RuggedCom News: Products & Functions

Werner Jud, RuggedCom Sales CEE

VAR Partner Day 2022 | September 12 -14 | Zagreb, Croatia

SIEMENS

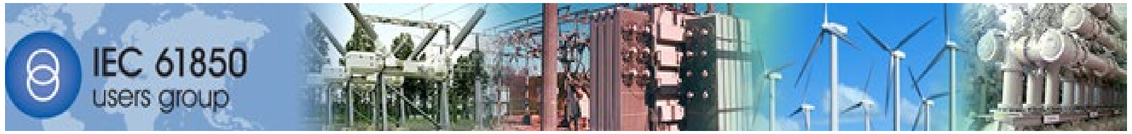
Agenda

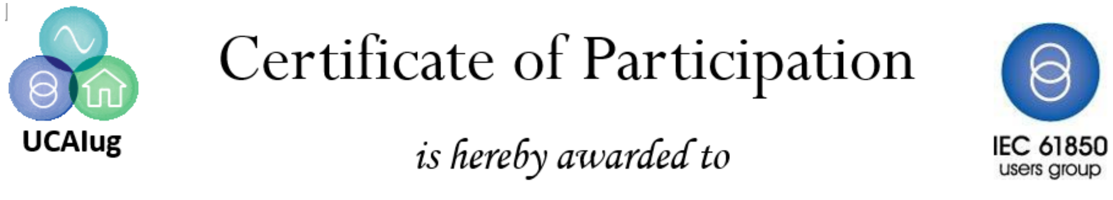
- Review UCAIop 2022 Event at CESI in Milan, regarding IEC 61850 Interoperability testing
- SCEP implementation
- Crossbow feature update
- ACLs (Layer 2 & 3)
- Multiple VLAN support
- Remote traffic mirroring (RSPAN)
- Extended warranty

Review UCAIug IOP 2022 Event at CESi in Milan, IEC 61850 Interoperability testing

SIEMENS

IEC 61850 Users Group & IEC 61850 Interoperability Testing Event




UCAIug

Certificate of Participation

is hereby awarded to

IEC 61850
users group

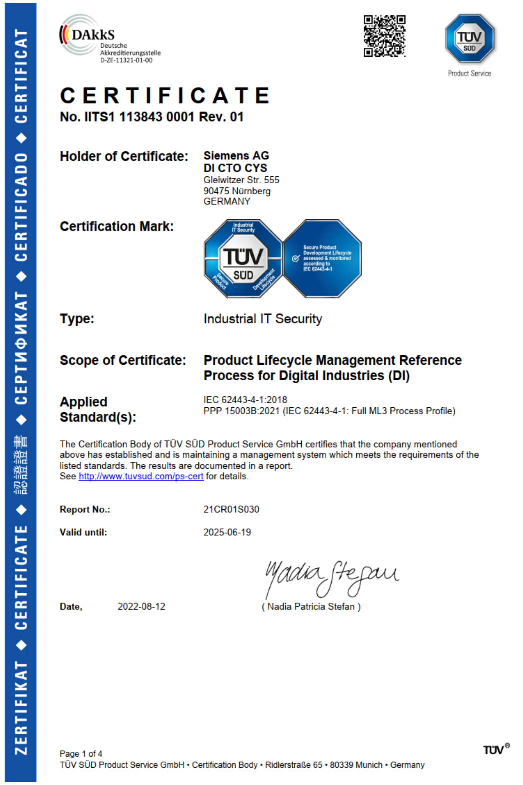
The IEC 61850 Interoperability Test Events consisting of utility users, supplier companies, certification bodies and witnesses dedicated to promoting integration and interoperability of electric/gas/water utility systems through the use of international standards-based technology
https://iec61850.ucaiug.org/2021-22_IOP/default.aspx

- UCA IOP testing events revolving event
- This year Face-to-Face July 14-22, 2022
- Hosted by CESi: Milan, Italy
- Testing of Tools, PTP over PRP, Client/Server, GOOSE/R-GOOSE, SV/R-SV, and Security

Siemens actively participated in every UCA Interoperability event since 2011 and has played a key role in defining network topologies, network test cases and providing network infrastructure. experts in standardization bodies and active contribution to IEC 62439 and IEC 61850 working groups, have helped develop and improve networking standards over the years

Highlight: Tests of the latest extensions of the IEC62439-3:2021 (Ed. 4. 5.2.2.10, 12/2021) using Siemens RUGGEDCOM RST2228 switch with the RNA module, covering PRP-HSR- RSTP coupling where we could prove our Siemens unique performance.

Technical Inspection Association Certifications leveraging Interoperability



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-11321-01-00

TÜV SÜD
Product Service

CERTIFICATE
No. IITS1 113843 0001 Rev. 01

Holder of Certificate: **Siemens AG**
DI CTO CYS
Gleiwitzer Str. 555
90475 Nürnberg
GERMANY

Certification Mark:

Industrial IT Security
TÜV SÜD
Secure Product Development Lifecycle
Secure Product Development Lifecycle assessed & monitored according to IEC 62443-4-1

Type: Industrial IT Security

Scope of Certificate: **Product Lifecycle Management Reference Process for Digital Industries (DI)**

Applied Standard(s): IEC 62443-4-1:2018
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See http://www.tuvsud.com/ps-cert for details.

Report No.: 21CR01S030

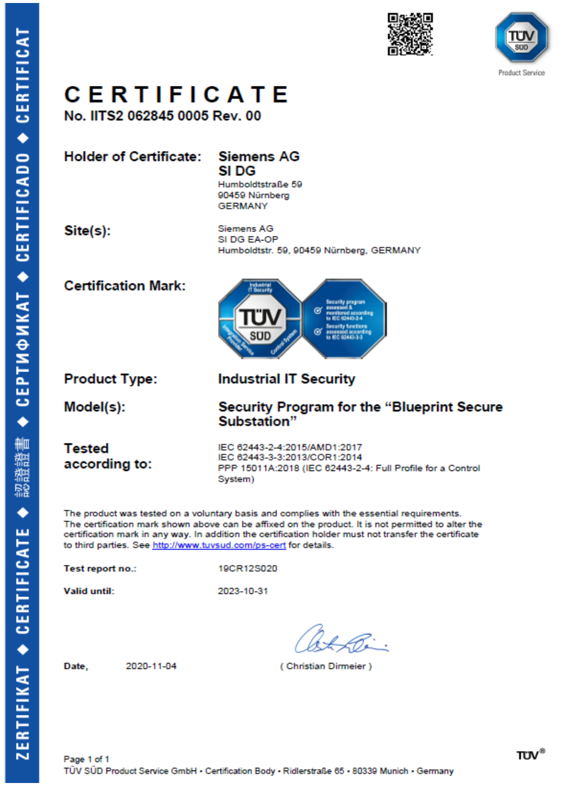
Valid until: 2025-06-19

Date, 2022-08-12

Nadia Stefan
(Nadia Patricia Stefan)

Page 1 of 4
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®



ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD
Product Service

CERTIFICATE
No. IITS2 062845 0005 Rev. 00

Holder of Certificate: **Siemens AG**
SI DG
Humboldtstraße 59
90459 Nürnberg
GERMANY

Site(s): Siemens AG
SI DG EA-OP
Humboldtstr. 59, 90459 Nürnberg, GERMANY

Certification Mark:

Industrial IT Security
TÜV SÜD
Integration Service Provider
Control System
Security program assessed & monitored according to IEC 62443-2-4
Security functions assessed according to IEC 62443-3-3

Product Type: **Industrial IT Security**

Model(s): **Security Program for the “Blueprint Secure Substation”**

Tested according to: IEC 62443-2-4:2015/AMD1:2017
IEC 62443-3-3:2013/COR1:2014
PPP 15011A:2018 (IEC 62443-2-4: Full Profile for a Control System)

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 19CR12S020

Valid until: 2023-10-31

Date, 2020-11-04

(Christian Dirmeier)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

-Secure Product Development LifeCycle from Siemens certified according to IEC 62443-4-1

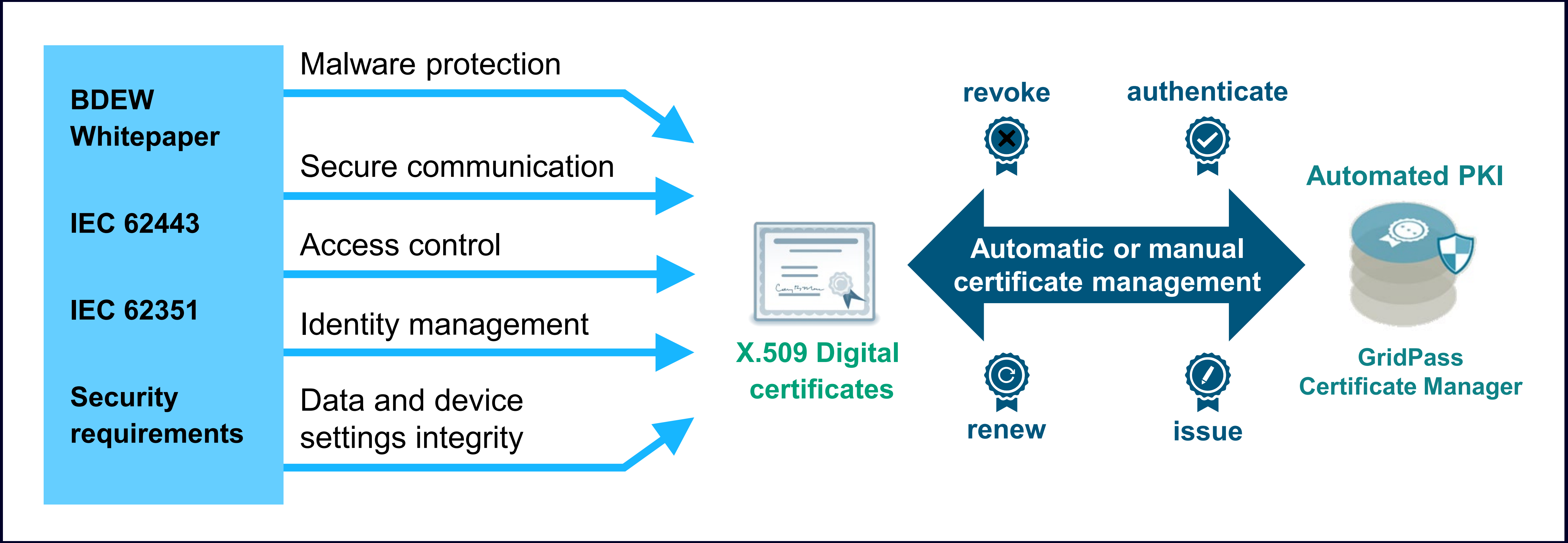
-Secure substation framework from Siemens certified along

IEC 62443-2-4 (requirements for system integrators)

IEC 62443-3-3 (requirements for the security functions of systems)

SCEP implementation

PKI and usage of Digital Certificates in Electrical Grids



Automatic certificate enrollment protocols: SCEP, EST, CMP, …

Acronyms:

PKI	Public Key Infrastructure
SCEP	Simple Certificate Enrollment Protocol
EST	Enrollment over Secure Transport protocol
CMP	Certificate Management Protocol

CrossBow Serial Feature

RUGGEDCOM CROSSBOW support for SIPROTEC 4 Serial devices

Current Situation and Challenges

- CROSSBOW allows an Intelligent Electronic Device (IED) maintenance application to remotely communicate with its associated IEDs as if the users were directly connected to the device.
- Large installed base of SIPROTEC 4 and SIPROTEC Compact devices - several hundred thousand devices installed worldwide over the last 20 years
- Electrical utilities identify cybersecurity as one of their top priorities
- User Authentication and Role Based Access Control (RBAC) are becoming mandatory requirements

Key Benefits

- CROSSBOW supports utilities and industrial customers with large installed base of legacy SIPROTEC 4 devices
- Increased productivity by automation of device management via CROSSBOW
- CROSSBOW provides additional layer of cybersecurity allowing to check DIGSI 4 user authenticity for remote access control

RUGGEDCOM CROSSBOW
SIPROTEC device support overview

SIPROTEC 4 Serial

- DIGSI connection via CROSSBOW RBAC
- Configuration management
- FW version management
- Data Retrieval (COMTRADE)

*USB interface is not supported

SIPROTEC 4 (Ethernet based)

- DIGSI connection via CROSSBOW RBAC
- Configuration management
- FW version management
- Data Retrieval (COMTRADE and SOE)

SIPROTEC 5

- DIGSI connection via CROSSBOW RBAC
- Configuration management
- FW version management
- Data Retrieval (COMTRADE and SOE)
- Change password

*Advanced security functionality (customer PKI) is not supported

- Configuration Management
  - CROSSBOW connects to SIPROTEC devices, reads config, and compares to known baseline
  - Alerts are raised when inconsistency detected. Alerts can be exported to external tracking systems (e.g. Syslog) via ELDS service
- Firmware Version Management
  - CROSSBOW connects to SIPROTEC devices, reads FW version, compares to known baseline
  - Alerts are raised when inconsistency detected. Alerts can be exported to external tracking systems (e.g. Syslog) via ELDS service
- Data Retrieval
  - CROSSBOW connects to SIPROTEC devices, retrieves oscillography files and/or SOEs files. Files can be exported to external FTP server via File Export Service

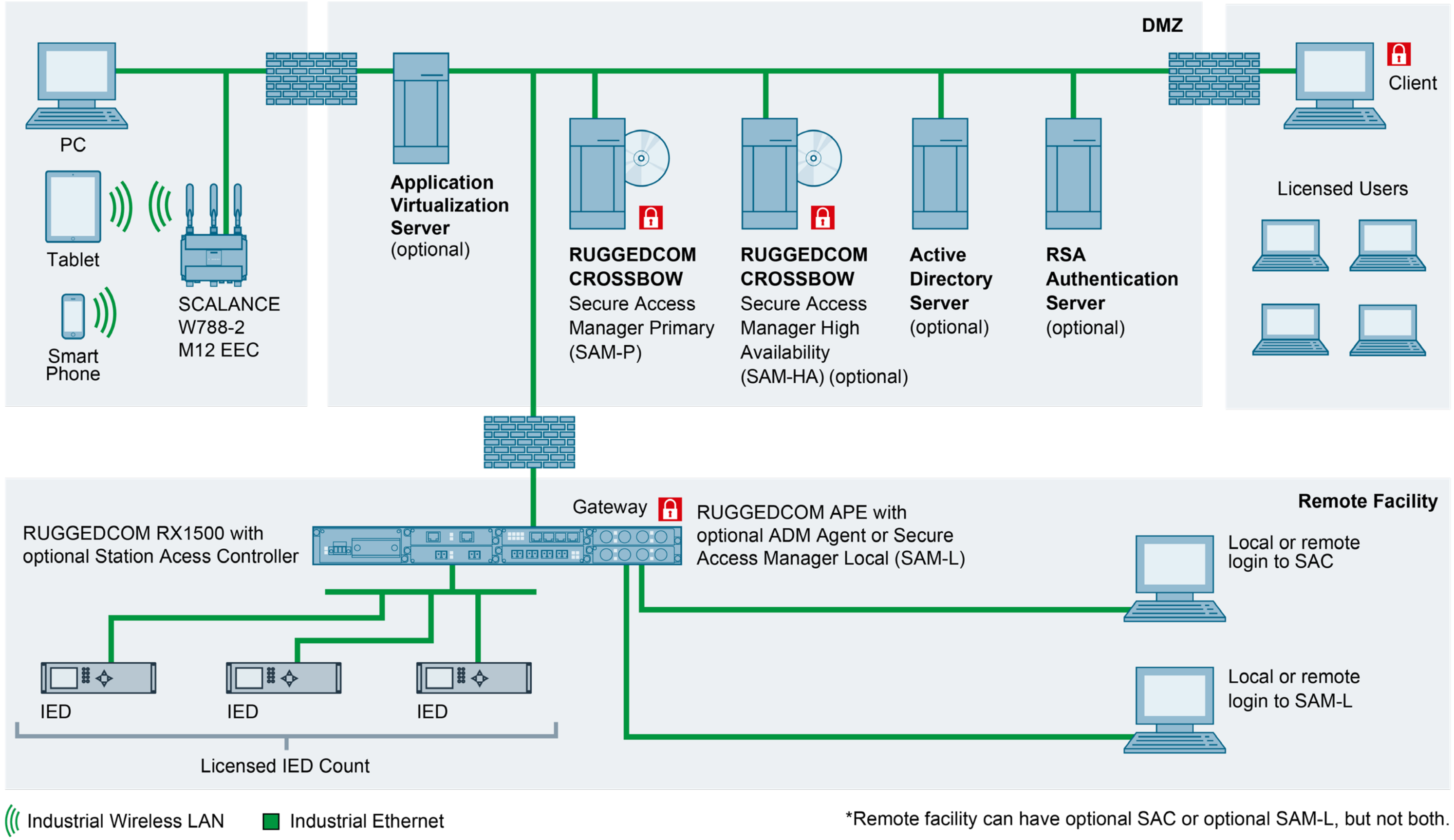
RUGGEDCOM CROSSBOW
Use case. Providing secure remote access and automation functions

Centralized Remote Access

- Simplex or Redundant server
- Two-factor Authentication
- Secure TLS connection to server from client
- Optional installation of client on virtual application server for centralized virtual client

Remote Location(s)

- Access to SIP4 serial devices on the service/ operator port using DIGSI4 native protocol



DMZ
PC
Tablet
Smart Phone
SCALANCE W788-2 M12 EEC
Application Virtualization Server (optional)
RUGGEDCOM CROSSBOW Secure Access Manager Primary (SAM-P)
RUGGEDCOM CROSSBOW Secure Access Manager High Availability (SAM-HA) (optional)
Active Directory Server (optional)
RSA Authentication Server (optional)
Client
Licensed Users
Gateway
RUGGEDCOM RX1500 with optional Station Acess Controller
RUGGEDCOM APE with optional ADM Agent or Secure Access Manager Local (SAM-L)
Remote Facility
Local or remote login to SAC
Local or remote login to SAM-L
IED
IED
IED
Licensed IED Count
Industrial Wireless LAN
🟩 Industrial Ethernet

*Remote facility can have optional SAC or optional SAM-L, but not both.

*Local connection from DIGSI 4 is still possible via DIGSI cable directly plugged into the device

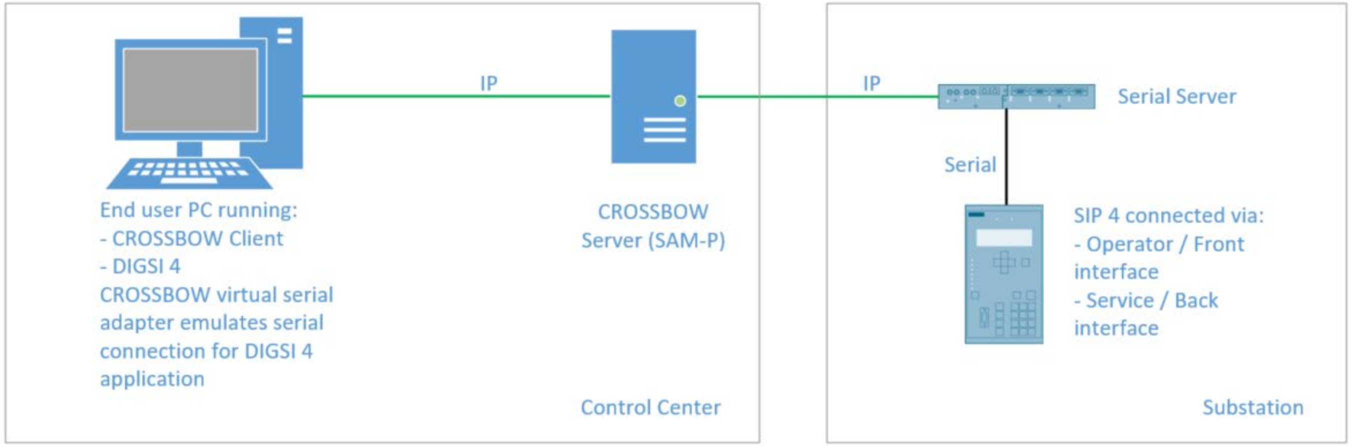
RUGGEDCOM CROSSBOW
Introducing additional layer of security

Current DIGSI4 connection mechanism:

- There is no mechanism in SIP4 / SIP4 Compact to check the authenticity of the connecting user
- DIGSI 4 does not natively support multiple users or RBAC
- Certain actions in DISGI 4, e.g. setting change, command or firmware upgrade command require 6 character numerical passcodes that are sent without encryption via IP or serial to IEDs

Key benefits of introducing CROSSBOW solution:

- Introduction of additional layer of security when connecting remotely to SIP4 Serial/ SIP4 Compact devices
- Automation of configuration, FW and Data management for SIP4 Serial devices
- User permission verification before executing DIGSI commands


IP
IP
Serial Server
Serial
End user PC running:
- CROSSBOW Client
- DIGSI 4
CROSSBOW virtual serial adapter emulates serial connection for DIGSI 4 application
CROSSBOW Server (SAM-P)
SIP 4 connected via:
- Operator / Front interface
- Service / Back interface
Control Center
Substation

Access Control Lists L2&L3

What is an Access Control List?

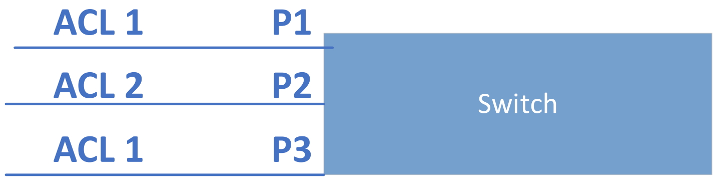
- An Access Control List (ACL) is an ordered list of rules to filter and control the traffic on a networking device.

- ACLs are configurable by MAC address control entry, IP address control entry and control packet access entry settings.

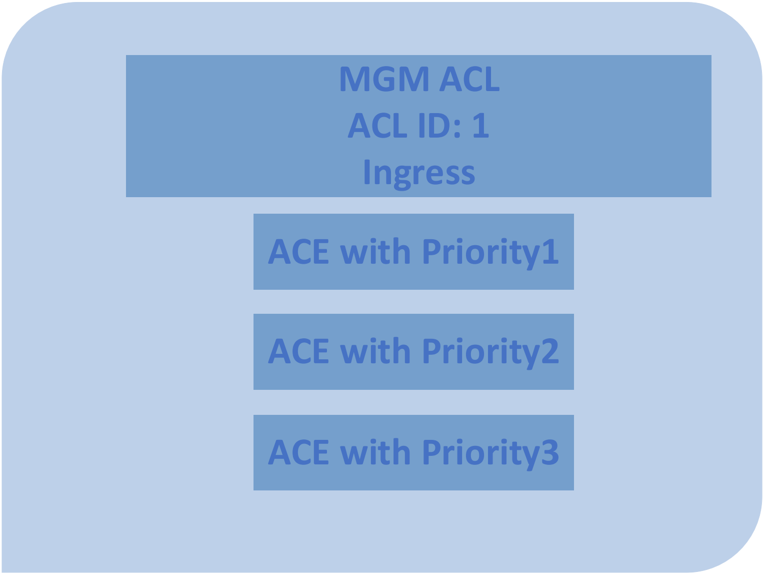
- Rules are defined by an Access Control Entries (ACE).
  Each ACE includes a match criterion and actions. The match criteria can apply to packet headers.

- An action (deny/permit) specifies what to do with the packet when the matching criteria is met.

- Actions are applied to the first matching ACE with no processing of subsequent ACEs.



ACL 1 P1
ACL 2 P2
ACL 1 P3
Switch



MGM ACL
ACL ID: 1
Ingress

ACE with Priority1

ACE with Priority2

ACE with Priority3

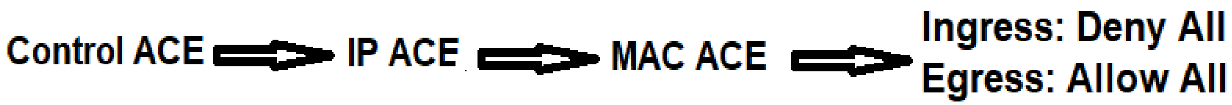
Introducing Network Access Control List (ACL) in ROS 5.6.0

- Access control list (ACL) are introduced with ROS 5.6.0

- A new menu item named ‘Access Control List’ is added to ROS UI under “Network Access Control”

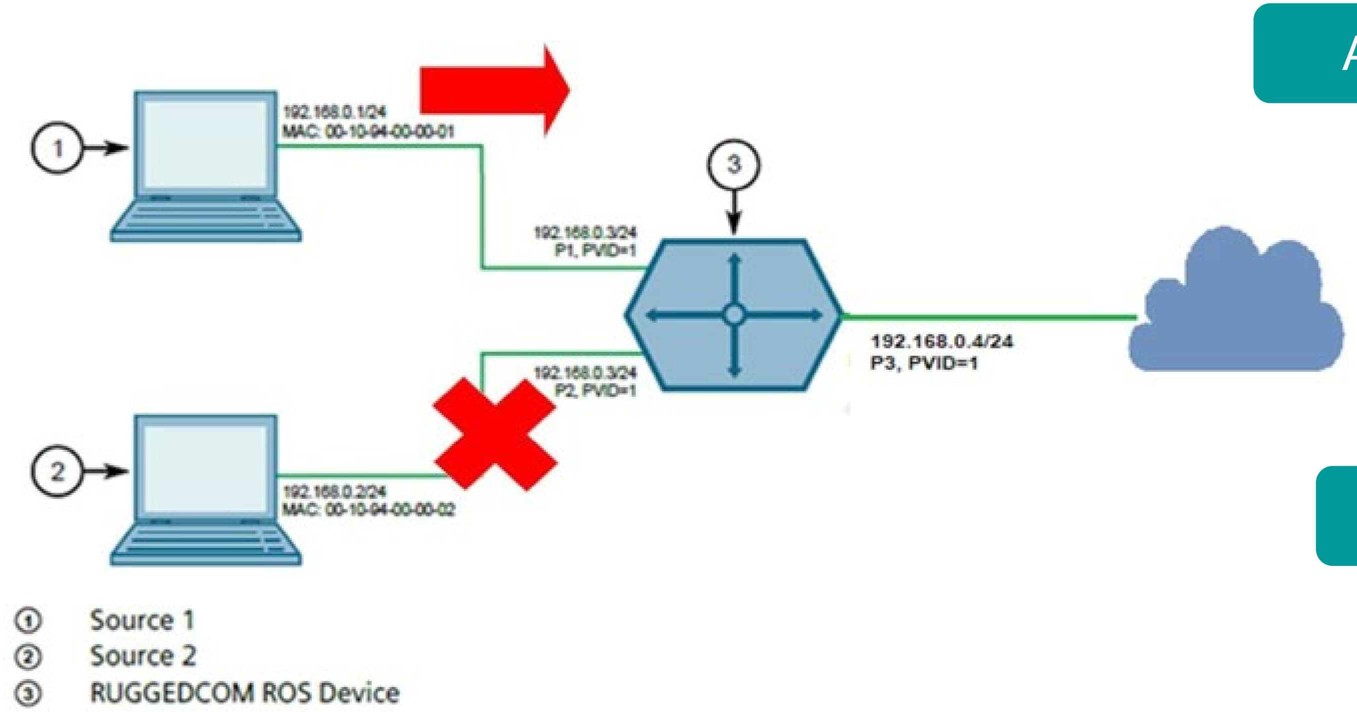
- The ACL is mostly designed for filtering data plane traffic but there are 11 control packets (management frames) that ROS will be able to filter as well.

- The ACL feature is only available for the ROS product RST2228. Some other devices will be covered in further releases.

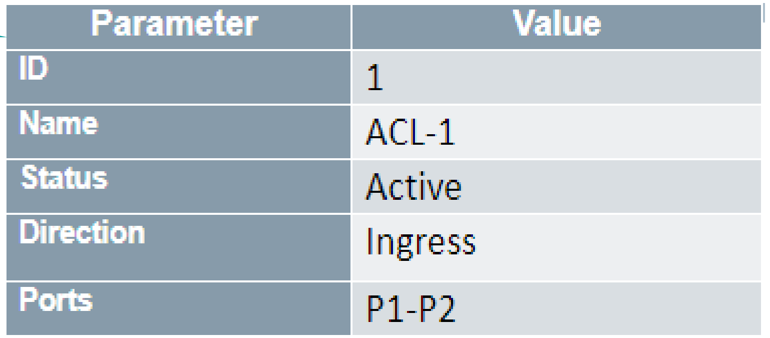


Control ACE → IP ACE → MAC ACE → Ingress: Deny All
Egress: Allow All

Scenario-1 (Multiple Ports)

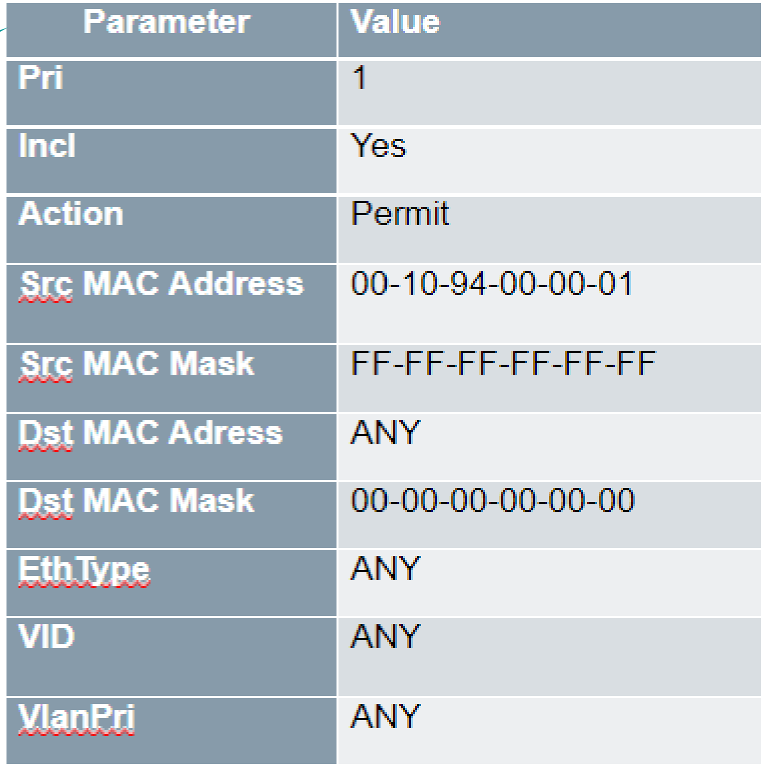


ACL



Parameter	Value
ID	1
Name	ACL-1
Status	Active
Direction	Ingress
Ports	P1-P2

ACE

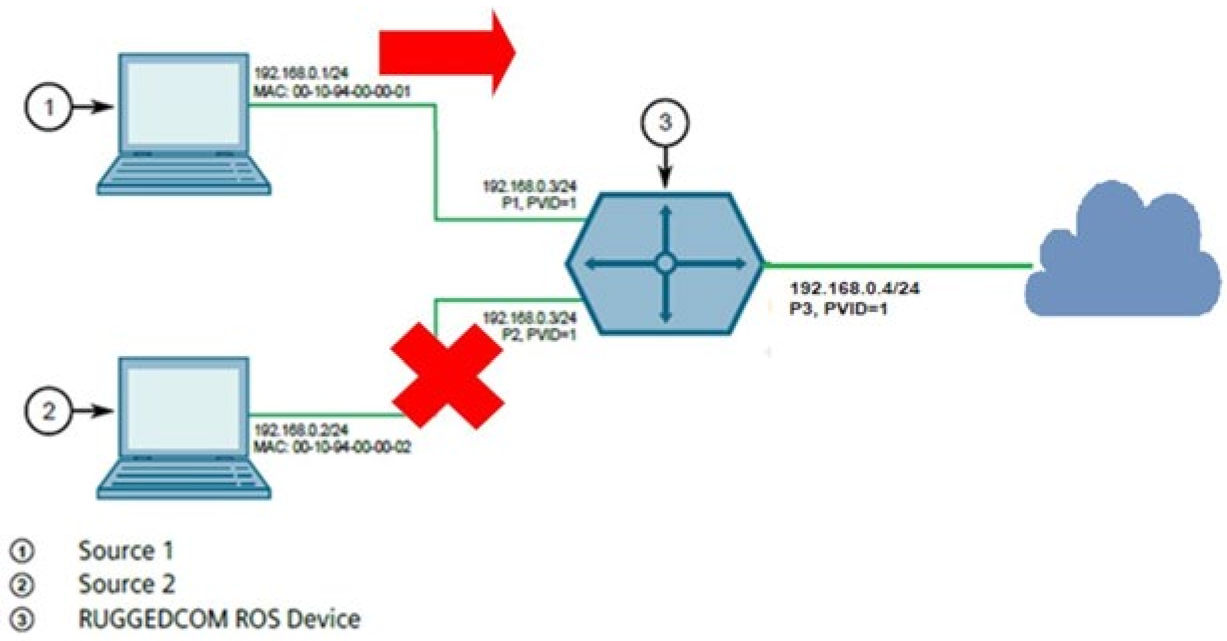


Parameter	Value
Pri	1
Incl	Yes
Action	Permit
Src MAC Address	00-10-94-00-00-01
Src MAC Mask	FF-FF-FF-FF-FF-FF
Dst MAC Adress	ANY
Dst MAC Mask	00-00-00-00-00-00
EthType	ANY
VID	ANY
VlanPri	ANY

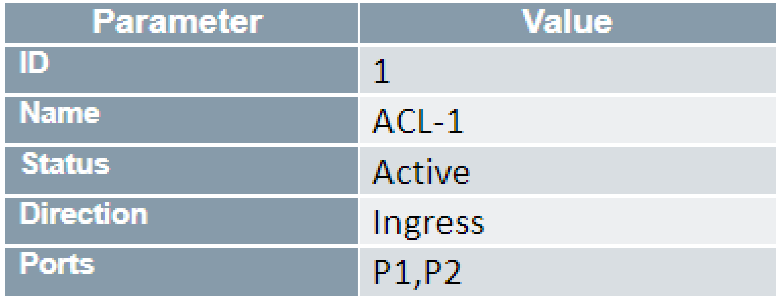
- A scenario where a ROS device (3) is configured to accept any traffic from Source 1 and block all other traffic.
- A MAC ACE is attached to an ACL of Ingress direction at ports P1 & P2.
- Implicit rule (Deny for ingress) will be applicable for traffic from Source 2.

SIEMENS

Scenario-2 (IP ACE)

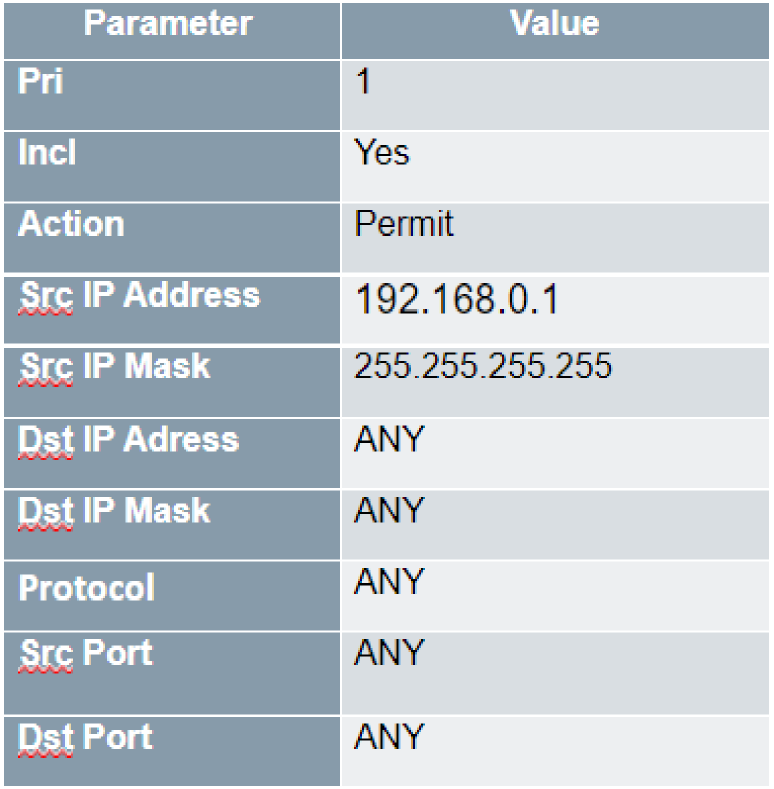


ACL



Parameter	Value
ID	1
Name	ACL-1
Status	Active
Direction	Ingress
Ports	P1,P2

ACE



Parameter	Value
Pri	1
Incl	Yes
Action	Permit
Src IP Address	192.168.0.1
Src IP Mask	255.255.255.255
Dst IP Adress	ANY
Dst IP Mask	ANY
Protocol	ANY
Src Port	ANY
Dst Port	ANY

- A scenario where a ROS device (3) is configured to accept traffic from Source 1 and block all other traffic.
- An IP ACE is attached with an ACL of ingress direction.
- Implicit rule (Deny for ingress) will be applicable for traffic from Source 2.

Limitations of ACL

- Currently ACL is only available for the ROS product RST2228. More devices will be covered in further releases.
- Control Packets can not be filtered in Egress direction.
- Max 116 MAC ACE and 128 IP ACE can be configured.
- Max 256 ACLs are provisioned to configure but also limited to maximum number of ports the device in each direction.

Remote Traffic Mirroring (aka RSPAN Protocol) MACsec

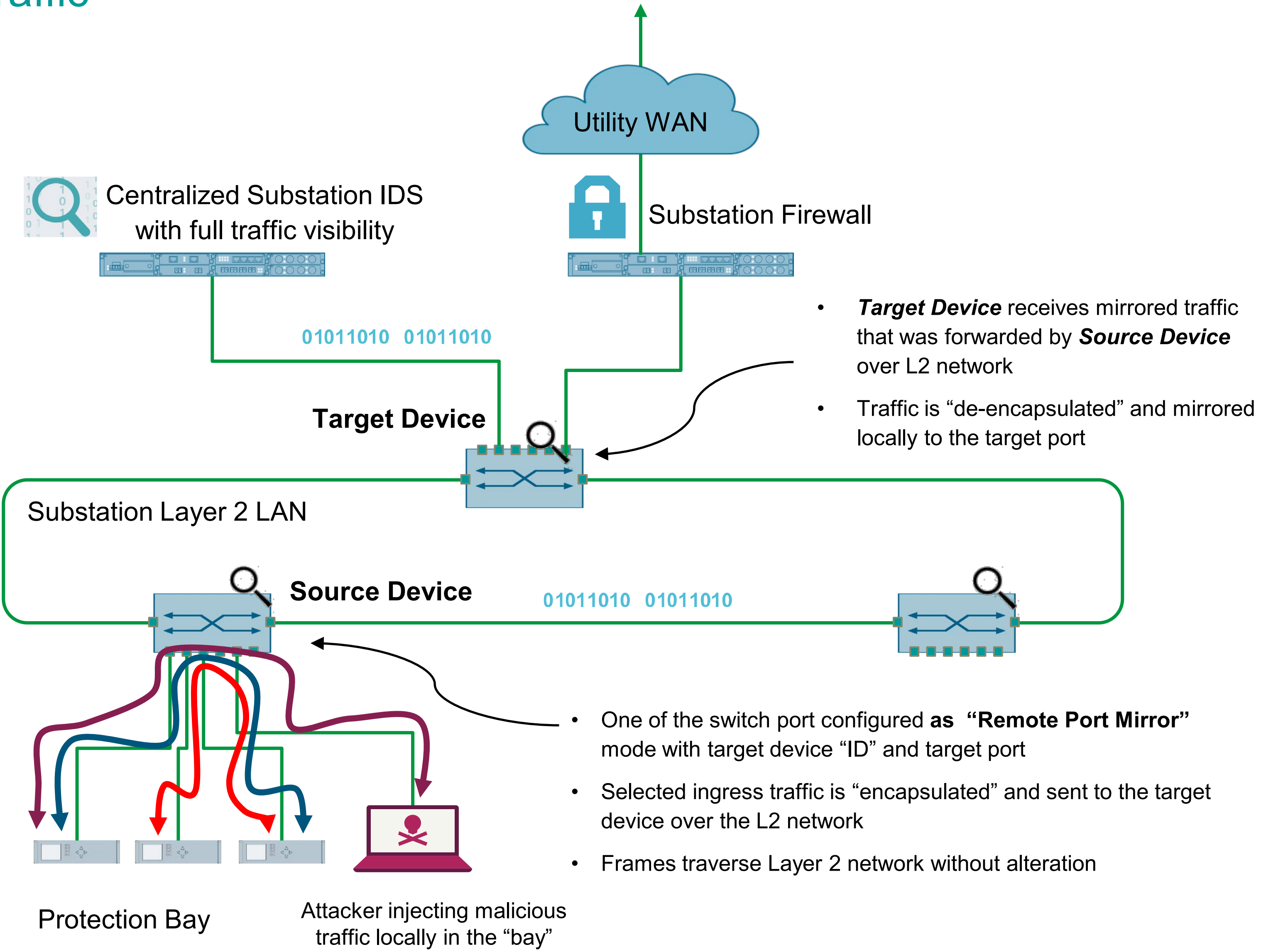
Remote Traffic Mirroring (aka RSPAN Protocol) -
Get the full visibility of substation traffic

Challenge

- Certain types of traffic (e.g. GOOSE or Sampled Values) are “local” to protection bays and not forwarded on “trunk ports”
- How to get full visibility of substation traffic and detect sophisticated cyber threats and attacks ?

Solution & Key Benefits

- Remote port mirroring “serving” all data flows to central IDS
- Cost saving – no need to install dedicated sensors in every “bay”. Ethernet switches act as sensors



- ***Target Device*** receives mirrored traffic that was forwarded by ***Source Device*** over L2 network
- Traffic is “de-encapsulated” and mirrored locally to the target port

- One of the switch port configured **as “Remote Port Mirror”** mode with target device “ID” and target port
- Selected ingress traffic is “encapsulated” and sent to the target device over the L2 network
- Frames traverse Layer 2 network without alteration

10 years extended warranty

10 Years Extended Warranty

- RUGGEDCOM products are designed with **long lifecycles** in mind to help protect return on investment
- **Piece of mind** to end users thanks to standard 5 years warranty
- Now we are glad to offer even **higher value**
- **Extended 10-years warranty** that can be added as an option to majority of RUGGEDCOM hardware products

WARRANTY
10 YEARS
WARRANTY

NOTE: Available for new devices only and for on configured products only, not loose modules or accessories such as SFPs

Disclaimer

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Contact

Reinhard Besemer
Field Application Consultant
DI PA DCP SUP PSS 3
E-Mail: reinhard.besemer@siemens.com

Werner Jud
Regional Sales Manager Ruggedcom
RC-AT DI PA PR DCP
E-Mail: werner.jud@siemens.com

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations, product names, etc. may contain trademarks or other rights of Siemens AG, its affiliated companies or third parties.
Their unauthorized use may infringe the rights of the respective owner.