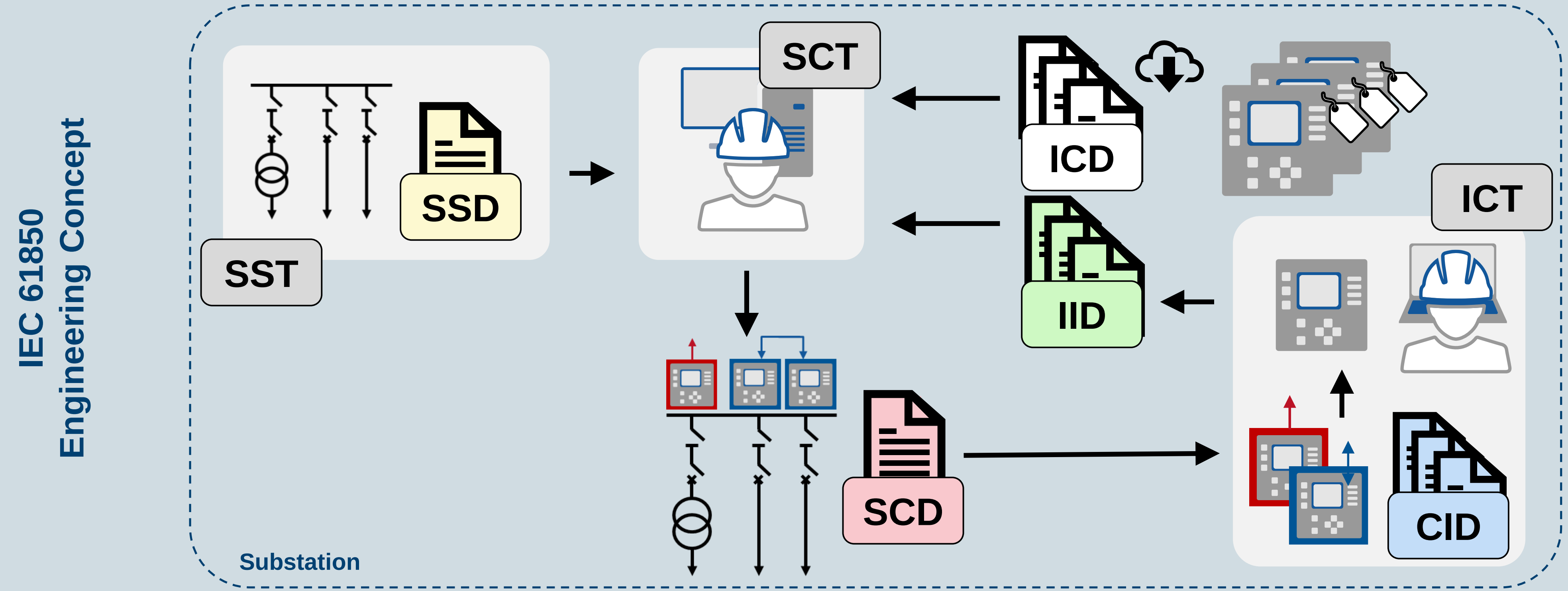
Logical Node

in the **Data Model**

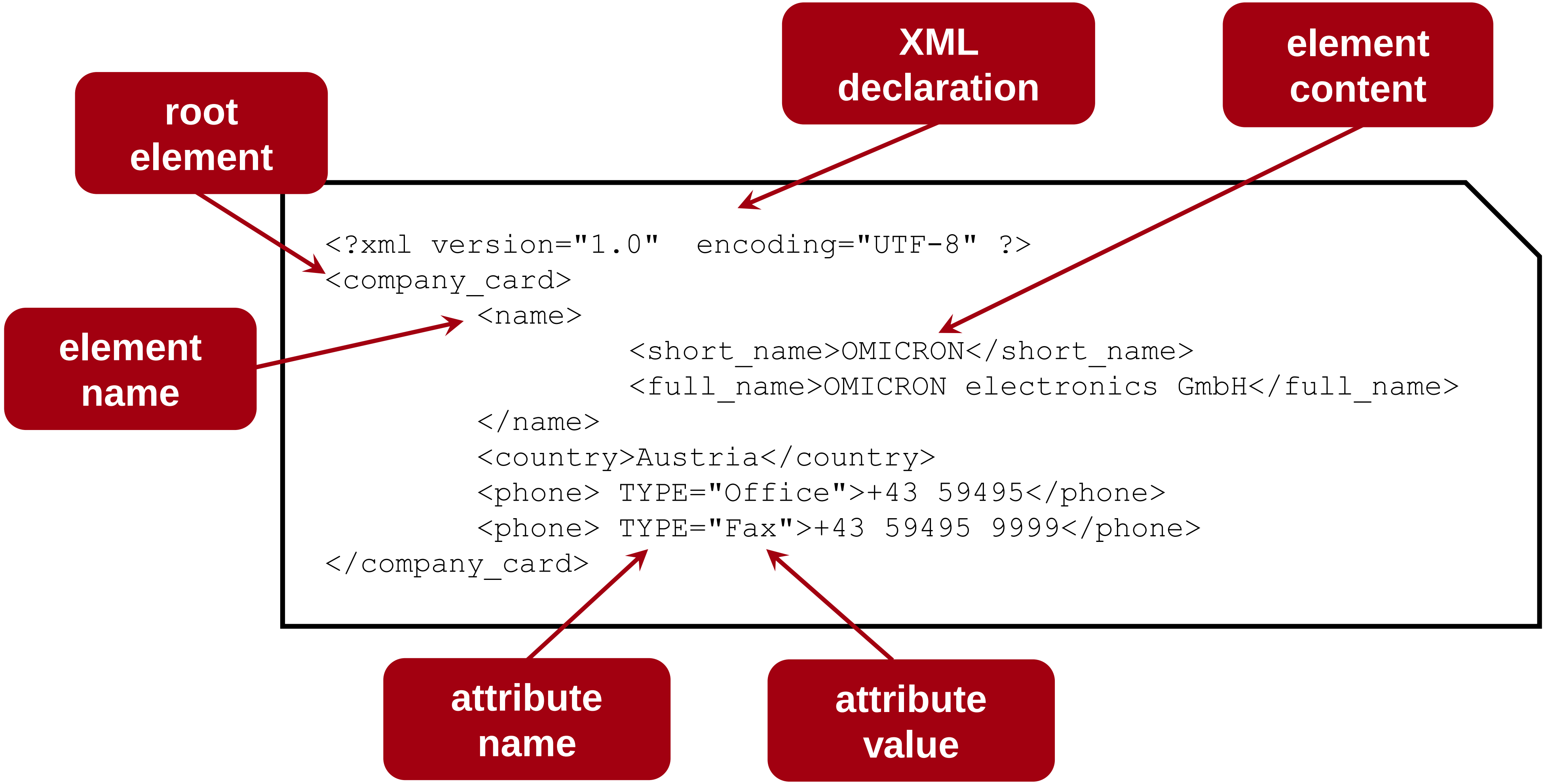


Engineering concept based on SCL

SST	System Specification Tool	ICD	IED Capability Description
SCT	System Configuration Tool	SCD	System Configuration Description
ICT	IED Configuration Tool	CID	Configured IED Description
SSD	System Specification Description	IID	Instantiated IED Description



What is XML?



root element

XML declaration

element content

element name

```
<?xml version="1.0"  encoding="UTF-8" ?>
<company_card>
        <name>
                <short_name>OMICRON</short_name>
                <full_name>OMICRON electronics GmbH</full_name>
        </name>
        <country>Austria</country>
        <phone> TYPE="Office">+43 59495</phone>
        <phone> TYPE="Fax">+43 59495 9999</phone>
</company_card>
```

attribute name

attribute value

IEDScout

Versatile Software Tool for Working with IEC 61850 Devices

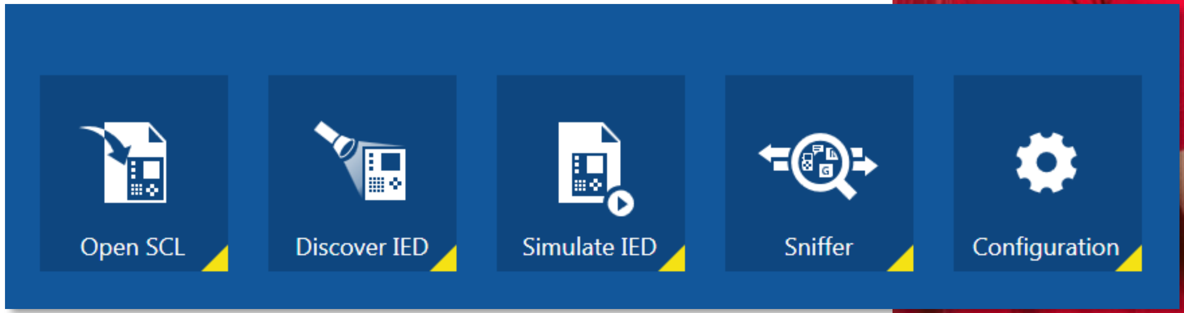
Examine IEC 61850 devices

IEDScout is...

- a universal client to IEC 61850 servers,
- an analyzing tool for client/server traffic and GOOSE messages, and
- a simulation tool for the communication features of IEC 61850 servers.

The software is used in substations and laboratories for:

- Testing
- Troubleshooting
- Commissioning
- IED development

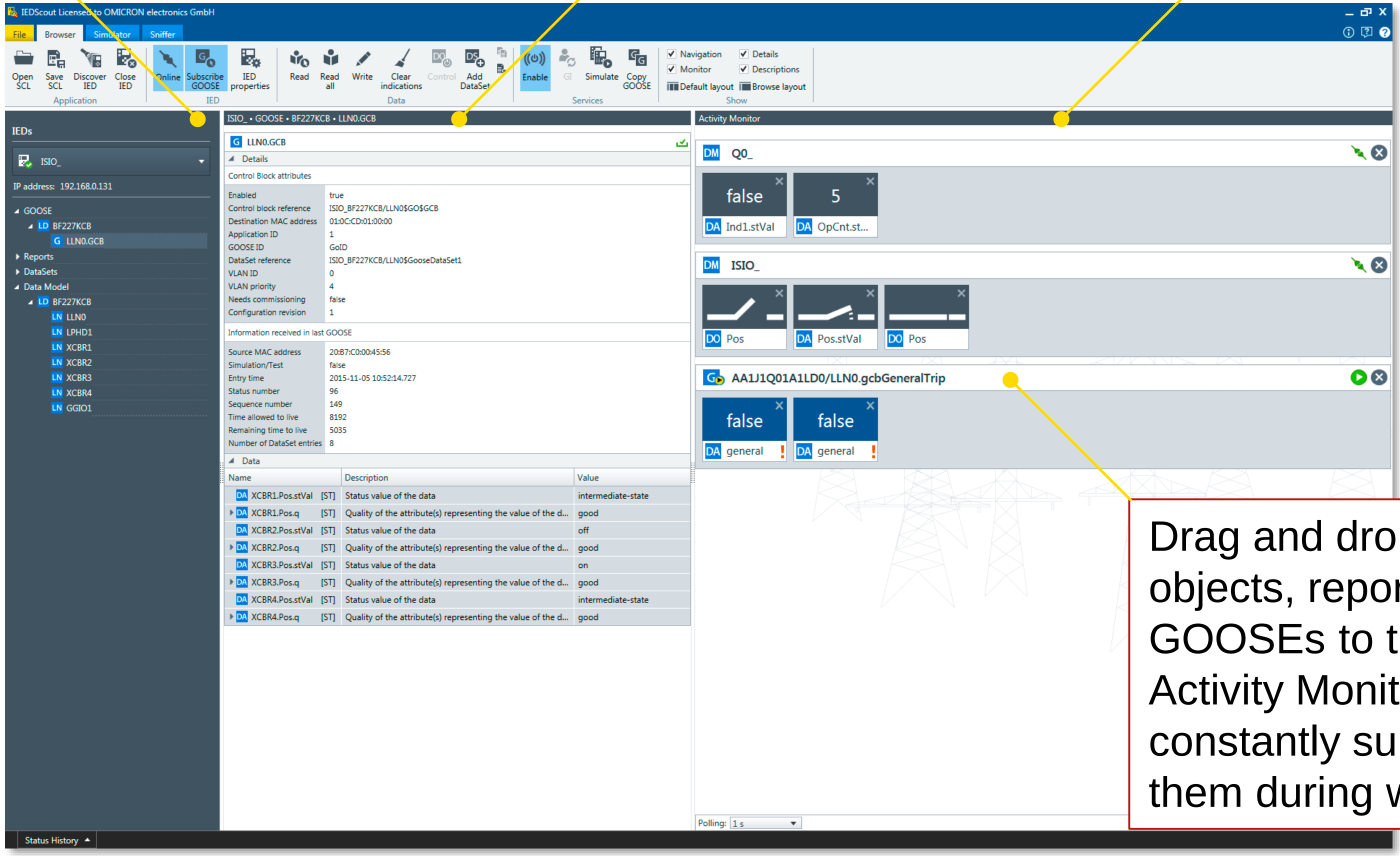


Unveil the inside of IEC 61850 devices

Navigation

Details view

Activity Monitor



ISIO_ • GOOSE • BF227KCB • LLN0.GCB

G LLN0.GCB

Details

Control Block attributes

Enabled	true
Control block reference	ISIO_BF227KCB/LLN0$GO$GCB
Destination MAC address	01:0C:CD:01:00:00
Application ID	1
GOOSE ID	GoID
DataSet reference	ISIO_BF227KCB/LLN0$GooseDataSet1
VLAN ID	0
VLAN priority	4
Needs commissioning	false
Configuration revision	1

Information received in last GOOSE

Source MAC address	20:B7:C0:00:45:56
Simulation/Test	false
Entry time	2015-11-05 10:52:14.727
Status number	96
Sequence number	149
Time allowed to live	8192
Remaining time to live	5035
Number of DataSet entries	8

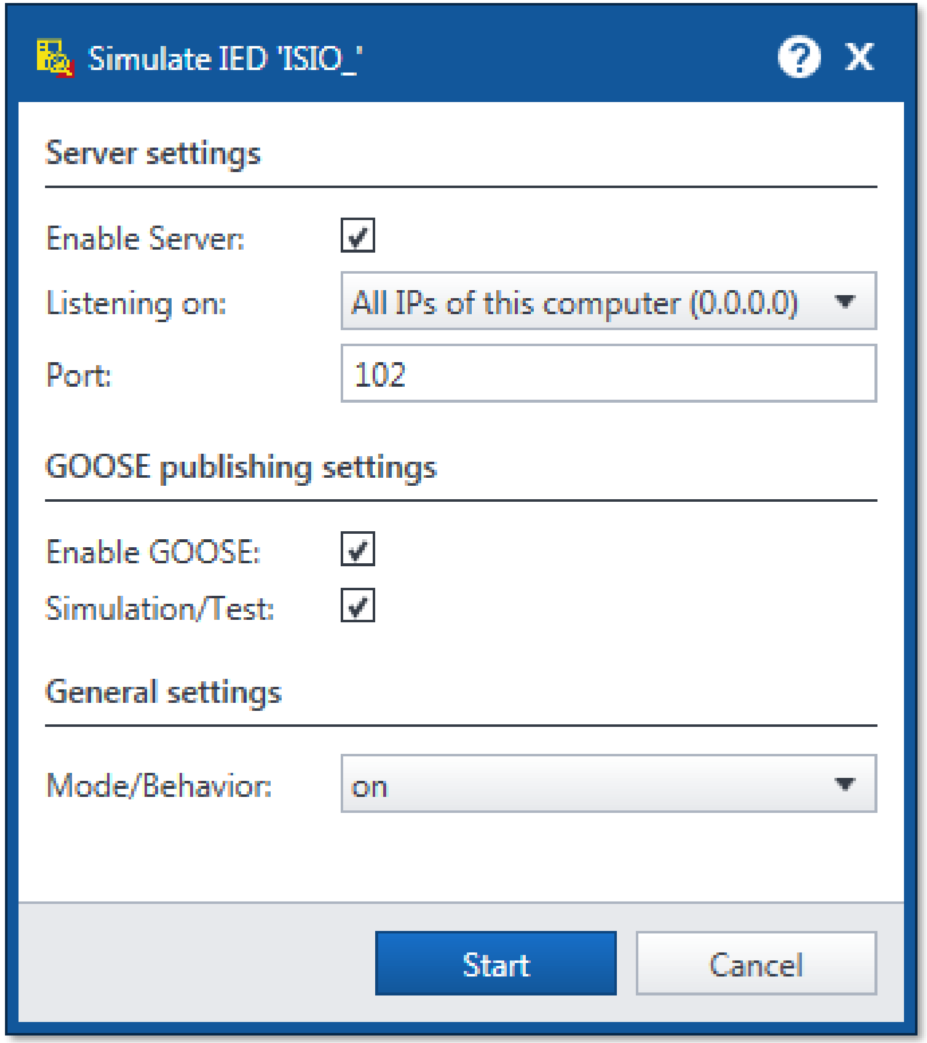
Data

Name		Description	Value
DA XCBR1.Pos.stVal	[ST]	Status value of the data	intermediate-state
DA XCBR1.Pos.q	[ST]	Quality of the attribute(s) representing the value of the d...	good
DA XCBR2.Pos.stVal	[ST]	Status value of the data	off
DA XCBR2.Pos.q	[ST]	Quality of the attribute(s) representing the value of the d...	good
DA XCBR3.Pos.stVal	[ST]	Status value of the data	on
DA XCBR3.Pos.q	[ST]	Quality of the attribute(s) representing the value of the d...	good
DA XCBR4.Pos.stVal	[ST]	Status value of the data	intermediate-state
DA XCBR4.Pos.q	[ST]	Quality of the attribute(s) representing the value of the d...	good

Drag and drop data objects, reports, and GOOSEs to the Activity Monitor to constantly supervise them during work

Simulate IEDs

- Simulate entire IEC 6150 Ed.2 and Ed.1 IEDs
- You can easily modify the configuration of the simulated GOOSE and reports. Changing data values in the simulated IED automatically triggers GOOSE and reports.
- You only need an SCL file to simulate most of the IEC 61850 communication aspects of an IED.
- Support of test modes as well as simulation indication for GOOSE



Simulate IED 'ISIO_'

Server settings

Enable Server: ☑

Listening on: All IPs of this computer (0.0.0.0)

Port: 102

GOOSE publishing settings

Enable GOOSE: ☑

Simulation/Test: ☑

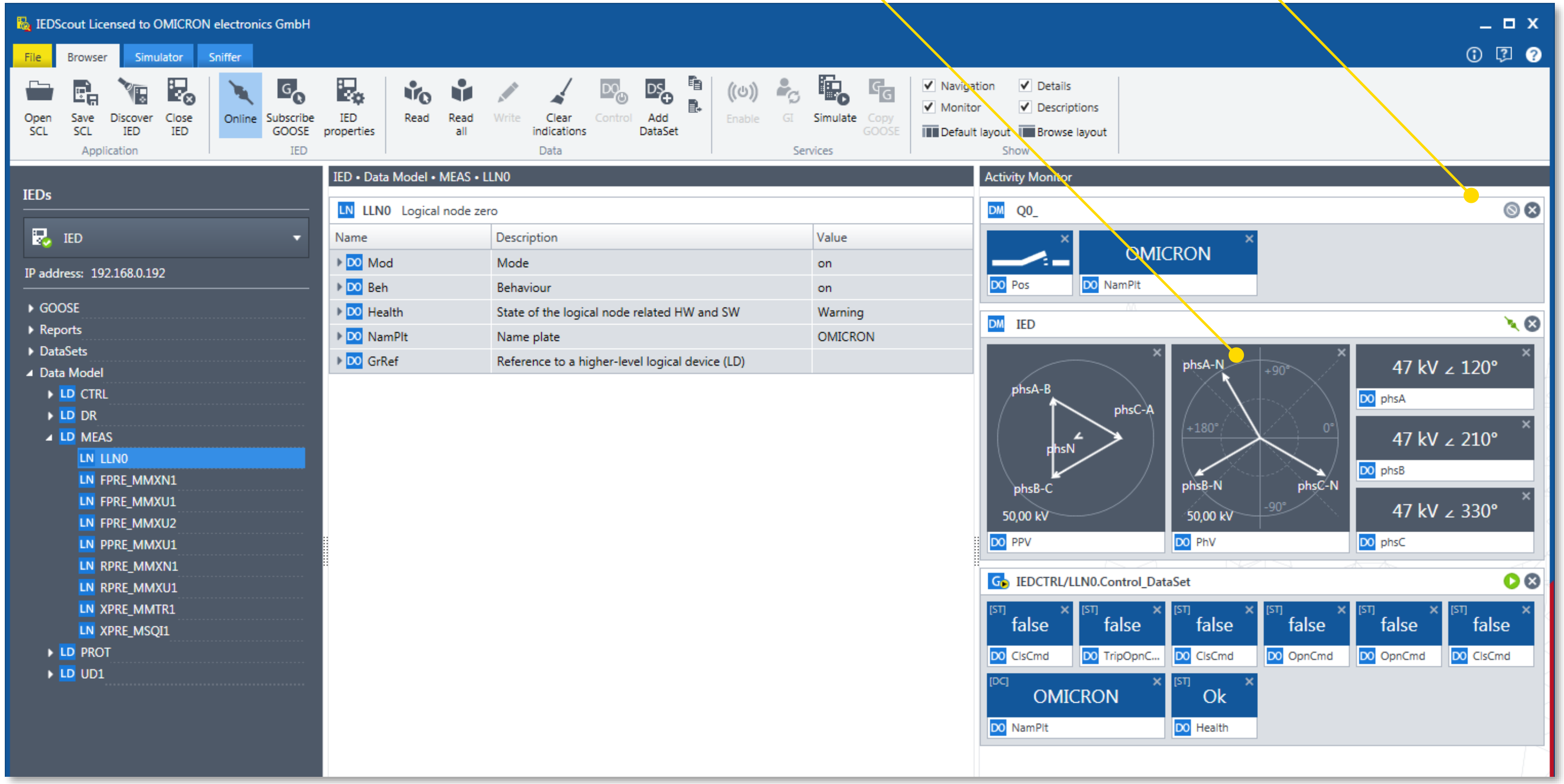
General settings

Mode/Behavior: on

Activity Monitor combination

Observed IED

Simulated IED



IP address: 192.168.0.192

- GOOSE
- Reports
- DataSets
- Data Model
  - LD CTRL
  - LD DR
  - LD MEAS
    - LN LLN0
    - LN FPRE_MMXN1
    - LN FPRE_MMXU1
    - LN FPRE_MMXU2
    - LN PPRE_MMXU1
    - LN RPRE_MMXN1
    - LN RPRE_MMXU1
    - LN XPRE_MMTR1
    - LN XPRE_MSQI1
  - LD PROT
  - LD UD1

IED • Data Model • MEAS • LLN0

LN LLN0 Logical node zero

Name	Description	Value
DO Mod	Mode	on
DO Beh	Behaviour	on
DO Health	State of the logical node related HW and SW	Warning
DO NamPlt	Name plate	OMICRON
DO GrRef	Reference to a higher-level logical device (LD)	

Activity Monitor

DM Q0_

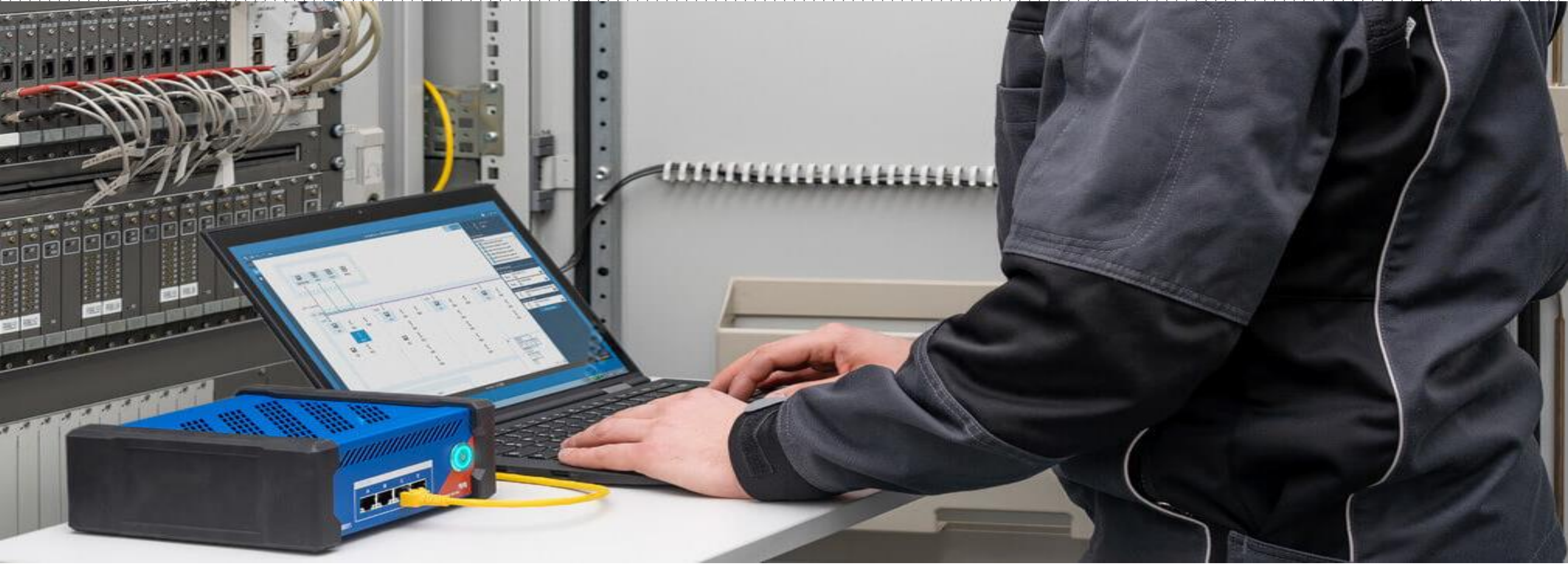
	OMICRON
DO Pos	DO NamPlt

DM IED

		47 kV ∠ 120°
DO PPV	DO PhV	DO phsA
		47 kV ∠ 210°
		DO phsB
		47 kV ∠ 330°
		DO phsC

IEDCTRL/LLN0.Control_DataSet

[ST] false	[ST] false	[ST] false	[ST] false	[ST] false	[ST] false
DO ClsCmd	DO TripOpnC...	DO ClsCmd	DO OpnCmd	DO OpnCmd	DO ClsCmd
[DC] OMICRON	[ST] Ok				
DO NamPlt	DO Health				



StationScout

Simplified testing for Substation Automation Systems…

- © OMICRON

StationScout

➢Software or hardware?

Yes, StationScout is a combination of

- Software(**StationScout**)
- Hardware(**PC)**
- Test set (**MBX1** / **RBX1**)

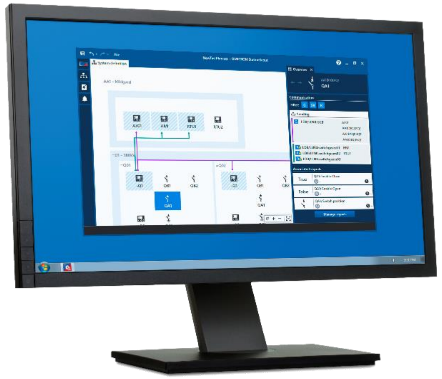
or

- Virtual machine (**VBX1**)

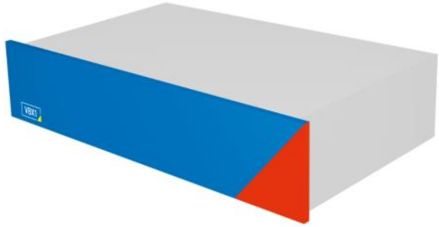
➢Does it support different operating systems?

- It’s supported on different types latest Windows OS.
- StationScout can be deployed on Windows and third-party virtual machine host platforms.

Software



StationScout



VBX1

Hardware

MBX1

RBX1

Main features

„Live Overview“

- Live status display
- “Zero-Line” view
- Communication view
- Watch selected signals

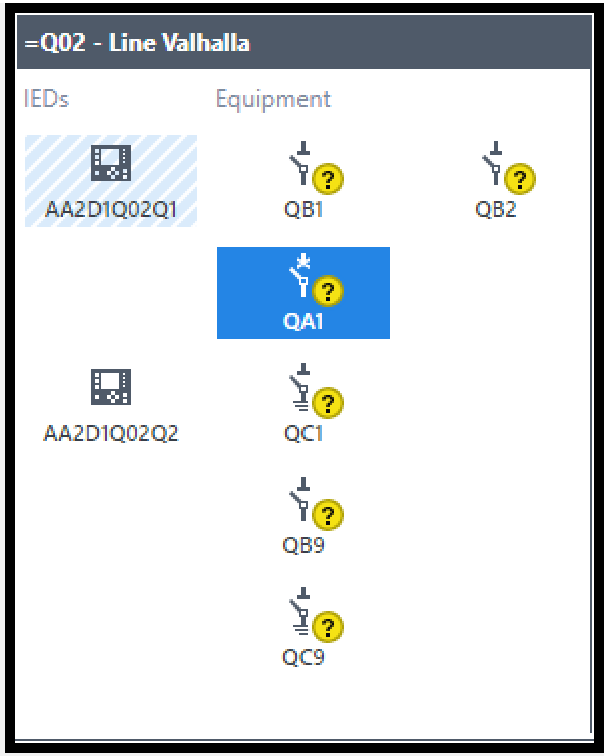
Simulation

- Simulate missing equipment
- Simulate (protection) events
- Stimulate signals for testing

Test cases (Commissioning features)

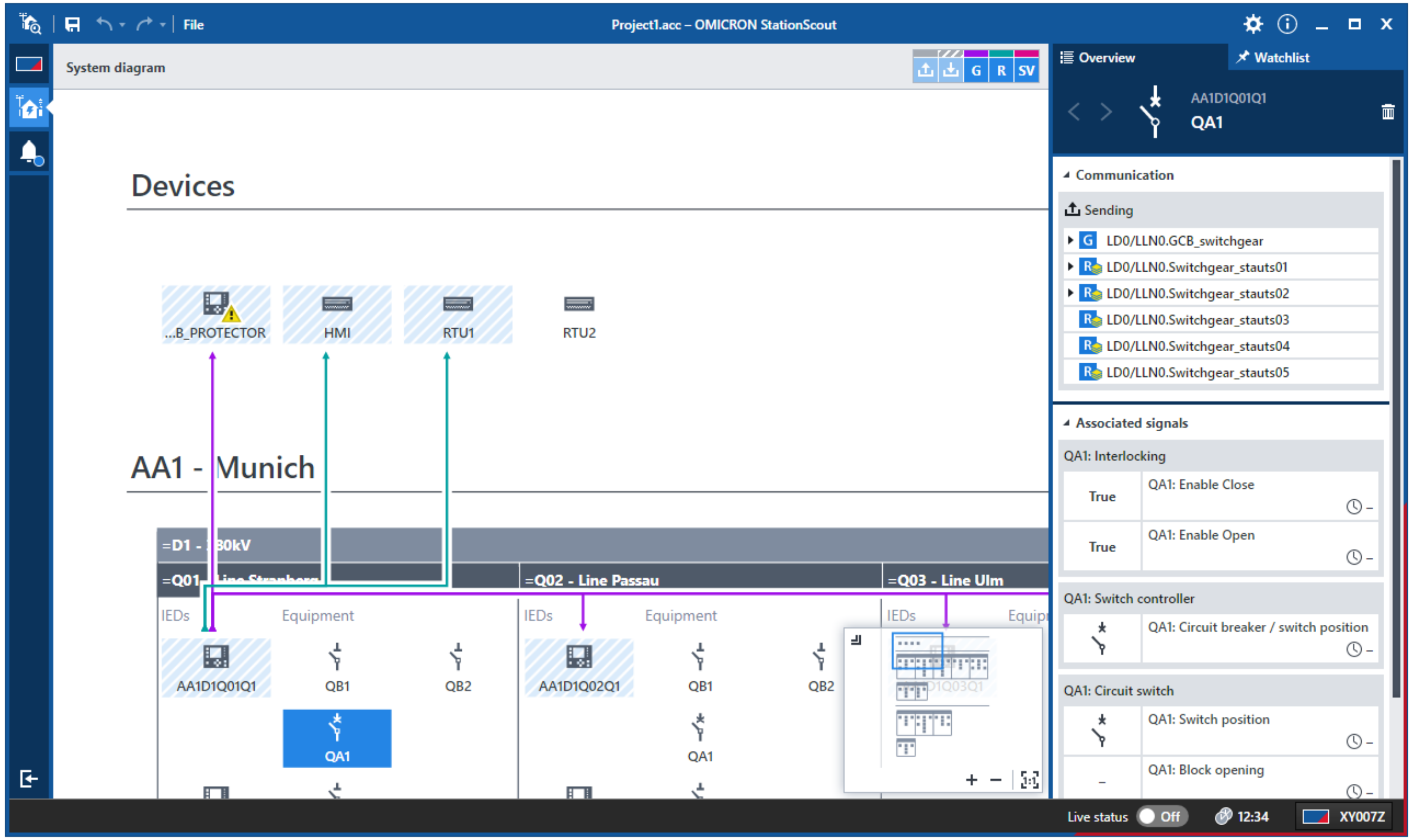
- Repeatable tests
- Flexible for changes in SCD
- Printable test reports

✓



Live overview – “ZeroLine”

- OMICRON introduces the “ZeroLine View”, because single line information is often not available in IEC 61850 engineering files (SCD)
- IEDs are grouped into bays and primary assets like switchgear



Communication

Sending

- LD0/LLN0.GCB_switchgear
- LD0/LLN0.Switchgear_stauts01
- LD0/LLN0.Switchgear_stauts02
- LD0/LLN0.Switchgear_stauts03
- LD0/LLN0.Switchgear_stauts04
- LD0/LLN0.Switchgear_stauts05

Associated signals

QA1: Interlocking

True	QA1: Enable Close –
True	QA1: Enable Open –

QA1: Switch controller

QA1: Circuit breaker / switch position –

QA1: Circuit switch

	QA1: Switch position –
–	QA1: Block opening –

Live status Off 12:34 XY007Z

OMICRON Academy

StationGuard

- Functional Security Monitoring for the Power Grid

CyberSecurity

What does CyberSecurity mean ?

Who is responsible for security in your organization ?

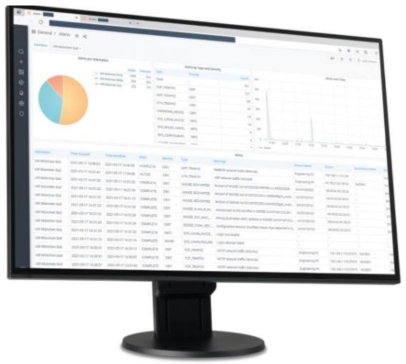
What is possible vectors ?

What can you do to prevent attacks ?

The StationGuard Solution

StationGuard

Cybersecurity and Functional Monitoring for the Power Grid



GridOps

Central Management System for StationGuard

RBX1

Robust and cybersecure 19-inch platform

MBX1

Mobile, hardened test set for powerful communication analysis

VBX1

Virtualized platform for cybersecurity and testing applications

How StationGuard is securing the 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

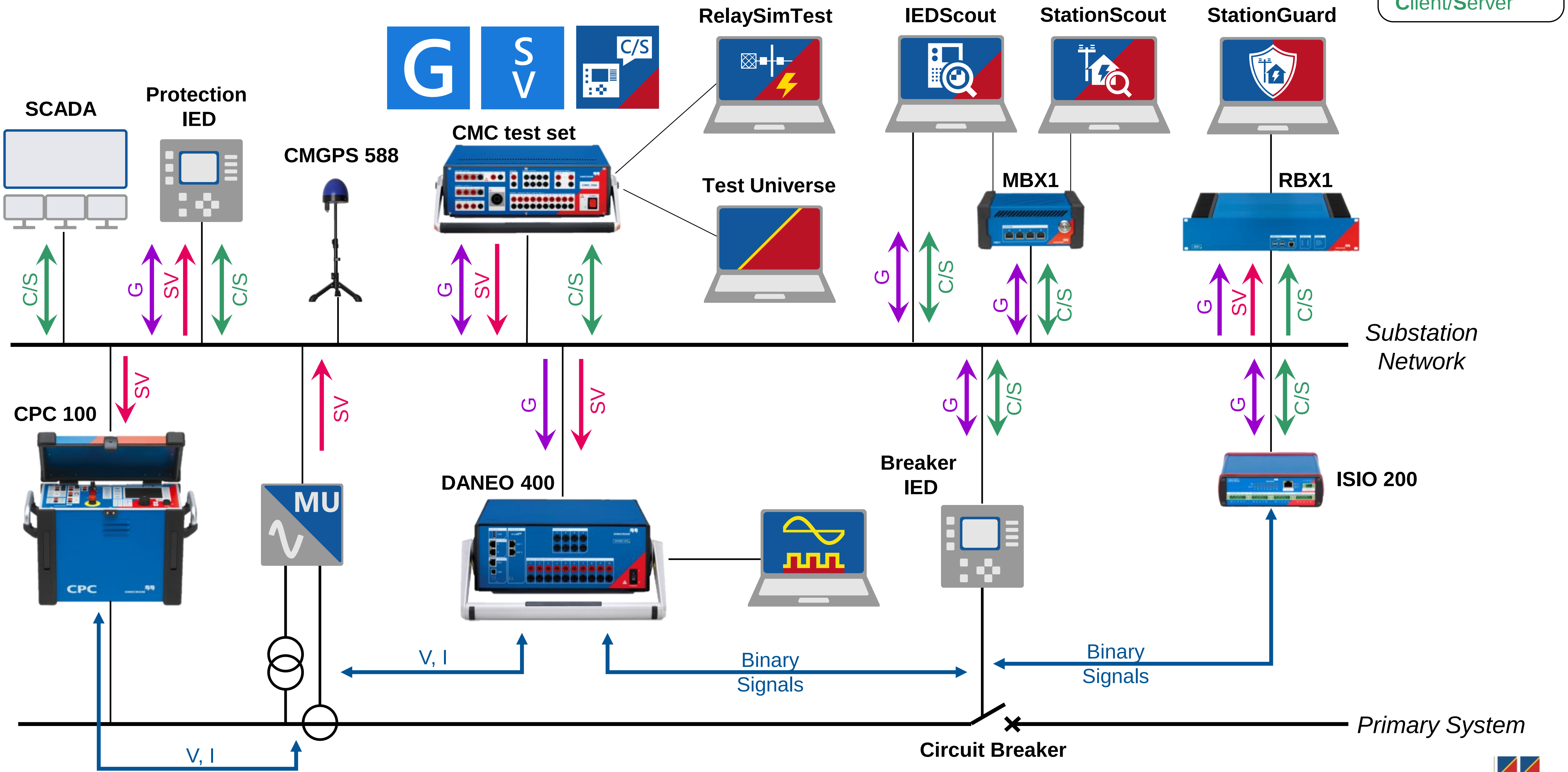
- Built-in ICS knowledge enables fewer false alarms, easier analysis, and faster response

Functional monitoring

- Detect malfunctions and configuration errors

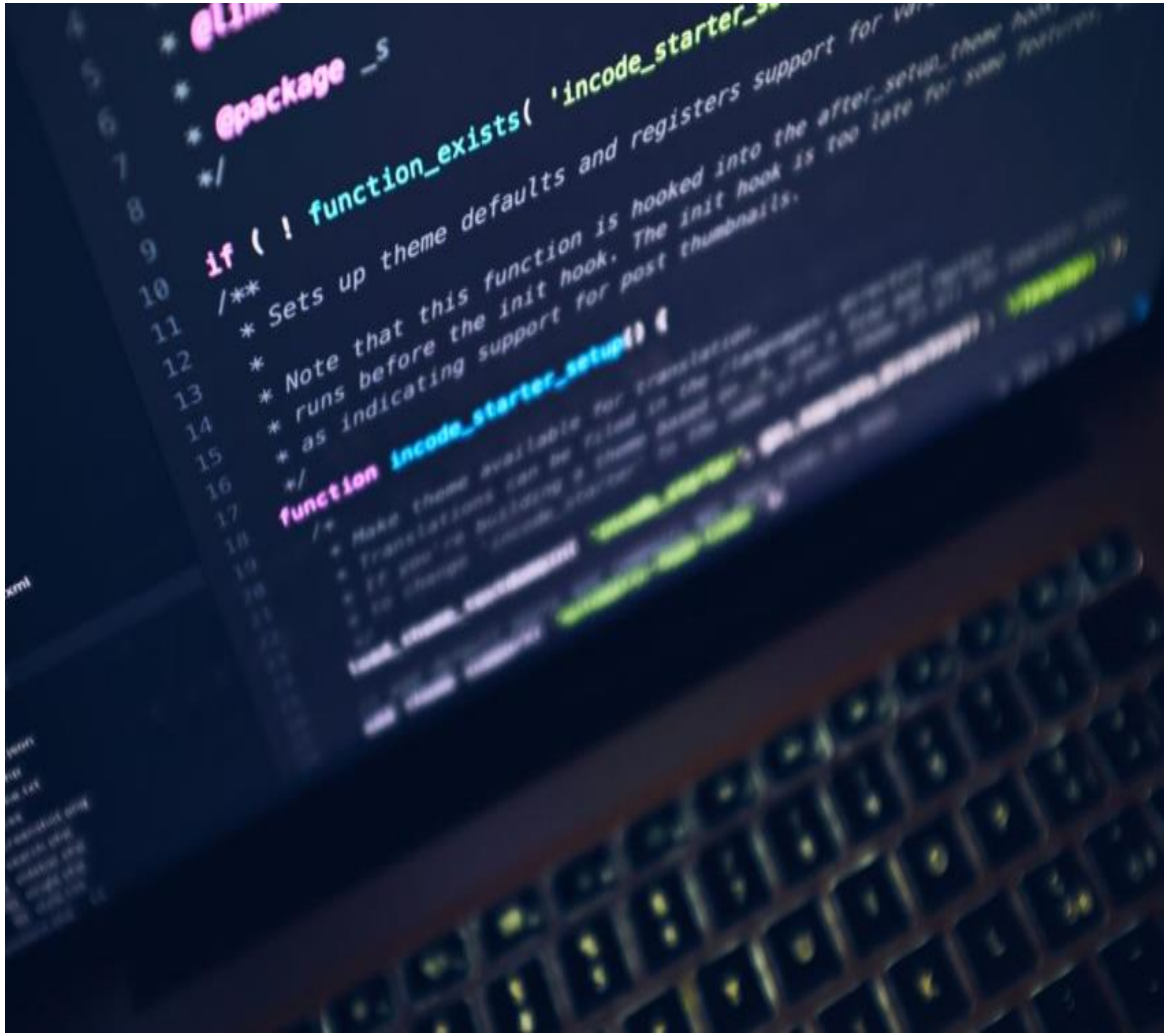
OMICRON's IEC 61850 testing solutions

GOOSE
Sampled **V**alues
Client/**S**erver



Preventing Cyber attacks on your network

- Don’t use your configuration pc – for personal use on the internet.
- Don’t click on any link’s
- Verify suspicious emails – check the sender email address.
- Call the sender to verify if something looks off
- Keep all software up to date
- Regularly change passwords
- Wifi devices on the network



Questions ?