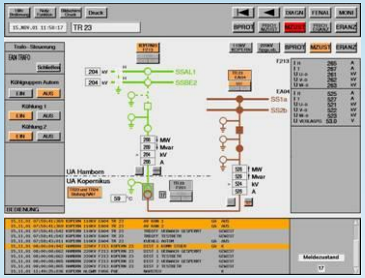


IEC 61850 Global 2018 Conference Berlin

Ensuring cyber security in the implementation of feature rich multi-vendor IEC 61850 that includes GOOSE

Part 1 - Global Considerations

Peter Rümenapp

Agenda

1 OE - BDEW-Whitepaper History

2 ISMS at Amprion

3 New tender for substation control technology

OE - BDEW White Paper History

Requirements for Secure Control and Telecommunication Systems

- OE-BDEW White Paper ed.1 - 2010
  - OE – BDEW Best Practice Paper
- OE-BDEW White Paper ed.1.1 - 03/2015
  - Adjusted references to ISO / IEC 27002: 2013 and ISO / IEC TR 27019: 2013
- OE – BDEW White Paper ed. 2 – 05/2018
  - Includes the OE – BDEW Best Practice Paper

Amprion is launching its ISMS in March 2010 voluntarily

One of the important topics:

All new secondary technologies must be tested with regard of IT security based on oe-bdew Whitepaper

- Amprion has published an internal policy with the title "Implementing new Technologies“
  - **all new technologies, which will be installed in our substations, must be tested with regard of IT security based on oe-bdew Whitepaper**
  - **the oe-bdew Whitepaper must be taken into account in all tenders**

Amprion published a new tender for substation control technology based on IEC 61850 in 2014

Interoperability and Interchangeability are very important

- Amprion has published its own data model
- IED's from different suppliers can be interchanged without adapting the data model

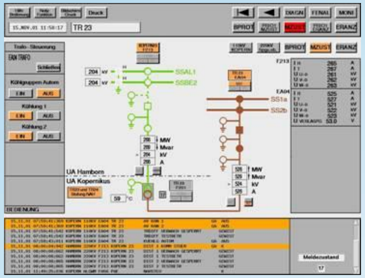
IT-Security is also important for interchangeability

- The IEC 62351 series of standards is not yet fully implemented in the IEDs of different suppliers e.g.
  - Part 8 role-based access control (RBAC)
  - Part 9 cyber security key management especially the autoenrollment via SCEP (IETF-Draft) or EST (RFC7030)

Amprion published a new tender for substation control technology based on IEC 61850 in 2014

Chapter IT-Security

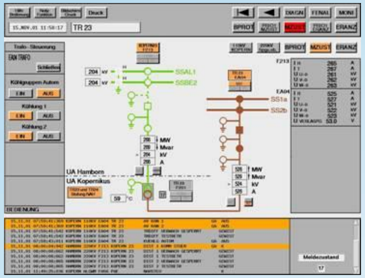
- Audits in the context of the award procedure
- Basic security requirements
- Security requirements for network and components
  - e.g. Separation of productive LAN and diagnostic LAN
  - Each IED requires two independent LAN ports
- Safety requirements for station HMI
- Safety requirements for the field displays
- Safety requirements for the control center interface
- Requirements for processes and security at the provider



The strong power network | www.amprion.net

amprion

5001


Druck
DIAGN
FENAL
MONI
15.NOV.01 11:58:17
TR 23
BPROT
MZUST
ERANZ
Trafo- Steuerung
Schließen
Kühlgruppen Autom
EIN
AUS
Kühlung 1
Kühlung 2
204 kV
SSAL1
SSBE2
F213
EA04
SS1a
SS2b
MW
Mvar
kV
A
UA Hamborn
UA Kopernikus
59 °C
BEDIENUNG
Meldezustand
17

F1 TRDIFF
F2 UMZ OSPG
F3 DIST MISPG

Backup

History RWE TSO Strom GmbH (1)

Examination of the existing substation control system with regard to IT-security in 2005

Results

- HMI (Human-machine interface) at all substations easily compromised
  - No patches were installed after first commissioning
  - (saying: never change a running system)
- Availability of industrial components can be limited
- Internal function of the systems can be permanently disturbed
- no firewall protection between the substations

History RWE TSO Strom GmbH (2)

Examination of the existing substation control system with regard to IT-security in 2005

Security measures

- Encapsulation of SLT communication → Firewall, VPN-Technology
- Securing the central components →Patch- and Update-management, Antivirus
- Central application and data delivery → Protection and control technology data server
- Secure access to the terminal server → strong authentication, Citrix, RSA
- Ban of third party components → own service laptop are provided to suppliers within the substation