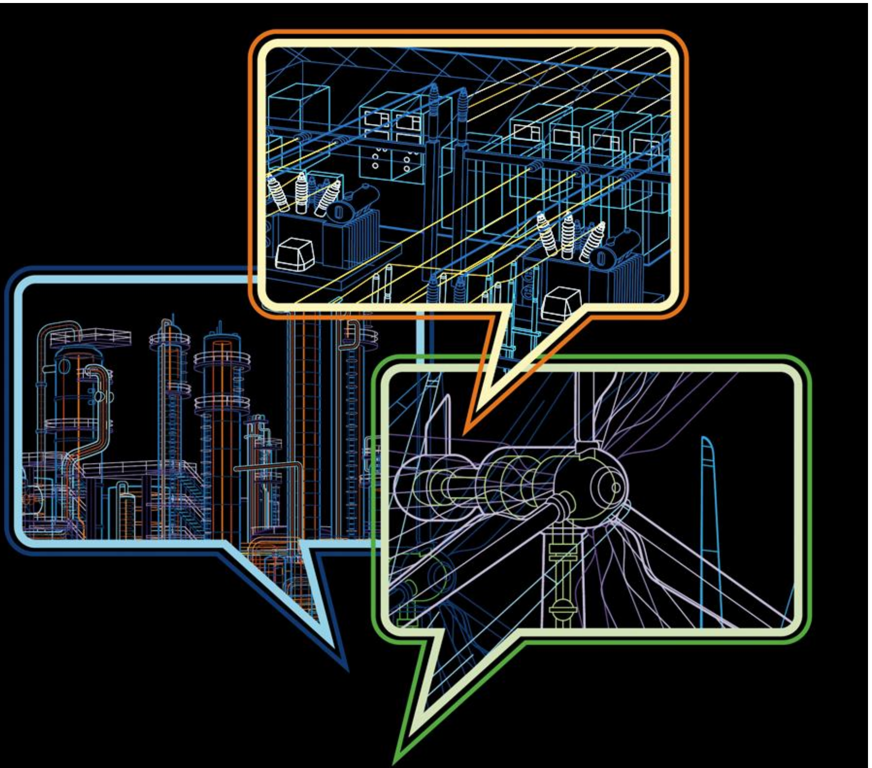


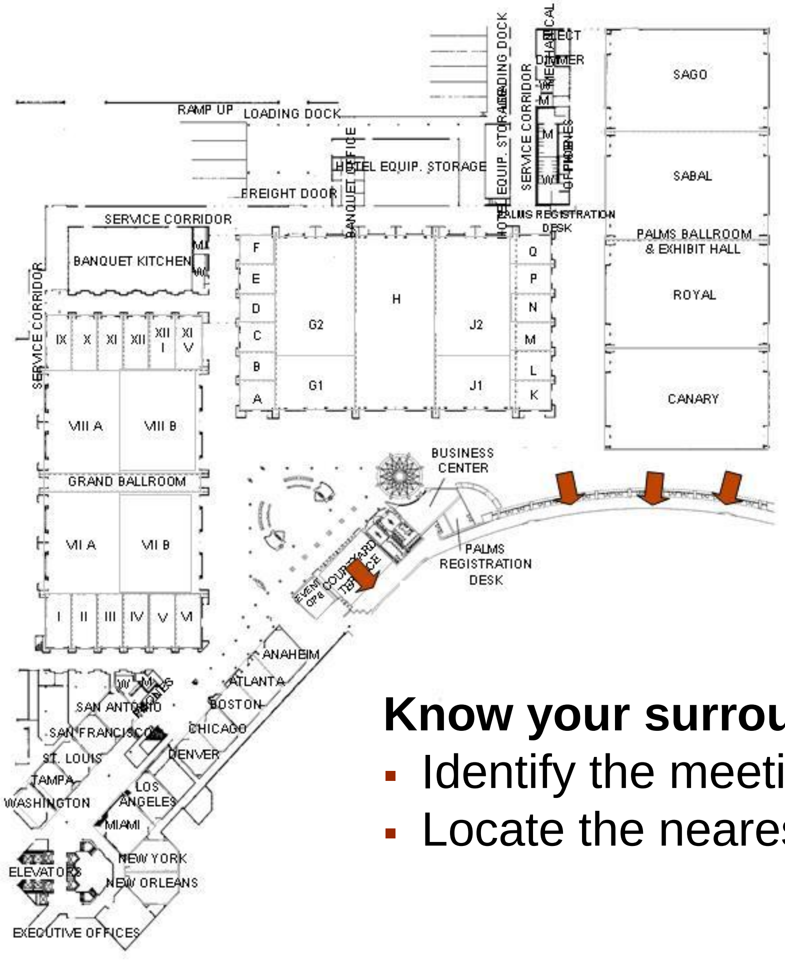
ABB Automation & Power World: April 18-21, 2011

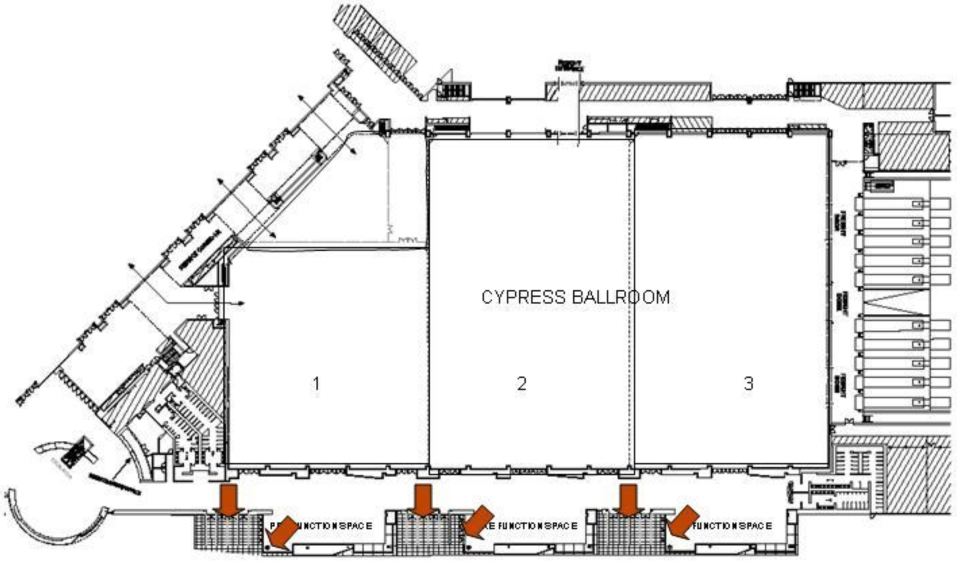
WPS-107-1
Cyber security in your Relion®-based protection and control solutions

Your safety is important to us
Please be aware of these emergency procedures

- In the event of an emergency please dial ext. 55555 from any house phone. Do not dial 9-1-1.
- In the event of an alarm, please proceed carefully to the nearest exit. Emergency exits are clearly marked throughout the hotel and convention center.
- Use the stairwells to evacuate the building and do not attempt to use the elevators.
- Hotel associates will be located throughout the public space to assist in directing guests toward the closest exit.
- Any guest requiring assistance during an evacuation should dial “0” from any house phone and notify the operator of their location.
- Do not re-enter the building until advised by hotel personnel or an “all clear” announcement is made.

Your safety is important to us
Convention Center exits in case of an emergency





Know your surroundings:

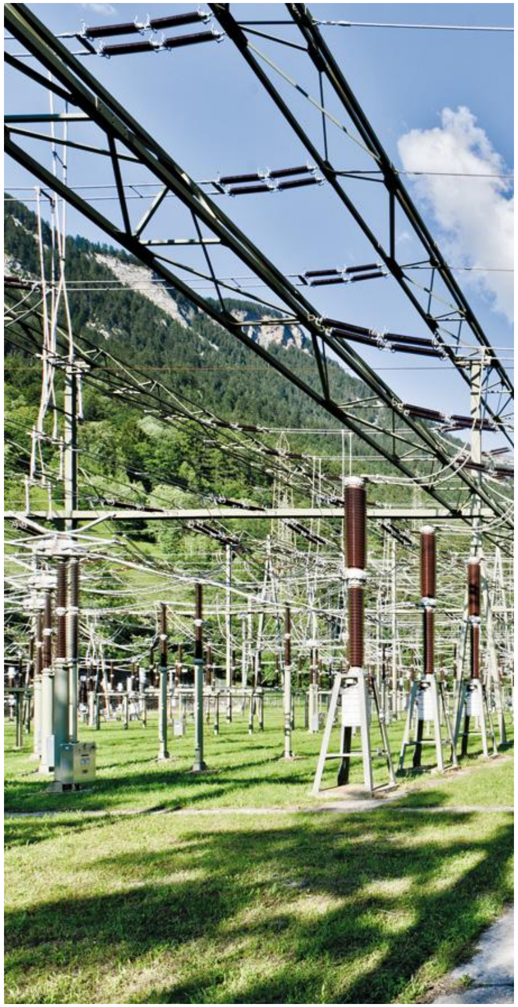
- Identify the meeting room your workshop is being held in
- Locate the nearest exit

WPS-107-1
Cyber security in your Relion®-based protection and control solutions

Speaker name:	Markus Braendle
Speaker title:	Group Head of Cyber Security
Company name:	ABB
Location:	Zurich, Switzerland

Speaker name:	Steven Kunsman
Speaker title:	VP and GM Substation Automation North America
Company name:	ABB Inc.
Location:	Raleigh

Cyber security in your Relion Solutions
Agenda



- Relion® protection and control
- IEC61850 Based Substation Automation Systems
- Cyber Security for Substation Automation Systems
- ABB approach
- Conclusions

Relion® product family
Complete confidence

The Relion® product family offers widest range of products for protection, control, measurement and supervision for power systems supporting both ANSI and IEC applications

To ensure interoperable and future-proof solutions, Relion products have been designed to implement the core values of the IEC 61850 standard.

With ABB’s leading-edge technology, global application knowledge and experienced support network, you can be completely confident that your system performs reliably - in any situation.

Relion® Family - generation to interconnected transmission grids to secondary distribution networks

- **670 series**
  Flexibility, performance and customizable for generation, transmission and sub-transmission applications

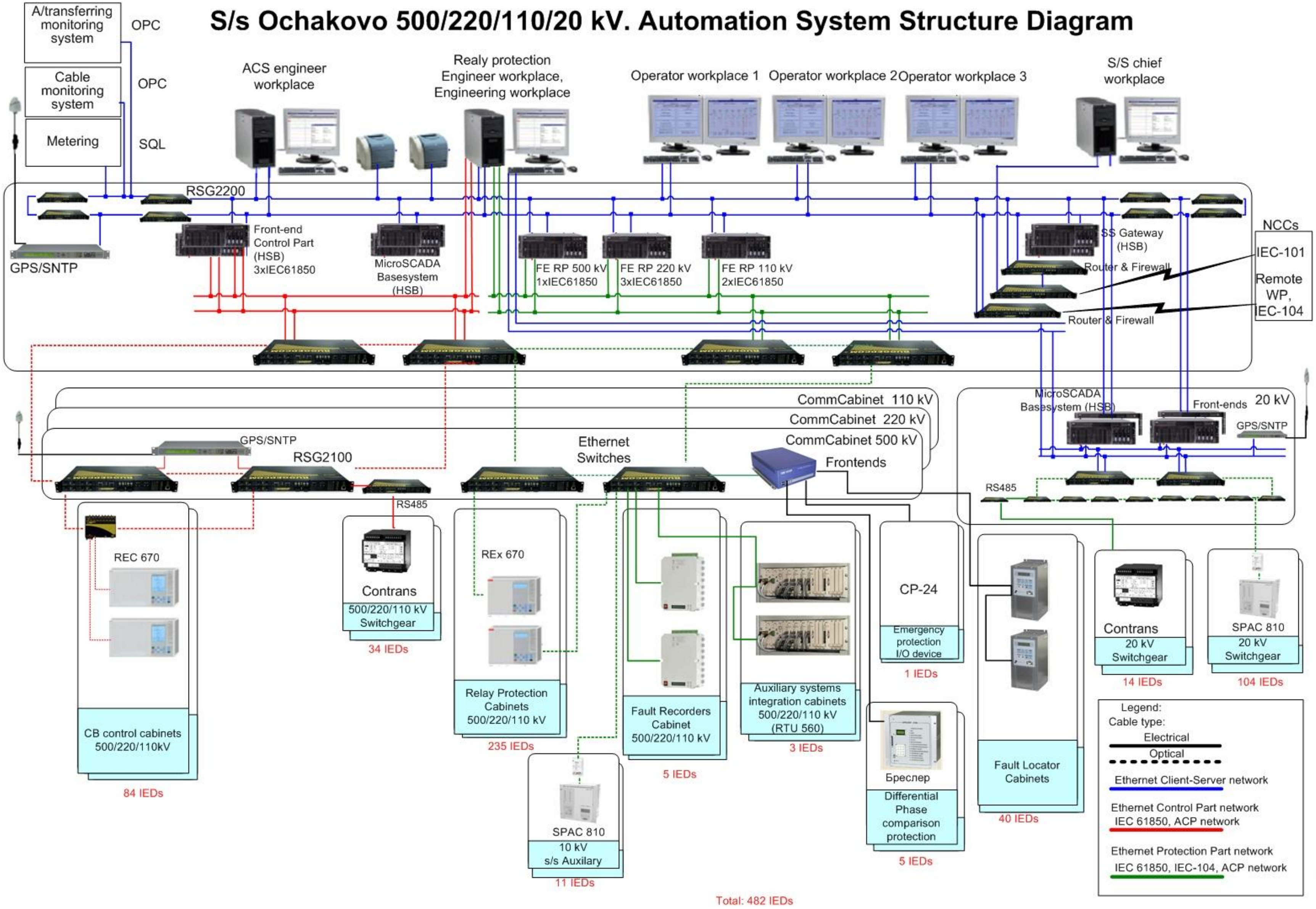
- **650 series**
  Pre-configured and ready-to-use solutions for generation, transmission and sub-transmission applications

- **620 series**
  Flexibility and performance for demanding utility distribution and industrial applications

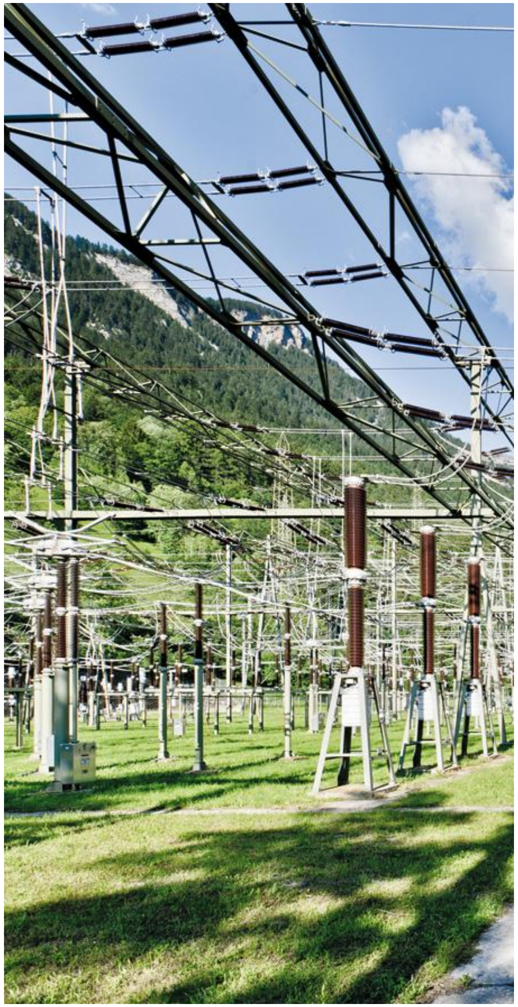
- **615 series**
  Compact and powerful solution for utility distribution and industrial applications

Ochakovo S/S, Russia
Substation Automation – System Overview

S/s Ochakovo 500/220/110/20 kV. Automation System Structure Diagram



Cyber security in your Relion Solutions
Agenda



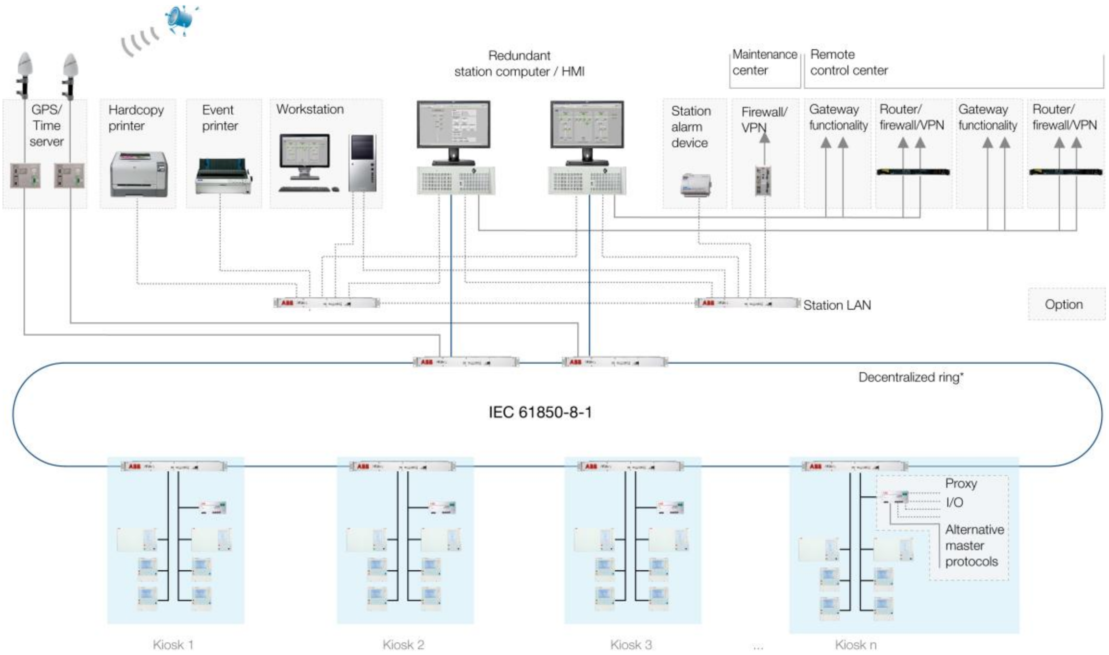
- Relion® protection and control
- IEC61850 Based Substation Automation Systems
- Cyber Security for Substation Automation Systems
- ABB approach
- Conclusions

Substation Automation
Functional allocation

Station Level

Bay Level

Process Level



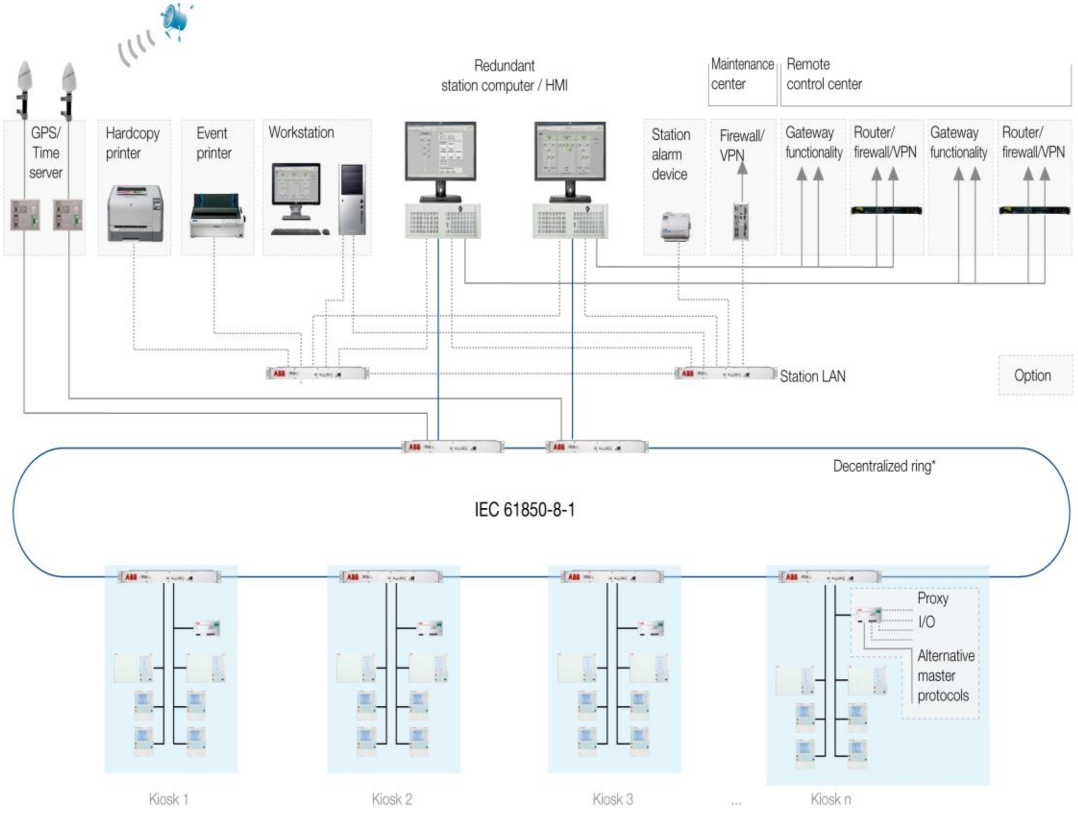
Functions

- Station Automation
- Monitoring
- Fault evaluation
- Event & Alarm Viewing and Acknowledgement
- Remote Communication for Telecontrol & Supervision

- Protection
- Control
- Monitoring
- Interlocking
- Data acquisition

- GIS or AIS Switchgear
- Instrument Transformers
- Power Transformers
- Surge Arresters
- Non-conventional trfrs

Substation Automation
Product portfolio



Station Level

MicroSCADA Pro

- SYS600
- SYS600C

RTU560

- RTU560A,C, G

COM600

Comm

AFS Family

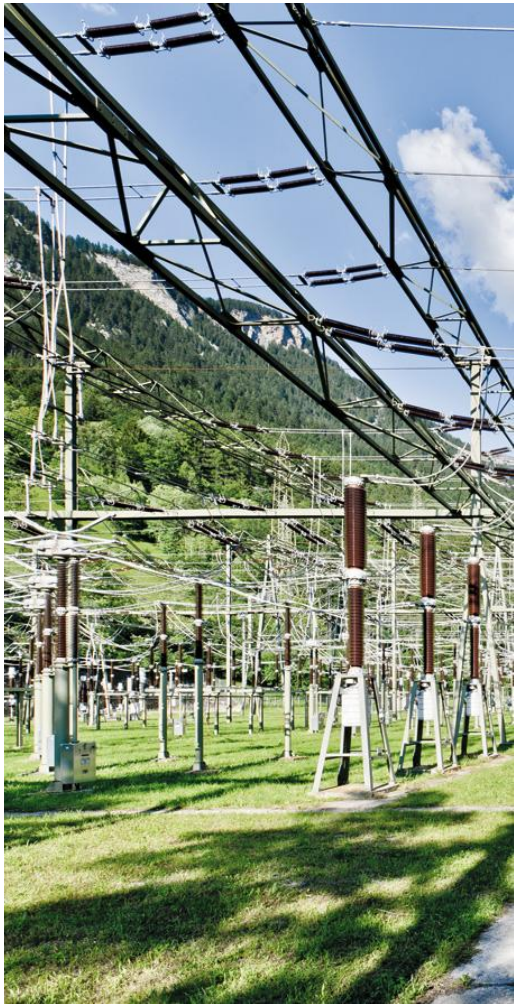
- AFS670, 675, 677
- AFS650, 655

Bay Level

Relion

- 670 Series
- 650 Series
- 630 Series
- 620 Series
- 615 Series

Cyber security in your Relion Solutions
Agenda



- Relion® protection and control
- IEC61850 Based Substation Automation Systems
- Cyber Security for Substation Automation Systems
- ABB approach
- Conclusions

Cyber Security for Substation Automation
Why is Cyber Security an issue?

- Cyber security has become an issue **by introducing Ethernet (TCP/IP) based communication protocols** to industrial automation and control systems. e.g. IEC60870-5-104, DNP 3.0 via TCP/IP or IEC61850
- **Connections to and from external networks** (e.g. office intranet) to industrial automation and control systems have opened systems and can be misused for cyber attacks.
- **Cyber attacks on industrial automation and control systems are real and increasing**, leading to large financial losses
- **Utilities need to avoid liability** due to non-compliance with regulatory directives or industry best practices;

Cyber Security for Substation Automation
Key Cyber-Security initiatives

Standard	Main Focus	Status
NIST SGIP-CSWG	Smart Grid Interoperability Panel – Cyber Security Working Group	On-going *
NERC CIP	NERC CIP Cyber Security regulation for North American power utilities	Released, On-going *
IEC 62351	Data and Communications Security	Partly released, On-going *
IEEE PSRC/H13 & SUB/C10	Cyber Security Requirements for Substation Automation, Protection and Control Systems	On-going*
IEEE 1686	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities	Finalized
ISA S99	Industrial Automation and Control System Security	Partly released, On-going *

* On-going: major changes will affect the final solution

NERC CIP – In a nutshell
The Standards

CIP-002	**Critical Cyber Asset Identification**
CIP-003	**Security Management Controls**
CIP-004	**Personnel and Training**
CIP-005	**Electronic Security Perimeters**
CIP-006	**Physical Security of Critical Cyber Assets**
CIP-007	**Systems Security Management**
CIP-008	**Incident Reporting and Response Planning**
CIP-009	**Recovery Plans for Critical Cyber Assets**

NERC CIP – Technical impact on SA Systems
CIP-005 Electronic Security Perimeter

- CIP-002
- CIP-003
- CIP-004
- **CIP-005**
- CIP-006
- CIP-007
- CIP-008
- CIP-009

the Responsible Entity shall

1. ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter
2. control electronic access at all electronic access points
3. monitor and log access at access points

NERC CIP – Technical impact on SA Systems
CIP-005 Electronic Security Perimeter

CIP-002
CIP-003
CIP-004
CIP-005
CIP-006
CIP-007
CIP-008
CIP-009

All Critical Cyber Assets must be inside Electronic Security Perimeter(s) with identified Access Points

Access Points must

- Deny access by default
- Have enabled only those ports and services for operations and monitoring the Cyber Assets inside the ESP
- Implement strong authentication for external access
- Log & monitor access
- Detect & alert unauthorized access attempts

NERC CIP – Technical impact on SA Systems
CIP-007 Systems Security Management

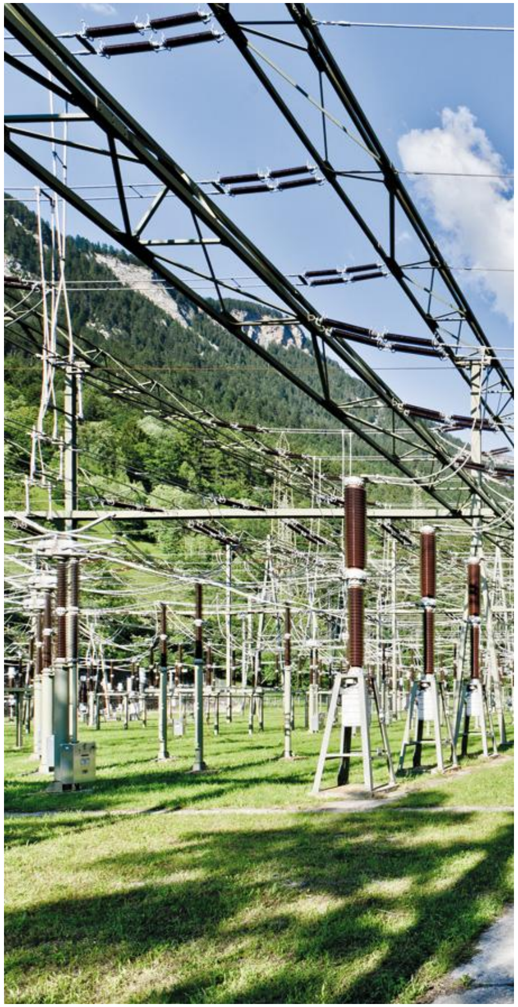
- CIP-002
- CIP-003
- CIP-004
- CIP-005
- CIP-006
- **CIP-007**
- CIP-008
- CIP-009

the Responsible Entity shall

1. shall ensure that only those Ports and Services required for normal and emergency operations are enabled
2. shall have a Security Patch Management program
3. shall use Malicious Software Prevention tools
4. enforce access authentication of and accountability for all user activity
5. shall implement Security Status Monitoring

→ **These requirements apply to all Cyber Assets within an Electronic Security Perimeter**

Cyber security in your Relion Solutions
Agenda

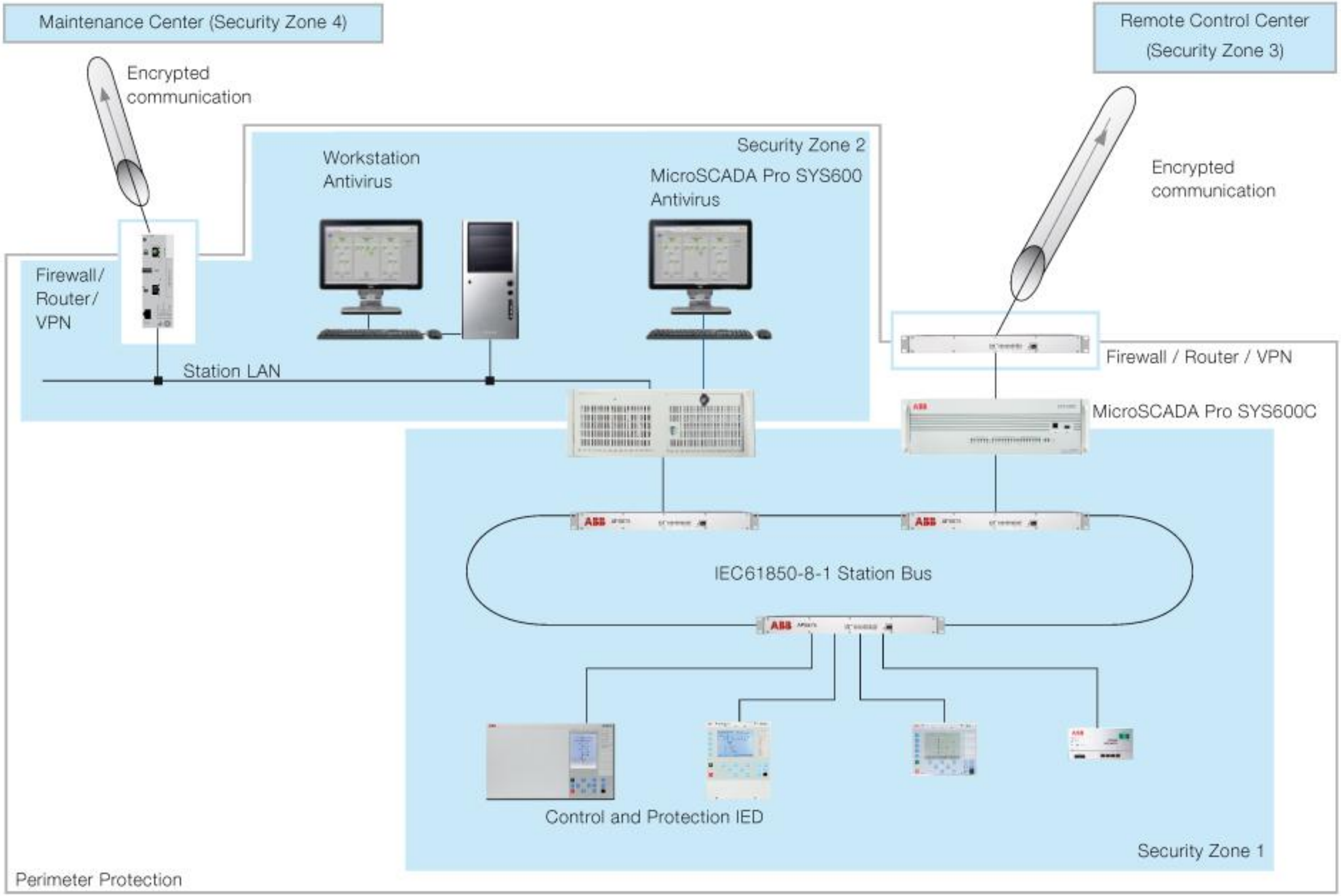


- Relion® protection and control
- IEC61850 Based Substation Automation Systems
- Cyber Security for Substation Automation Systems
- ABB approach
- Conclusions

Cyber Security for Substation Automation
Cyber security on system level

- Interactions between the substation automation system, corporate networks and the outside world are usually handled on the station level
- ABB uses best-in-class firewalls, intrusion detection or prevention systems, or VPN technology.
  - to protect all communication from the outside world to a substation
  - to divide systems into multiple security zones

Cyber Security for Substation Automation
Cyber security on system level



Cyber Security for Substation Automation
Cyber security features in station level products

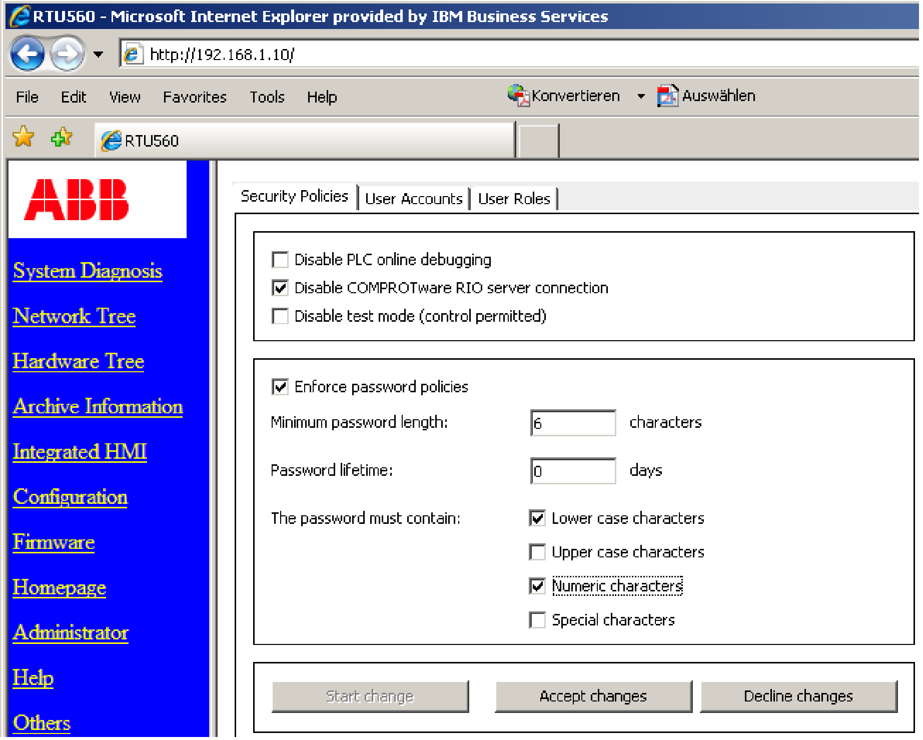
- Cyber security requirements need to be addressed both on system as well as on product level.
- ABB's station-level products MicroSCADA Pro and RTU560 have been designed with cyber security in mind and thus provide state-of-the-art functionality in this regard
- This allows our customers to easily address NERC CIP requirements and maintain compliance according to the standards and beyond

Cyber Security for Substation Automation
Cyber security features in station level products

Overview of security features

- Individual user accounts
- Role based access control
- Enforced password policies
- Session management
- Detailed audit trails
- Secure remote management connecti
- Built-in firewall
- Built-in VPN capabilities
- Support for antivirus solutions
- Disabled unused ports and services

Cyber Security for Substation Automation
Authentication and authorization



□ Disable PLC online debugging
☑ Disable COMPROTware RIO server connection
□ Disable test mode (control permitted)

☑ Enforce password policies

Minimum password length: 6 characters

Password lifetime: 0 days

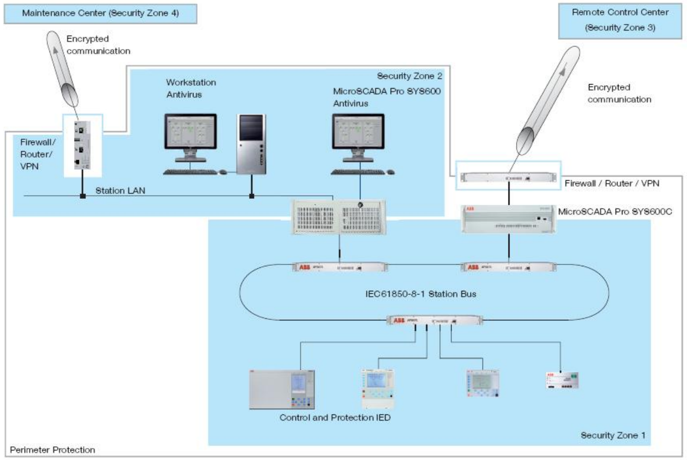
The password must contain:
☑ Lower case characters
□ Upper case characters
☑ Numeric characters
□ Special characters

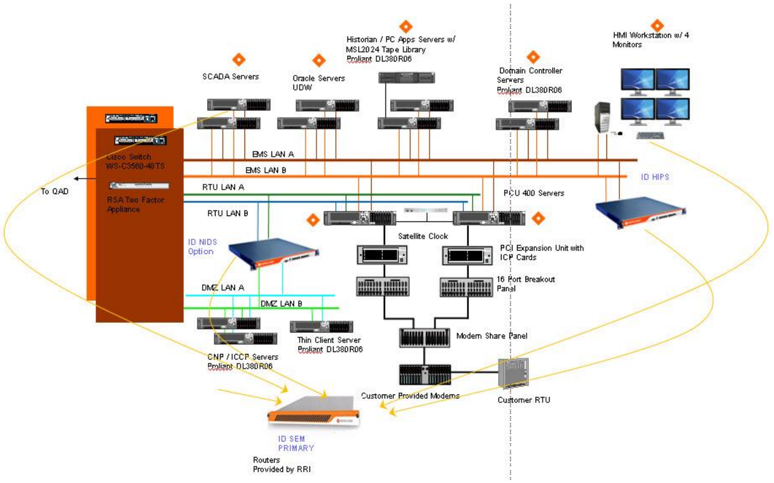
- Password construction
  - Following password complexities can be enforced by administration
    - Minimum password length
    - At least one upper and one lower case character
    - At least one number
    - At least one non-alphanumerical character
  - Encrypted password files can be exported or distributed to other RTU's via file transfer

Cyber Security for Substation Automation
Product and system hardening

- Our products are continuously being hardened. For example,
  - unused ports are closed and services have been removed
  - only ports and services for normal operation are enabled in ABB devices by default
- Hardening steps as well as the resulting configurations, such as open ports and services, are documented in detail
- ALL products are thoroughly tested at ABB‘s dedicated, independent security test center using state-of-the-art commercial and open source security testing tools.

ABB -Industrial Defender Partnership
Benefits for end-users





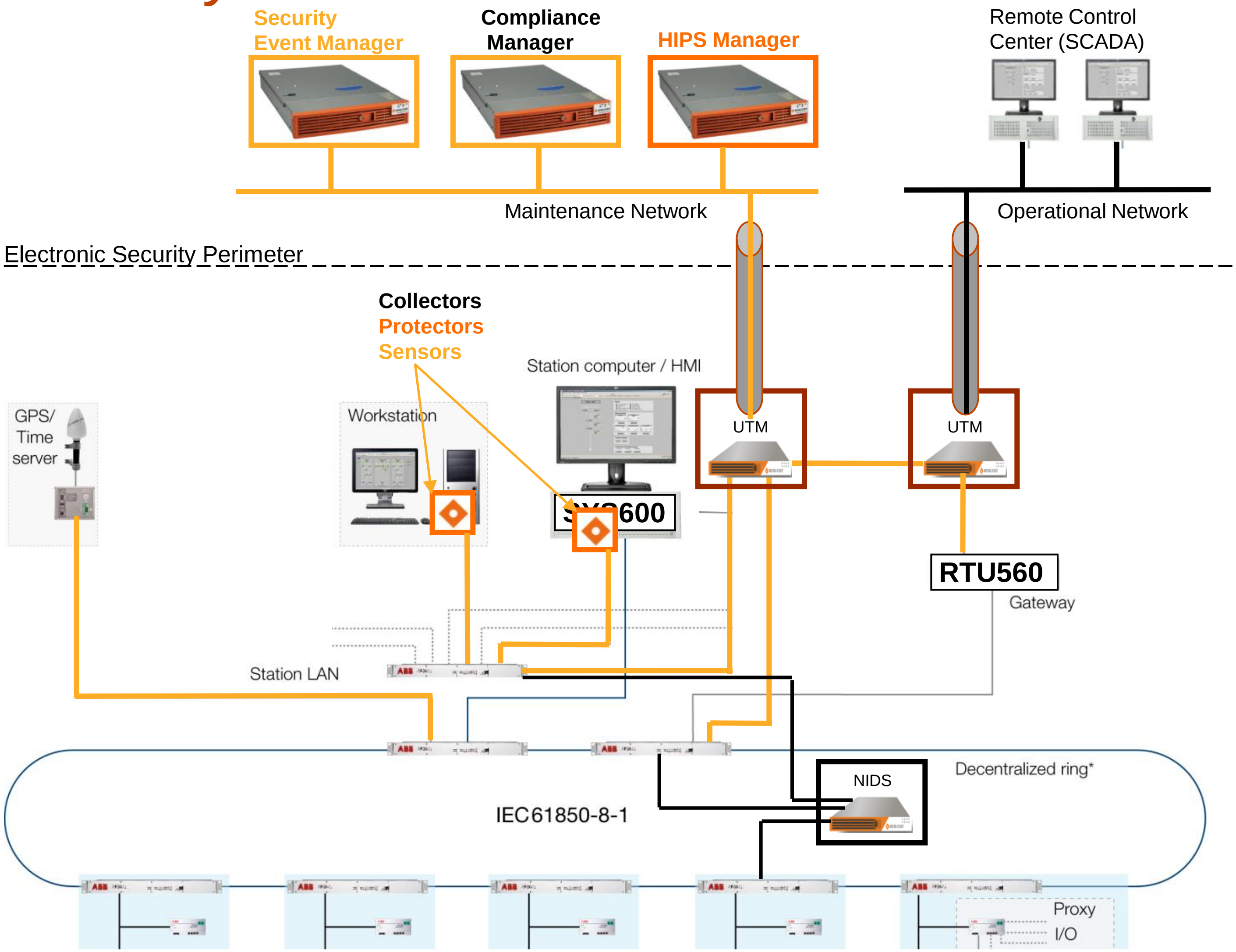
Robust,
security enabled
ABB – products

+

Industrial
Defender
cyber security
solutions

Defense in Depth

SAS 600 Series + Industrial Defender Security add-on’s



- Logging and alarming

  Centralized logging, management, analysis, reports, dashboard, …

- Perimeter protection

  UTM: Threat manager

- Secure communication

  VPN, IPSec

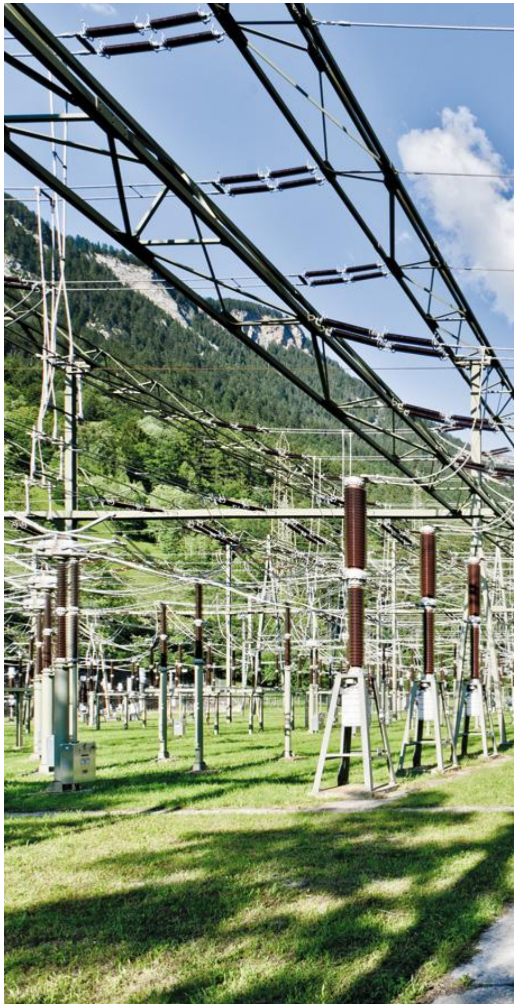
- Malware protection

  Host Intrusion Protection System (HIPS) / Protectors

- Intrusion detection

  Network intrusion detection (NIDS)

Cyber security in your Relion Solutions
Agenda



- Relion® protection and control
- IEC61850 Based Substation Automation Systems
- Cyber Security for Substation Automation Systems
- ABB approach
- Conclusions

ABB’s Cyber Security Activities
Summary

- Security is well established within ABB
- Today we can deliver products and systems that meet customer security requirements
- We will continue to adapt our products and system to meet additional requirements from customers and standards

Reminders
Automation & Power World 2011

- Please be sure to complete the workshop evaluation
- Professional Development Hours (PDHs) and Continuing Education Credits (CEUs):
  - You will receive a link via e-mail to print certificates for all the workshops you have attended during Automation & Power World 2011.
  - BE SURE YOU HAVE YOUR BADGE SCANNED for each workshop you attend. If you do not have your badge scanned you will not be able to obtain PDHs or CEUs.

Power and productivity
for a better world™