This webinar brought to you by The Relion® Product Family

Next Generation Protection and Control IEDs from ABB

Relion®. The perfect choice for every application.

The widest range of products for power systems protection, control, measurement and supervision. Interoperable and future-proof solutions designed to implement the core values of the IEC 61850 standard. ABB's leading-edge technology, global application knowledge and experienced support network ensures complete confidence that your system performs reliably - in any situation.

ABB Protective Relay School Webinar Series
Disclaimer

ABB is pleased to provide you with technical information regarding protective relays. The material included is not intended to be a complete presentation of all potential problems and solutions related to this topic. The content is generic and may not be applicable for circumstances or equipment at any specific facility. By participating in ABB's web-based Protective Relay School, you agree that ABB is providing this information to you on an informational basis only and makes no warranties, representations or guarantees as to the efficacy or commercial utility of the information for any specific application or purpose, and ABB is not responsible for any action taken in reliance on the information contained herein. ABB consultants and service representatives are available to study specific operations and make recommendations on improving safety, efficiency and profitability. Contact an ABB sales representative for further information.

ABB Protective Relay School webinar series

Cyber Security in Substations

Steven A. Kunsman

December 16, 2014

Power and productivity
for a better world™

Presenter

Steven A. Kunsman
Vice-President Business Development
ABB Power Systems
Substation Automation Products North America

Steve joined ABB Inc. in 1984 and has 30 years of experience in substation automation, protection and control. He graduated from Lafayette College with a BS in electrical engineering and Lehigh University with an MBA concentrated in management of technology. Today, Steve is responsible for ABB North American Power Systems Substation Automation Products business. He is an active member of the IEEE Power Engineering Society PSRC including working group chairperson for H13, an IEC TC57 US delegate in the development of the IEC61850 communication standard and UCA International Users Group Executive Committee co-chairperson.

Question

What are you mainly looking for today?

1. Better understanding of the drivers for cyber security
2. High level overview of how to address cyber security
3. Technical discussion on how to address cyber security
4. Understand what the future brings

Agenda

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

- Introduction to cyber security
- Main drivers
- Discussion of risk
- Challenges
- Solution approaches
- Conclusions

What is Cyber Security?

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

What is Cyber Security?

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

NERC CIP

or maybe not after all …

What is Cyber Security?

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

The goals of Cyber Security are

- **Availability** – avoid denial of service
- **Integrity** – avoid unauthorized modification
- **Confidentiality** – avoid disclosure
- **Authentication** – avoid spoofing / forgery
- **Authorization** – avoid unauthorized usage
- **Auditability** – avoid hiding of attacks
- **Non-repudiation** – avoid denial of responsibility

Cyber Security has

- **functional aspects** (e.g. user authentication, firewall, anti-virus)
- **quality aspects** (e.g. defense in depth, testing)

Why is it an issue?

Introduction

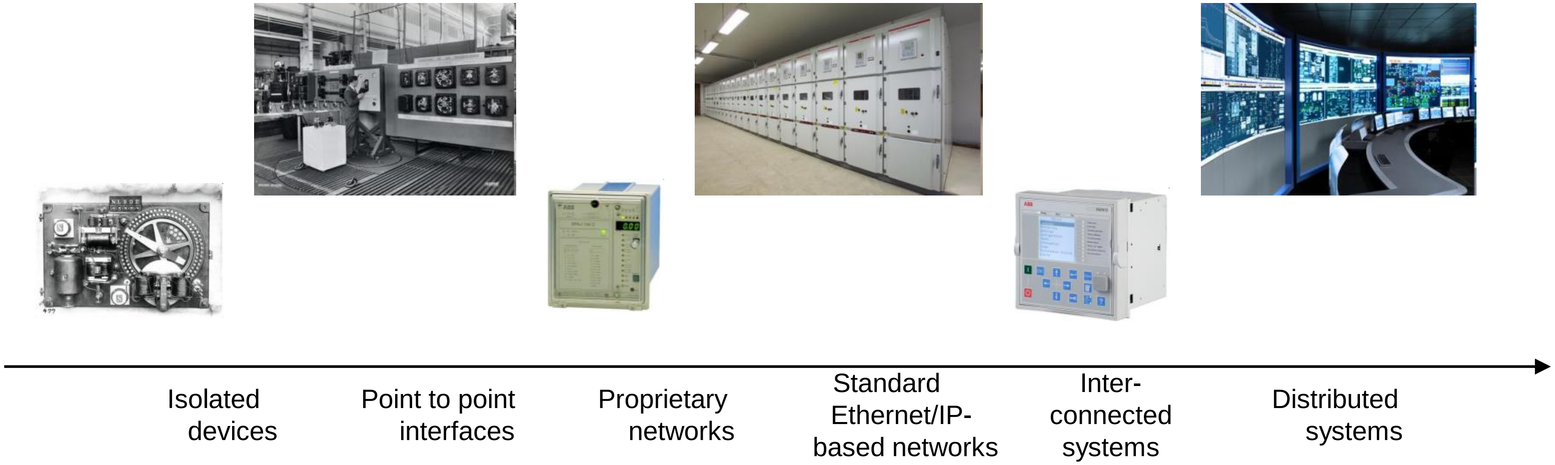
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



Isolated devices

Point to point interfaces

Proprietary networks

Standard Ethernet/IP-based networks

Inter-connected systems

Distributed systems

Modern automation, protection and control systems:

- **leverage standard IT components (e.g. MS Windows, Internet Explorer)**
- **use IP based communication protocols (“Internet technology”)**
- **are connected to external networks**
- **use mobile devices and storage media**

Modern control systems are specialized IT Systems

Demand & drivers for cyber security

Drivers for Cyber Security
The global picture

Introduction

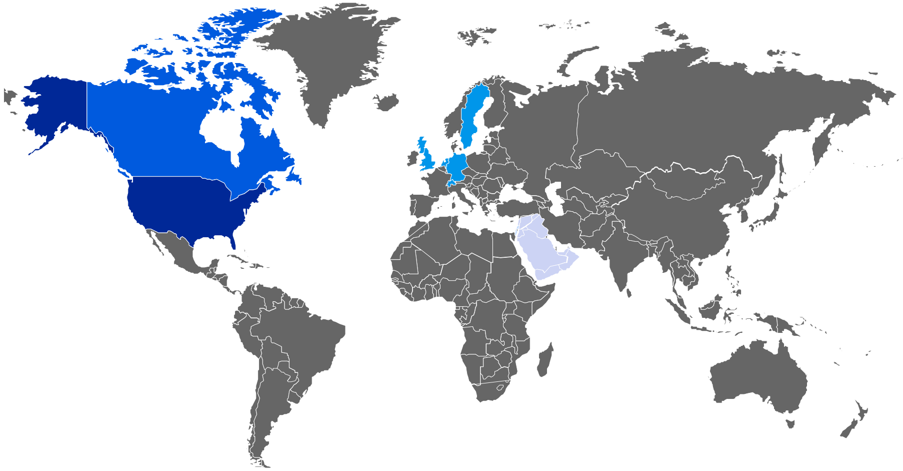
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



USA – biggest security demand, mainly driven by regulation and Smart Grid initiatives

Canada – similar to USA

Europe – less security demand, main drivers NL, Germany, Sweden, UK

Middle East – security demand still low to medium but increasing

Drivers for Cyber Security
By industry and applications

Introduction

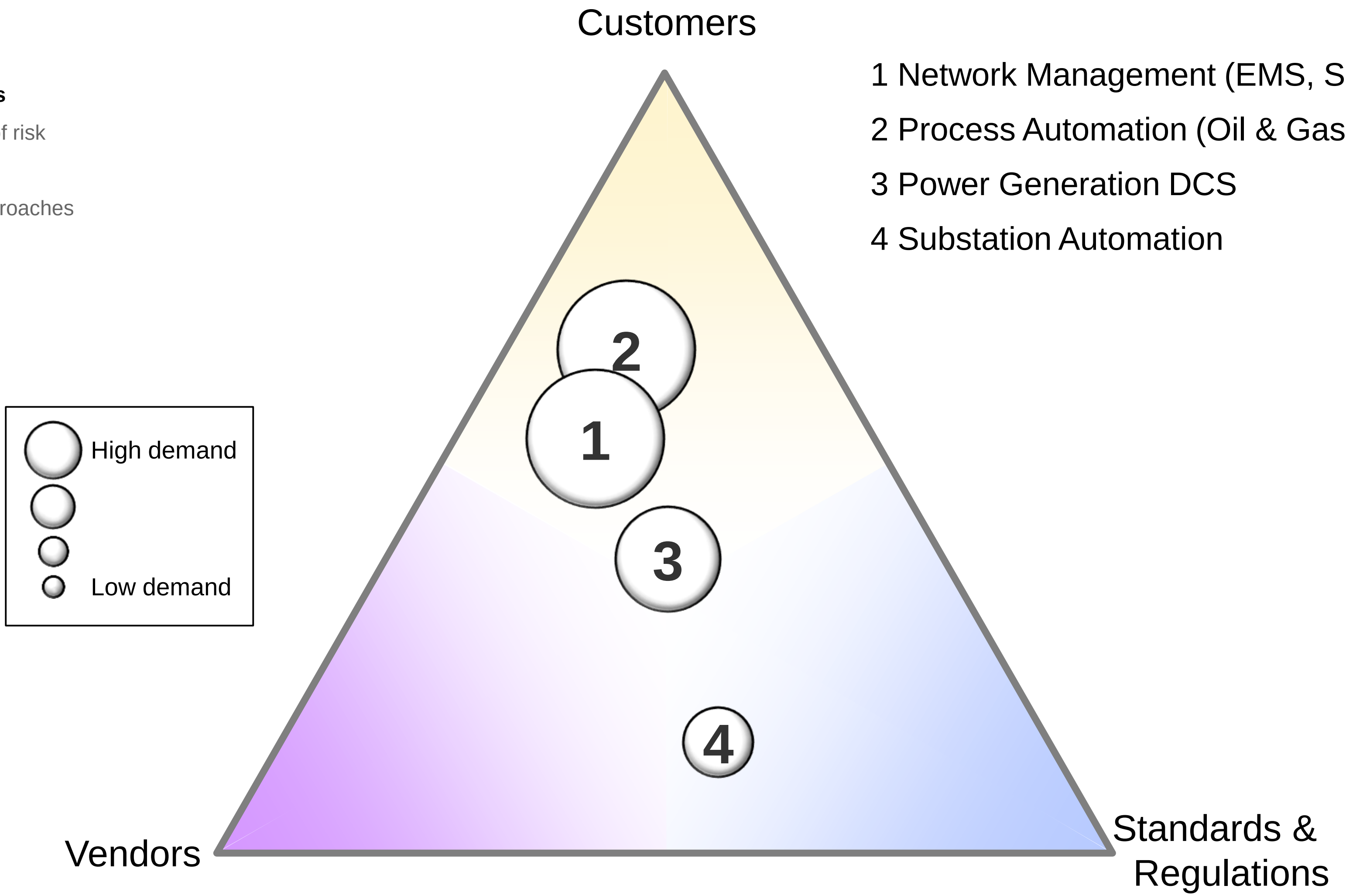
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



1 Network Management (EMS, SCADA)

2 Process Automation (Oil & Gas)

3 Power Generation DCS

4 Substation Automation

Drivers for Cyber Security
What about Smart Grid?

Introduction

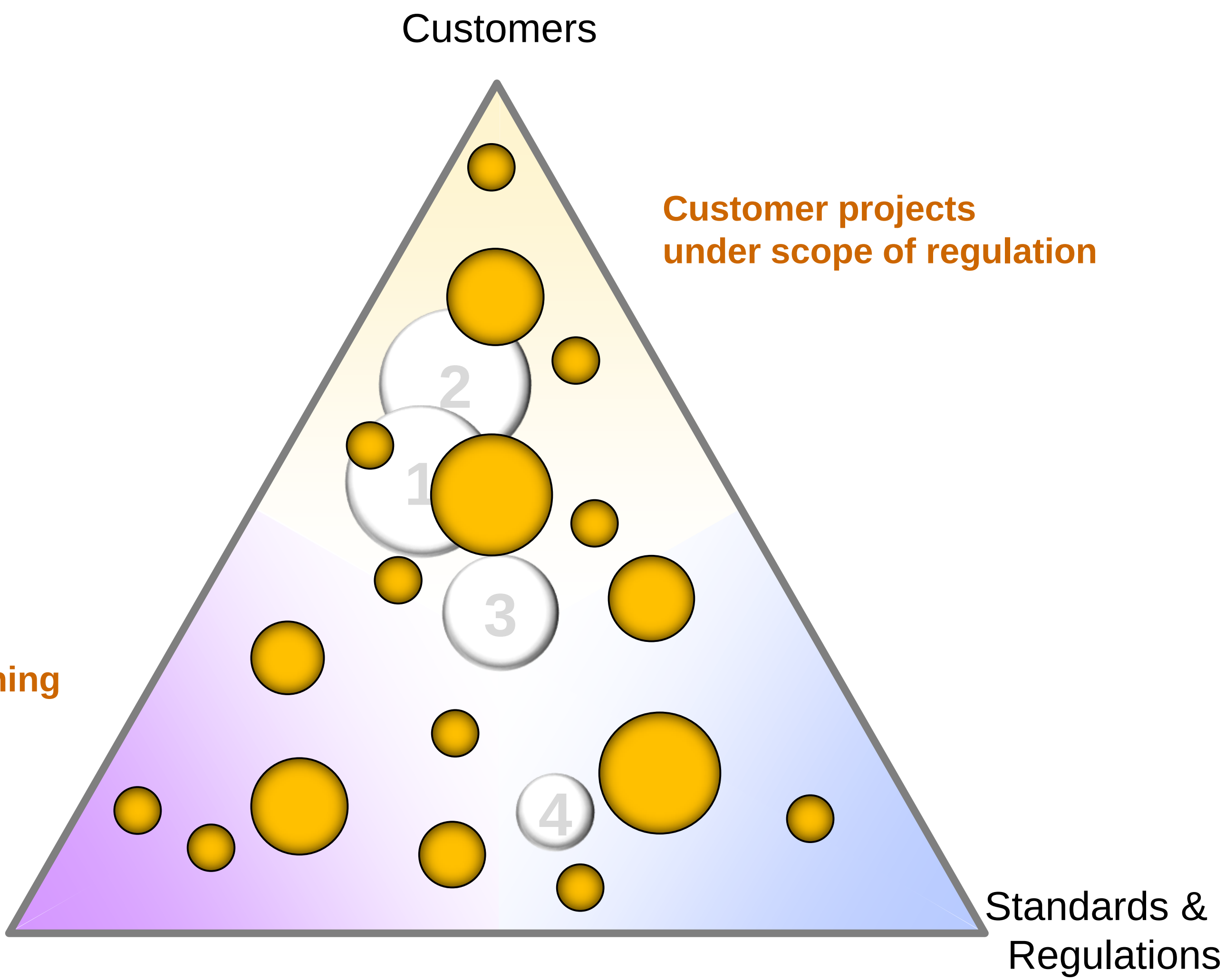
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



Customer projects under scope of regulation

Vendors pushing technology

NIST CSCTG

IEEE, AMI SEC, NERC CIP

Drivers for Cyber Security
Standards, regulations, best practices, …

Introduction

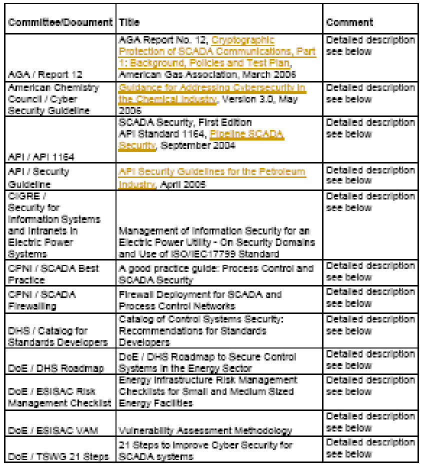
Main drivers

Discussion of risk

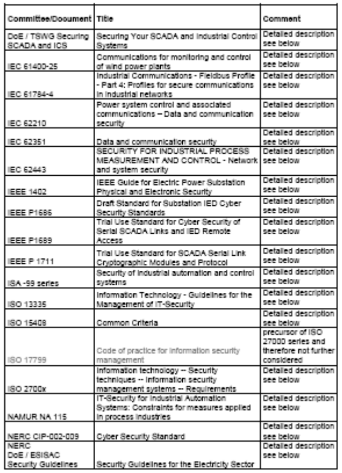
Challenges

Solution approaches

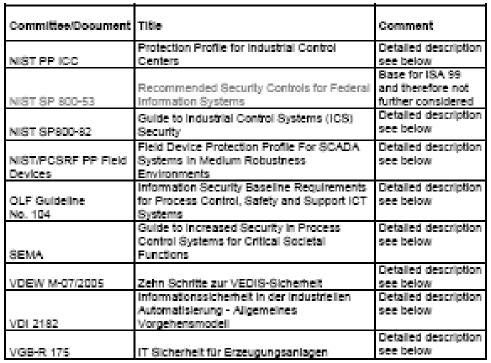
Conclusions



Committee/Document	Title	Comment
AGA / Report 12	AGA Report No. 12, Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, American Gas Association, March 2006	Detailed description see below
American Chemistry Council / Cyber Security Guideline	Guidance for Addressing Cybersecurity in the Chemical Industry, Version 3.0, May 2006	Detailed description see below
API / API 1164	SCADA Security, First Edition API Standard 1164, Pipeline SCADA Security, September 2004	Detailed description see below
API / Security Guideline	API Security Guidelines for the Petroleum Industry, April 2005	Detailed description see below
CIGRE / Security for Information Systems and Intranets in Electric Power Systems	Management of Information Security for an Electric Power Utility - On Security Domains and Use of ISO/IEC17799 Standard	Detailed description see below
CPNI / SCADA Best Practice	A good practice guide: Process Control and SCADA Security	Detailed description see below
CPNI / SCADA Firewalling	Firewall Deployment for SCADA and Process Control Networks	Detailed description see below
DHS / Catalog for Standards Developers	Catalog of Control Systems Security: Recommendations for Standards Developers	Detailed description see below
DoE / DHS Roadmap	DoE / DHS Roadmap to Secure Control Systems in the Energy Sector	Detailed description see below
DoE / ESISAC Risk Management Checklist	Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities	Detailed description see below
DoE / ESISAC VAM	Vulnerability Assessment Methodology	Detailed description see below
DoE / TSWG 21 Steps	21 Steps to Improve Cyber Security for SCADA systems	Detailed description see below



Committee/Document	Title	Comment
DoE / TSWG Securing SCADA and ICS	Securing Your SCADA and Industrial Control Systems	Detailed description see below
IEC 61400-25	Communications for monitoring and control of wind power plants	Detailed description see below
IEC 61784-4	Industrial Communications - Fieldbus Profile - Part 4: Profiles for secure communications in industrial networks	Detailed description see below
IEC 62210	Power system control and associated communications – Data and communication security	Detailed description see below
IEC 62351	Data and communication security	Detailed description see below
IEC 62443	SECURITY FOR INDUSTRIAL PROCESS MEASUREMENT AND CONTROL - Network and system security	Detailed description see below
IEEE 1402	IEEE Guide for Electric Power Substation Physical and Electronic Security	Detailed description see below
IEEE P1686	Draft Standard for Substation IED Cyber Security Standards	Detailed description see below
IEEE P1689	Trial Use Standard for Cyber Security of Serial SCADA Links and IED Remote Access	Detailed description see below
IEEE P 1711	Trial Use Standard for SCADA Serial Link Cryptographic Modules and Protocol	Detailed description see below
ISA -99 series	Security of industrial automation and control systems	Detailed description see below
ISO 13335	Information Technology - Guidelines for the Management of IT-Security	Detailed description see below
ISO 15408	Common Criteria	Detailed description see below
ISO 17799	Code of practice for information security management	precursor of ISO 27000 series and therefore not further considered
ISO 2700x	Information technology -- Security techniques -- Information security management systems -- Requirements	Detailed description see below
NAMUR NA 115	IT-Security for Industrial Automation Systems: Constraints for measures applied in process industries	Detailed description see below
NERC CIP-002-009	Cyber Security Standard	Detailed description see below
NERC DoE / ESISAC Security Guidelines	Security Guidelines for the Electricity Sector	Detailed description see below



Committee/Document	Title	Comment
NIST PP ICC	Protection Profile for Industrial Control Centers	Detailed description see below
NIST SP 800-53	Recommended Security Controls for Federal Information Systems	Base for ISA 99 and therefore not further considered
NIST SP800-82	Guide to Industrial Control Systems (ICS) Security	Detailed description see below
NIST/PCSRF PP Field Devices	Field Device Protection Profile For SCADA Systems in Medium Robustness Environments	Detailed description see below
OLF Guideline No. 104	Information Security Baseline Requirements for Process Control, Safety and Support ICT Systems	Detailed description see below
SEMA	Guide to Increased Security in Process Control Systems for Critical Societal Functions	Detailed description see below
VDEW M-07/2005	Zehn Schritte zur VEDIS-Sicherheit	Detailed description see below
VDI 2182	Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell	Detailed description see below
VGB-R 175	IT Sicherheit für Erzeugungsanlagen	Detailed description see below

…. and many, many more!

Technical vs. non-technical

Generic vs. application specific

End user vs. vendor centric

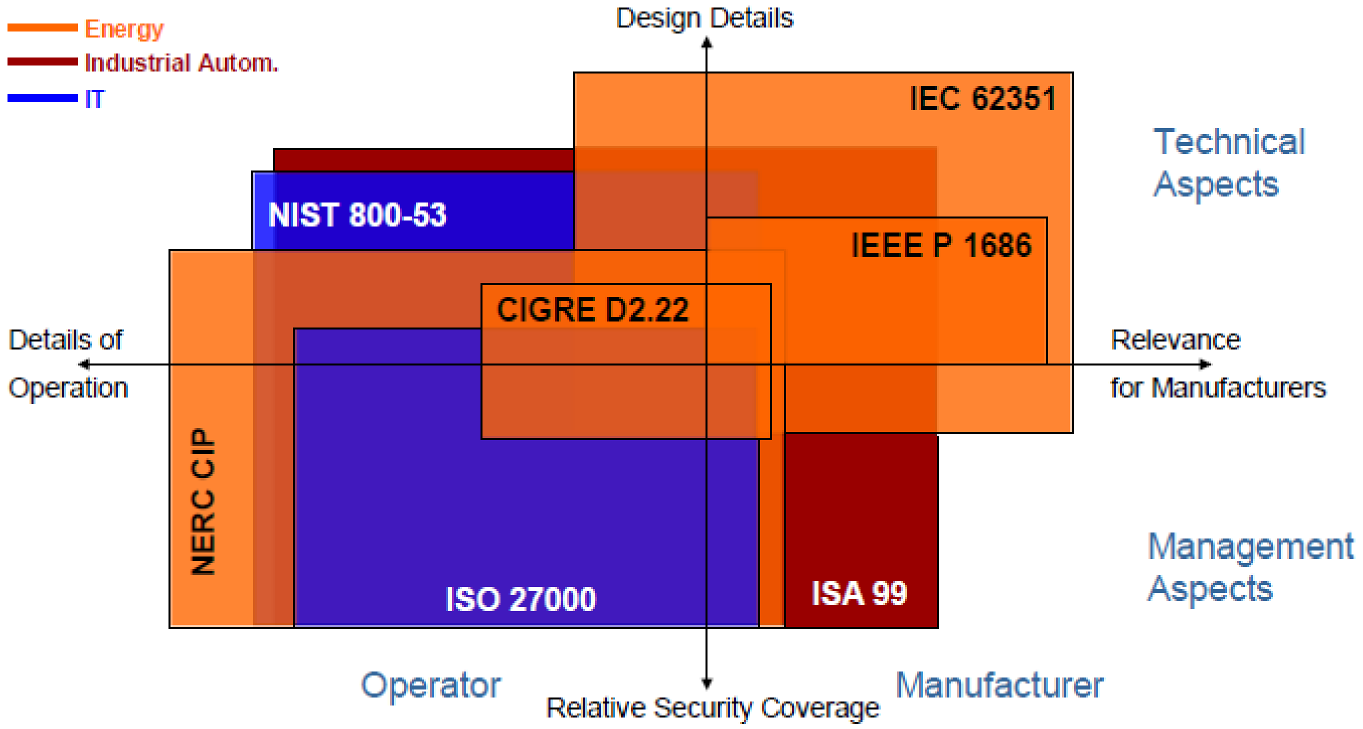
Drivers for Cyber Security
The most relevant efforts

- **NISTIR 7628 -** Smart Grid Cyber Security Strategy and Requirements
- **IEEE SA P2030 -** Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation With the Electric Power System (EPS), and End-Use Applications and Loads
- ★ **IEEE C37.240** - Cyber Security Requirements for Substation Automation, Protection and Control Systems
- ★ **IEEE P1686** - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
- ★ **IEEE P1711** - Trial Use Standard for Cyber Security of Serial SCADA Links and IED Remote Access
- ★ **IEC 62351** – Data and Communications Security
- **NERC CIP** – Security regulation for North American power utilities
- ISO/IEC 27001 – information security management processes
- ISA S99 – Industrial Automation and Control System Security

- ★ **Critical Infrastructure Cyber Community (aka "C Cubed") Voluntary Progam** – based on Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity* and released Presidential Policy Directive (PPD)-21: *Critical Infrastructure Security and Resilience*

http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program

Drivers for Cyber Security
Standards and their scope



- Graphical representation of scope and completeness of selected standards

*) source DTS IEC 62351-10 10: Security architecture guidelines

What is **really** driving Cyber Security?
What is driving the drivers?

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Currently many initiatives and activities driven by technology, solutions

however

Control System security should be based on an understanding of risk

So, how big is the risk?

Risk

Question

Who is responsible for most cyber security related incidents?

1. Hackers
2. Enemy States
3. Employees
4. Malware

Who are the attackers?

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

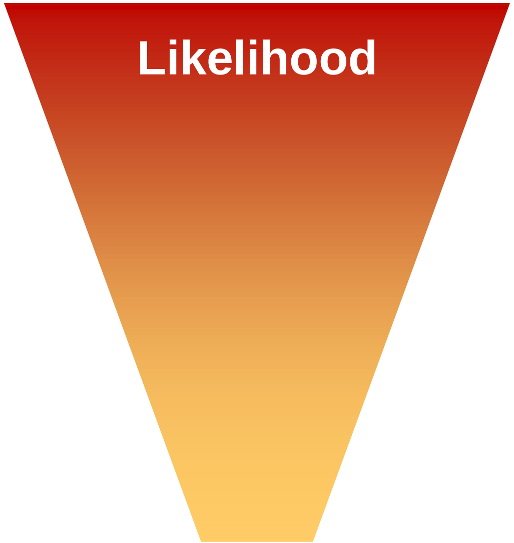
Accidents / Mistakes

Rogue insider

Malware

Thieves / Extortionists

Enemies / Terrorists



Bottom line is

- likelihood is unknown
- consequences are potentially huge

How big is the risk?

Introduction

Main drivers

Discussion of risk

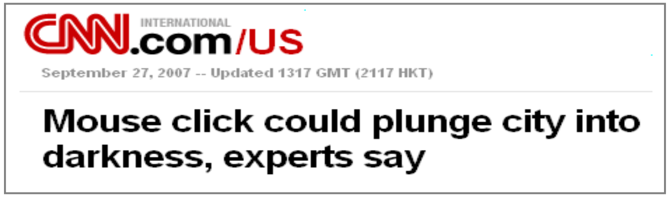
Challenges

Solution approaches

Conclusions

Stephen Cummings, director of the British government's Centre for the Protection of National Infrastructure,

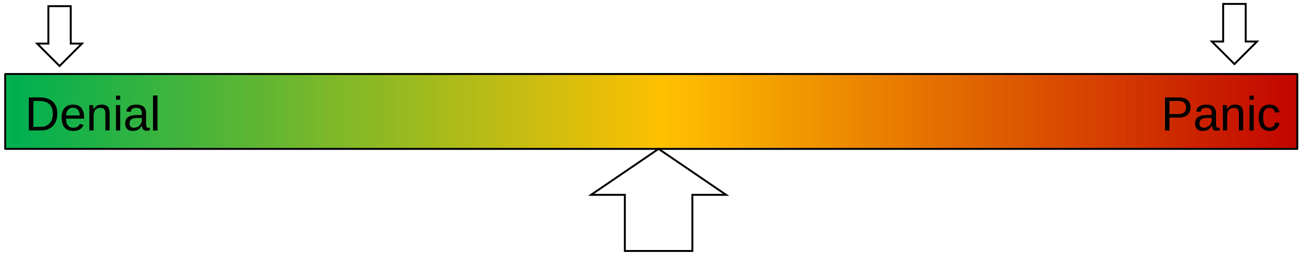
“Cyberterrorism is a myth”



CNN.com/US INTERNATIONAL

September 27, 2007 -- Updated 1317 GMT (2117 HKT)

Mouse click could plunge city into darkness, experts say



Reality

Cyber incidents are real and cyber security for industrial control systems must be taken seriously

but it is a challenge that **can** be met

TARGET

SONY

ABB

Challenges

Enterprise IT vs. Control Systems
A different set of challenges

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

	Enterprise IT	Control Systems
Primary object under protection	Information	Physical process
Primary risk impact	Information disclosure, financial	Safety, health, environment, financial
Main security objective	Confidentiality	Availability
Security focus	Central Servers (fast CPU, lots of memory, …)	Distributed System (possibly limited resources)
Availability requirements	95 – 99% (accept. downtime/year: 18.25 - 3.65 days)	99.9 – 99.999% (accept. downtime/year: 8.76 hrs – **5.25 minutes**)
Problem response	Reboot, patching/upgrade, isolation	Fault tolerance, online repair

Cyber Security vs. Safety
Similar but different

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Cyber Security = Safety

- Both require(d) a culture change
- Both are all about processes
- Both require training
- Both require top management support

Cyber Security ≠ Safety

- Safety is static and predictable (threats don’t change)
- Cyber Security is constantly changing (threats change)
- For Cyber Security the attacker evolves
- Safety solutions can be certified

NERC violation frequency

Introduction

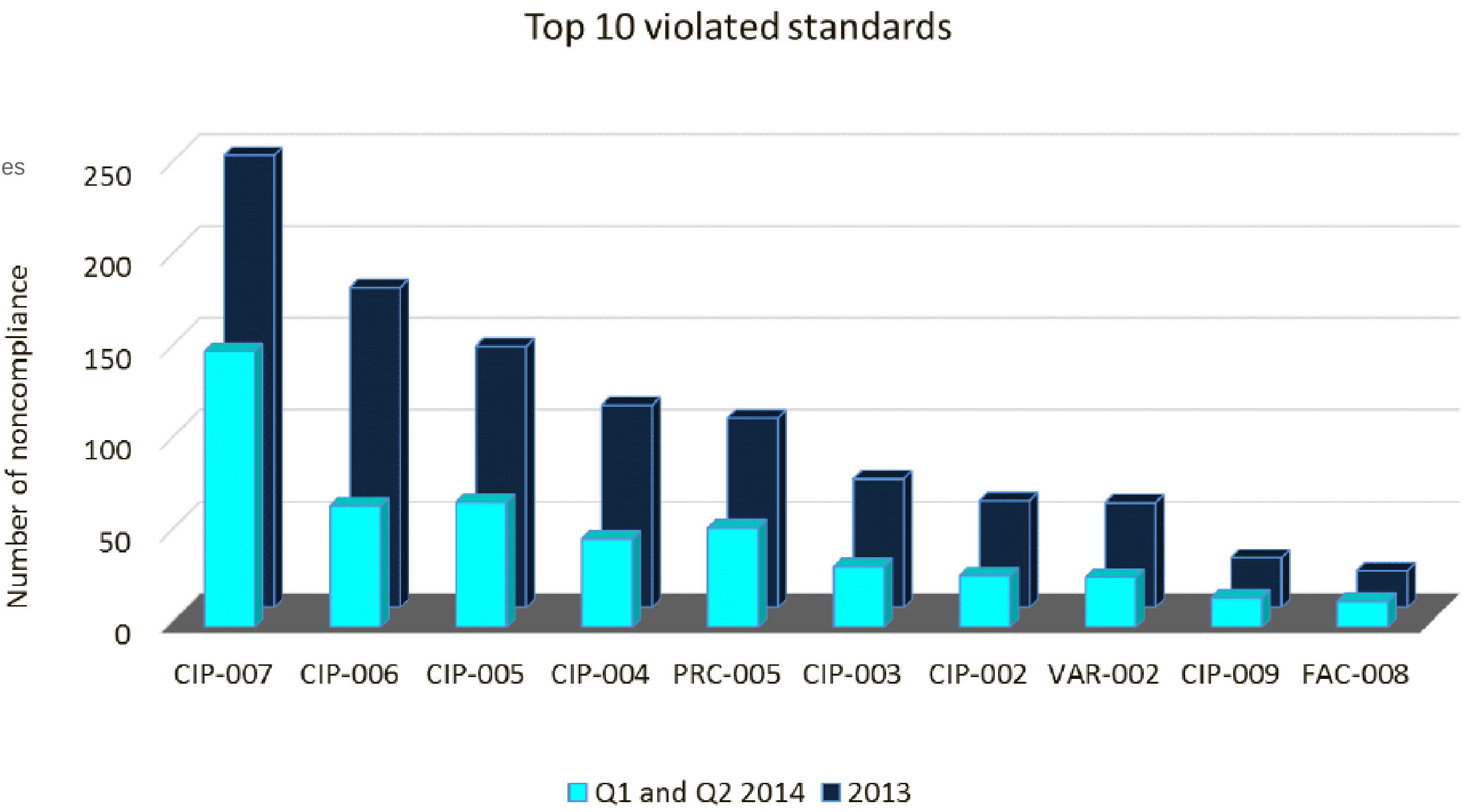
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/Key%20Comp%20Enf%20trends%20073014.pdf

CERC violation severity

Introduction

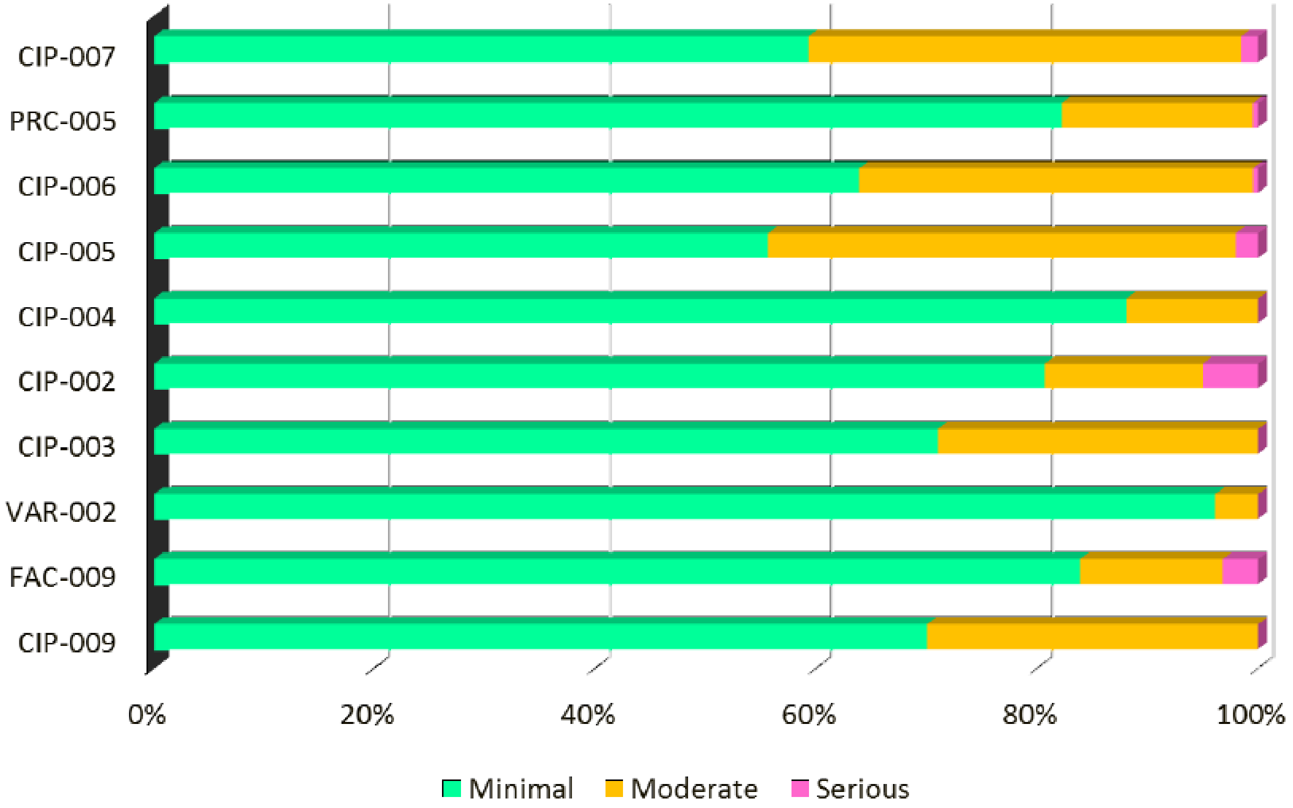
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



http://www.nerc.com/pa/comp/CE/Compliance%20Violation%20Statistics/Key%20Comp%20Enf%20trends%20073014.pdf

Main Challenges for End Users

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

WHY to protect **WHAT** from **WHOM** and **HOW**

Assessment of existing systems

Making cyber security part of risk management process

Definition of security requirements for vendors & system integrators

Operation and management of security architecture

- Continuous monitoring of the infrastructure
- Regular analysis of log files
- Regular reevaluation of security architecture
- Continuous threat modeling & risk management
- Development of IT-security policies and processes

Training of employees

Evaluation and planning of “new” costs

Main Challenges for End Users
Addressing risk

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Answer the what *ifs*

- What if I cannot operate this device
- What if someone else can operate this device
- What if this information gets disclosed

- **What if someone opens this breaker**
- **What if it does not open when it should**

Don’t fall for myths

Cyber security is only an issue for TCP/IP based systems

- Serial links are just as vulnerable
- Even isolated systems have entry points (e.g. portable media)

Cyber attacks will not come from within the physical perimeter because a physical attack would be easier

- Cyber attack can be much more sophisticated
- Substation could be used as entry point into system
- Cyber attack can be “accidental”

Security of “isolated” systems

- Most systems are NOT really isolated
- Virtual connections always exists (e.g. portable media, laptops)

Main Challenges for vendors

Introduction

Main drivers

Discussion of risk

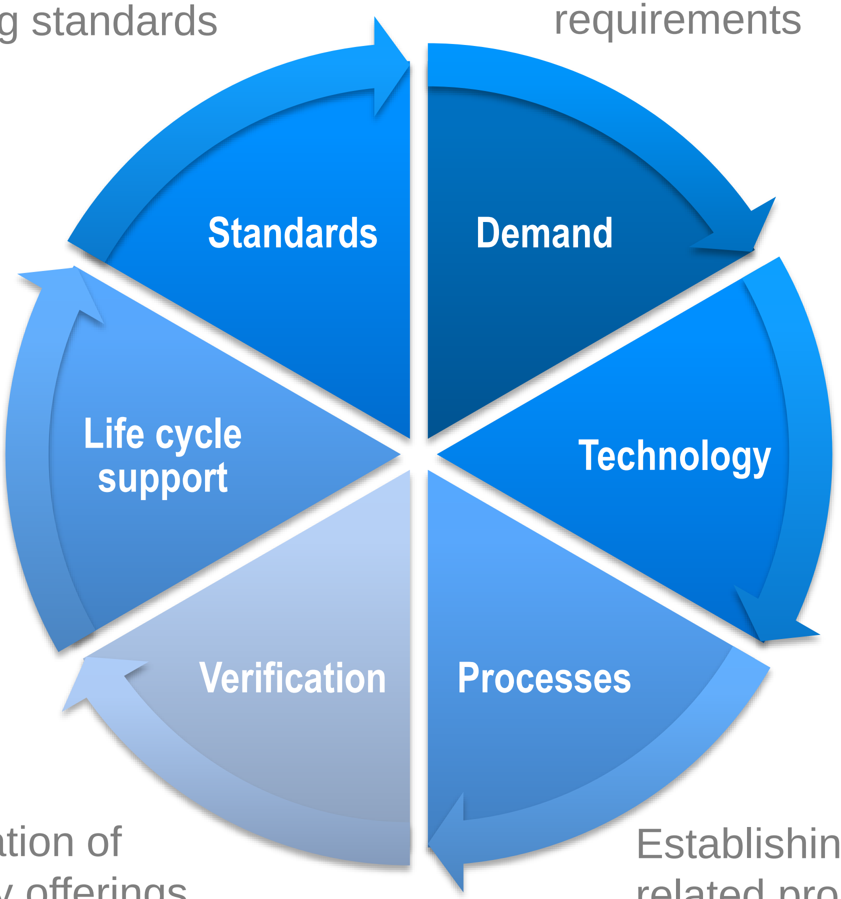
Challenges

Solution approaches

Conclusions

Supporting and driving standards

Different drivers and level of maturity
Different, sometimes contradictory requirements



Supporting customers in setting up and running security programs

Definition of requirements
Implementation of features
Integrating 3rd party solutions

Verification of security offerings

Establishing security related processes

Solution approaches

Back to the basics

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Accept responsibility

Security is about processes

Ignore compliance - at least at first

There is no such thing as 100% security

Security does not come for free

Use a pragmatic approach based on common best practices

Access Control & Least-privileges

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Make use of the possibility to have **personal** accounts

Make use of the ability to **change** passwords

Make use of (role based) access control to **limit** access privileges

System Hardening

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Systems already deployed can be hardened.

Servers and Workstations

- Removal of unused software
- Disabling unused services
- Removal unused accounts
- Change of default passwords

Network and other Devices

- Disabling unused services
- Removal unused accounts
- Change of default passwords

Network separation & Secure remote access
The basics

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Use firewalls, gateways etc. to create network zones

- Avoid flat networks

Create DMZ (demilitarized zones) for all external access

Block all traffic between zones by default

- Filter both on incoming and outgoing traffic

Use VPN gateways to secure remote access

- Terminate VPN connection outside a firewall

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 penalties due to non-compliance with regulatory directives or industry best practices

What to do today

Introduction

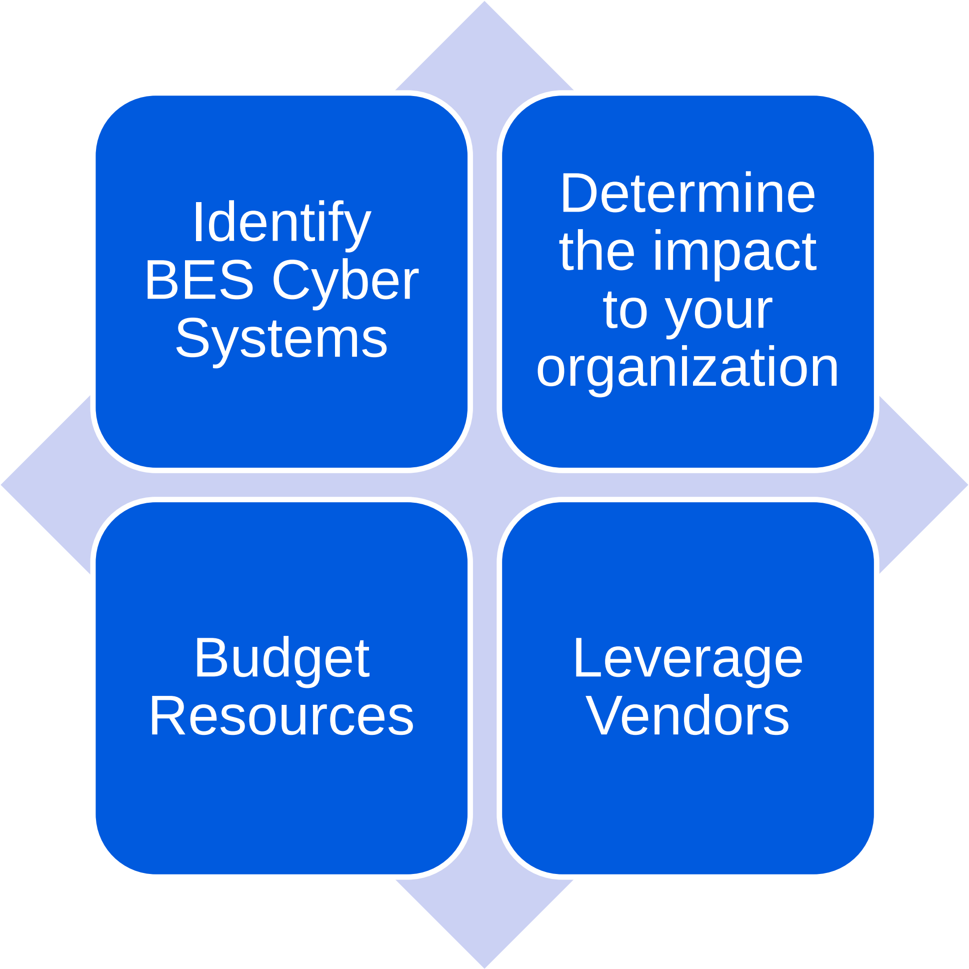
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions



Identify BES Cyber Systems

Determine the impact to your organization

Budget Resources

Leverage Vendors

Leveraging vendors
A holistic and collaborative approach

Introduction
Main drivers
Discussion of risk
Challenges
Solution approaches
Conclusions

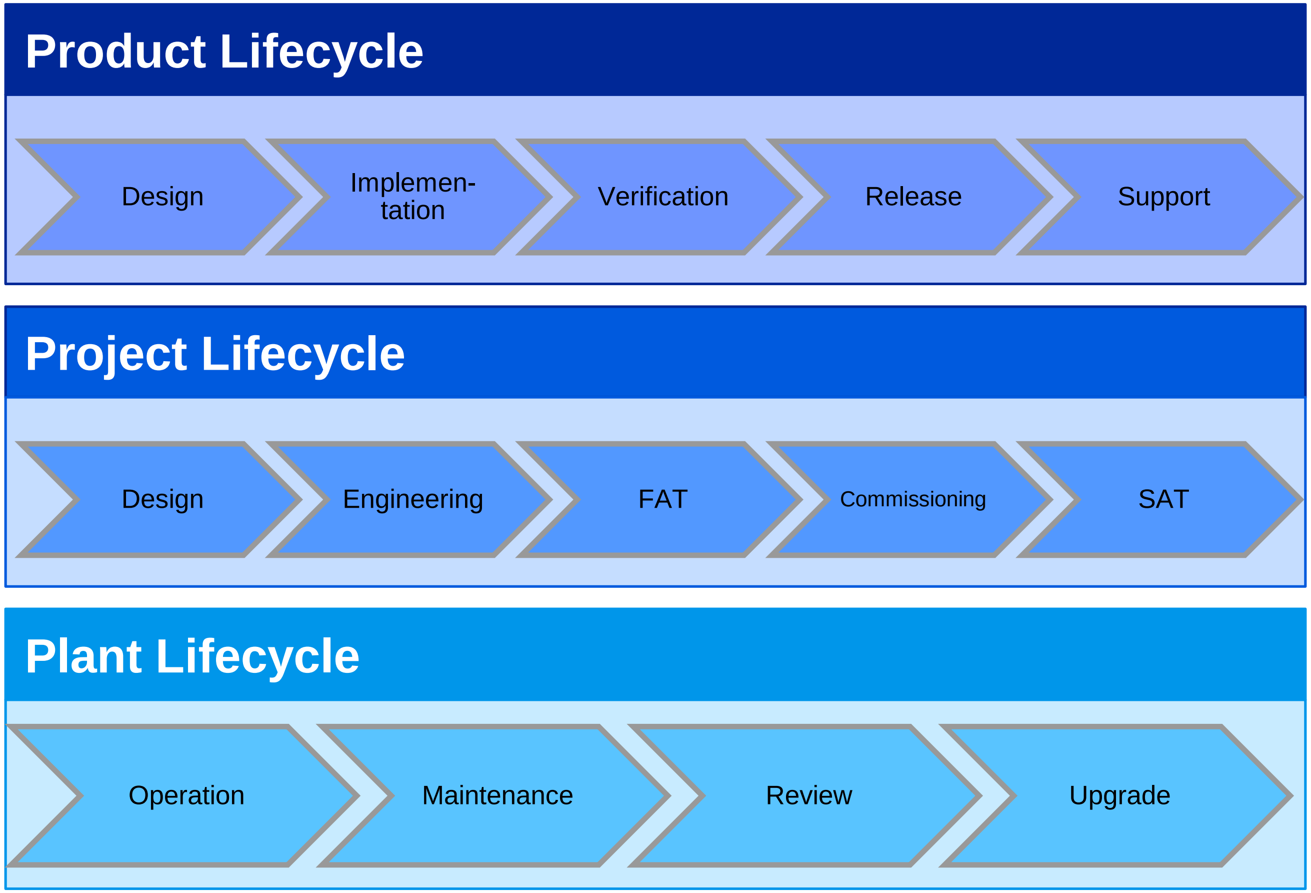
Vendor must view cyber security as an **integral** part of

- **product & project lifecycles** from product design, development, to delivery of solutions
  - Security must be baked in & not an after thought
- **rigorous security testing** to verify product maturity
- **prioritization of product capabilities** to support maturity in cyber security

Strong collaboration between customer and vendor

- Working closely with customers “Replacing Fear with Knowledge”
- Partnering with government organizations, industry partners or academia
- Actively participating and driving standards e.g. IEC 62431 & IEEE C37.240

ABB cyber security approach
From the product lifecycle to the plant lifecycle



Product Lifecycle

Design → Implementation → Verification → Release → Support

Project Lifecycle

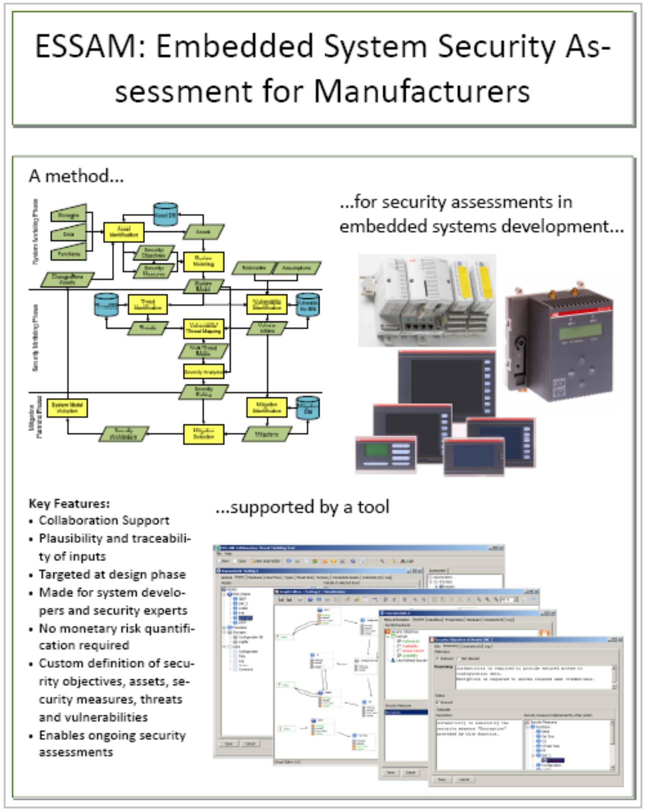
Design → Engineering → FAT → Commissioning → SAT

Plant Lifecycle

Operation → Maintenance → Review → Upgrade

Product lifecycle - design & implementation
Threat modeling

Product Lifecycle
Design
Implementation
Verification
Release
Support
Project Lifecycle
Design
Engineering
FAT
Commissioning
SAT
Plant Lifecycle
Operation
Maintenance
Renew
Upgrade



ESSAM: Embedded System Security Assessment for Manufacturers

A method...

System Modeling Phase
Security Modeling Phase
Mitigation Planning Phase
Data
Functions
Asset Identification
Asset DB
Assets
Security Objectives
Security Measures
System Modeling
System Model
Rationales
Assumptions
Threat Identification
Vulnerability Identification
Threats
Vulnerability/Threat Mapping
Severity Analysis
Severity Rating
System Model Adoption
Mitigation Identification
Mitigation Selection
Mitigations

...for security assessments in embedded systems development...

Key Features:

- Collaboration Support
- Plausibility and traceability of inputs
- Targeted at design phase
- Made for system developers and security experts
- No monetary risk quantification required
- Custom definition of security objectives, assets, security measures, threats and vulnerabilities
- Enables ongoing security assessments

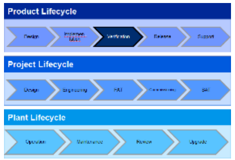
...supported by a tool

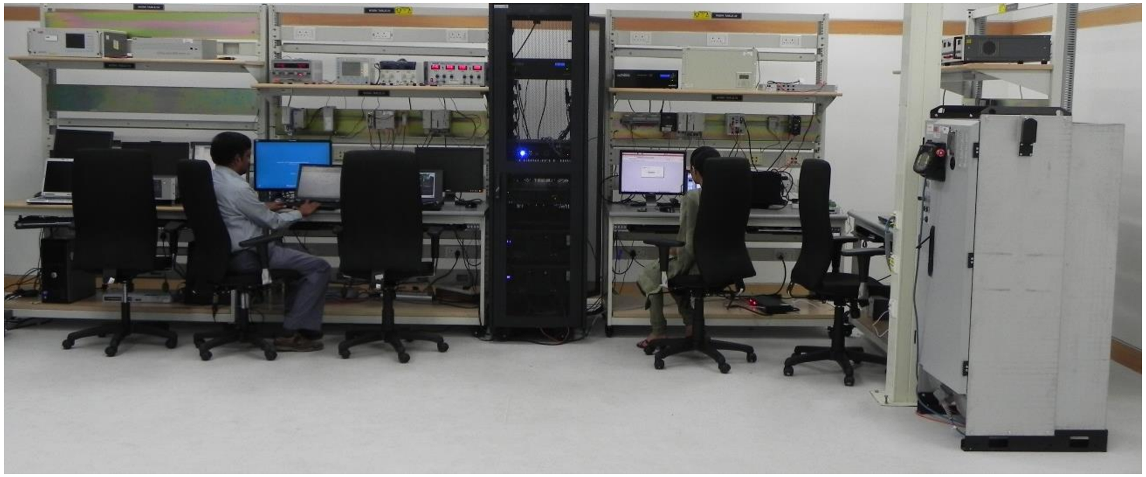
Design and development of products requires understanding of threats

Threat modeling methodology

- applicable to product-type systems
- applicable independent of deployment
- allows second parties to validate assumptions and compare results

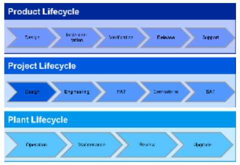
Product lifecycle - verification
Device security assurance center





- State-of-the-art cyber security testing
- Formally established, centralized and independent security test center
- Leveraging state-of-the-art open source, commercial and proprietary robustness and vulnerability analysis tools
- Close collaboration with product developers providing in-depth analysis and recommendations
- Test lab to be accredited (e.g. Wurldtech)

Project lifecycle – design / solution hardening
Electronic perimeter protection and defense in depth

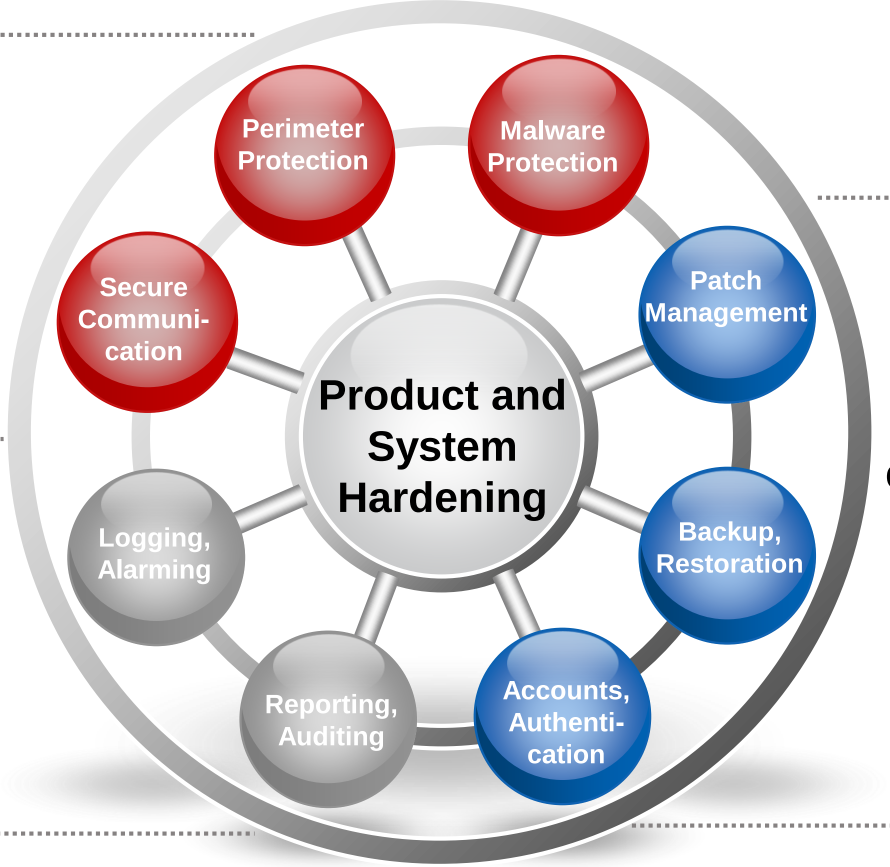


Protecting

against threats to substation automation systems

Monitoring

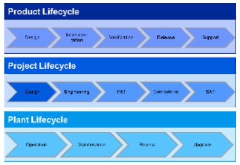
security and health activities in real-time

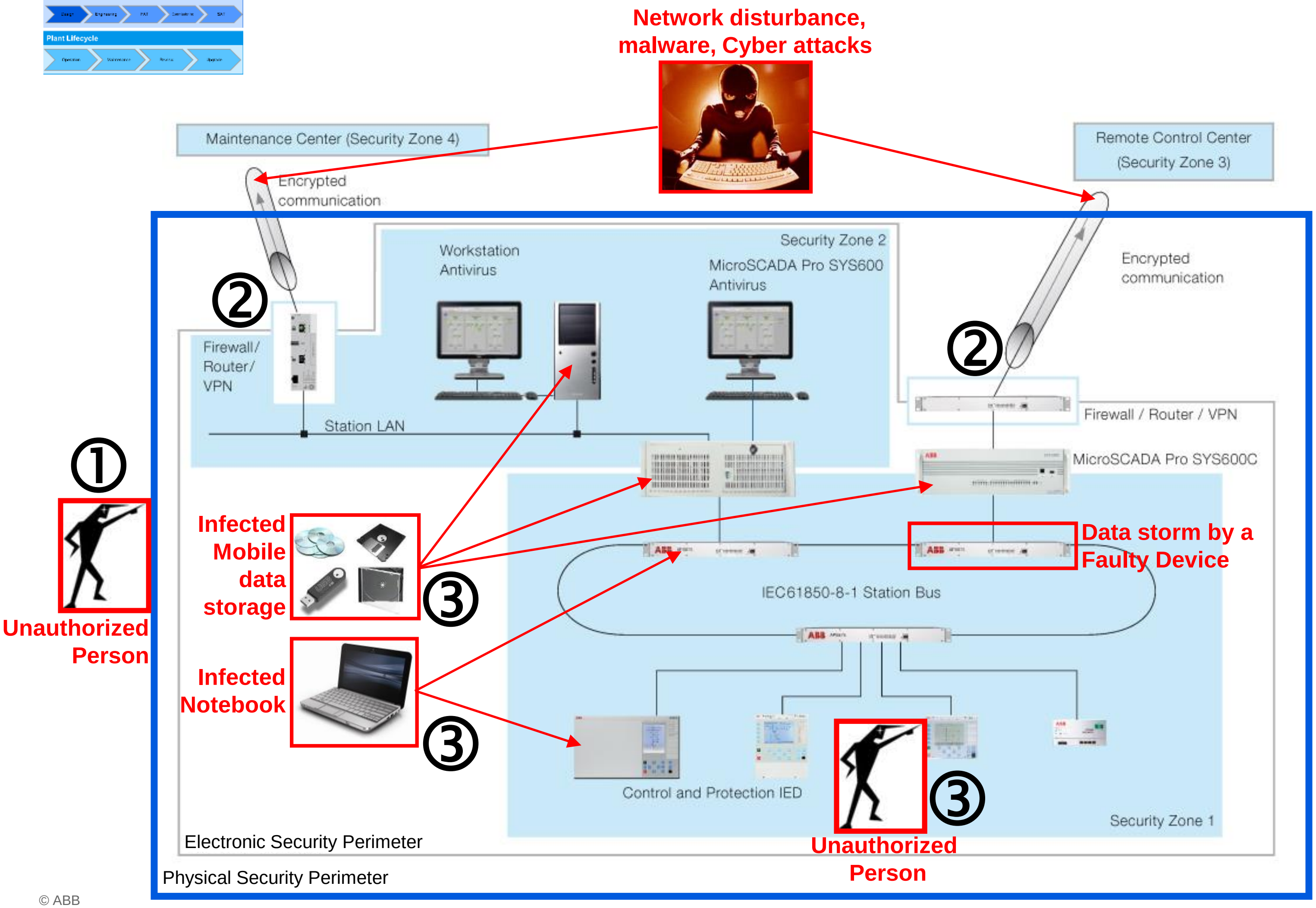


Managing

critical activities, such as configurations, changes and patches

Project lifecycle – design / system architecture
Understanding cyber security / robustness threats




Network disturbance, malware, Cyber attacks
Maintenance Center (Security Zone 4)
Encrypted communication
Remote Control Center (Security Zone 3)
Encrypted communication
②
Firewall/ Router/ VPN
Workstation Antivirus
Security Zone 2
MicroSCADA Pro SYS600 Antivirus
②
Station LAN
Firewall / Router / VPN
MicroSCADA Pro SYS600C
①
Unauthorized Person
Infected Mobile data storage
③
Data storm by a Faulty Device
IEC61850-8-1 Station Bus
Infected Notebook
③
Control and Protection IED
③
Unauthorized Person
Security Zone 1
Electronic Security Perimeter
Physical Security Perimeter

Security measures

① Physical perimeter protection

② Electronic perimeter protection

③ Defense in depth

Cyber Security for Substation Automation
Cyber security on system level

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

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 features in station level products

Introduction

Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

Cyber security requirements need to be addressed both on system as well as on product level.

Station-level products such as 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

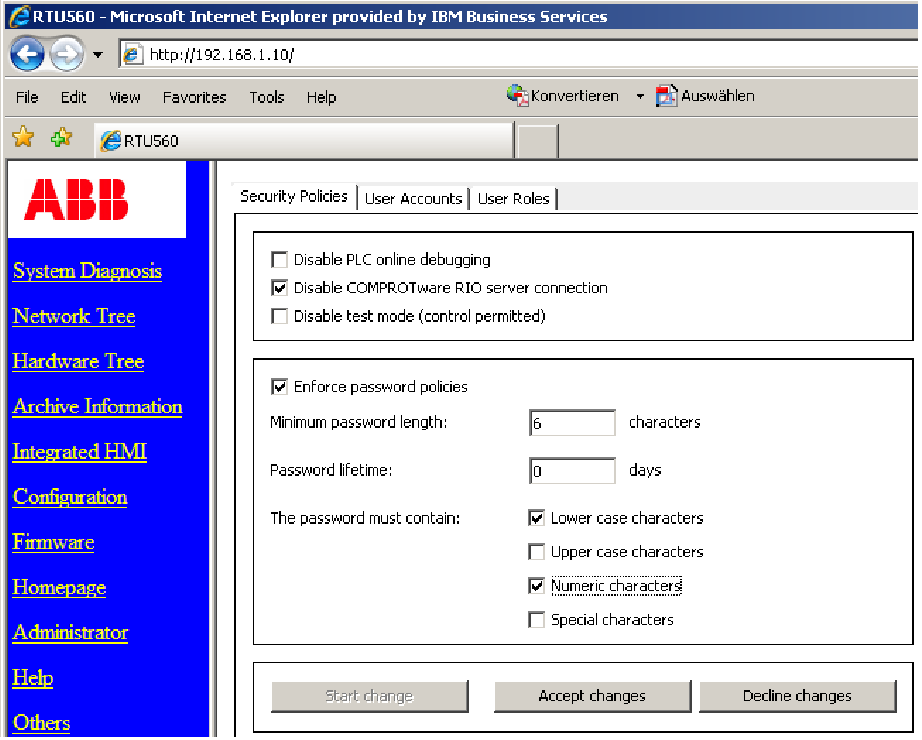
Cyber Security for Substation Automation
Cyber security features in station level products

- Introduction
- Main drivers
- Discussion of risk
- Challenges
- **Solution approaches**
- Conclusions

Overview of security features

- Individual user accounts
- Role based access control
- Enforced password policies
- Session management
- Detailed audit trails
- Secure remote management connectic…
- 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

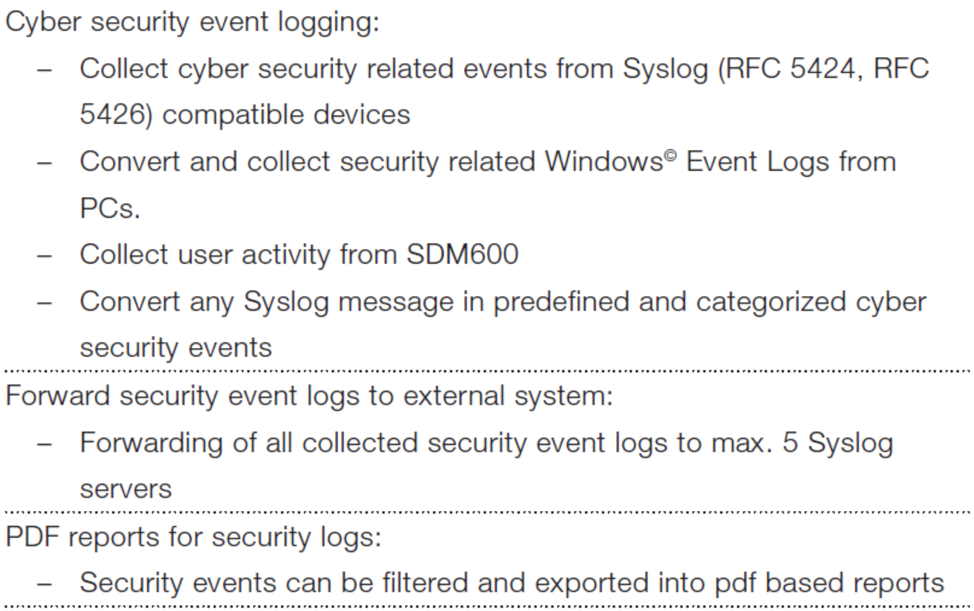
The password must contain:
☑ Lower case characters
□ Upper case characters
☑ Numeric characters
□ Special characters

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
Cyber Security – Network Access Control

- Central Role Based User Account (RBAC) Management for devices supporting:
  - IEC 62351-8 (Pull Model, Profile A)
  - All standard IEC 62351-8 roles supported
  - RADIUS (RFC 2865) devices
  - Windows Pc's
- Efficient configuration of new users
- Assignment of roles per user
- New users can be notified by email



Cyber security event logging:

- Collect cyber security related events from Syslog (RFC 5424, RFC 5426) compatible devices
- Convert and collect security related Windows© Event Logs from PCs.
- Collect user activity from SDM600
- Convert any Syslog message in predefined and categorized cyber security events

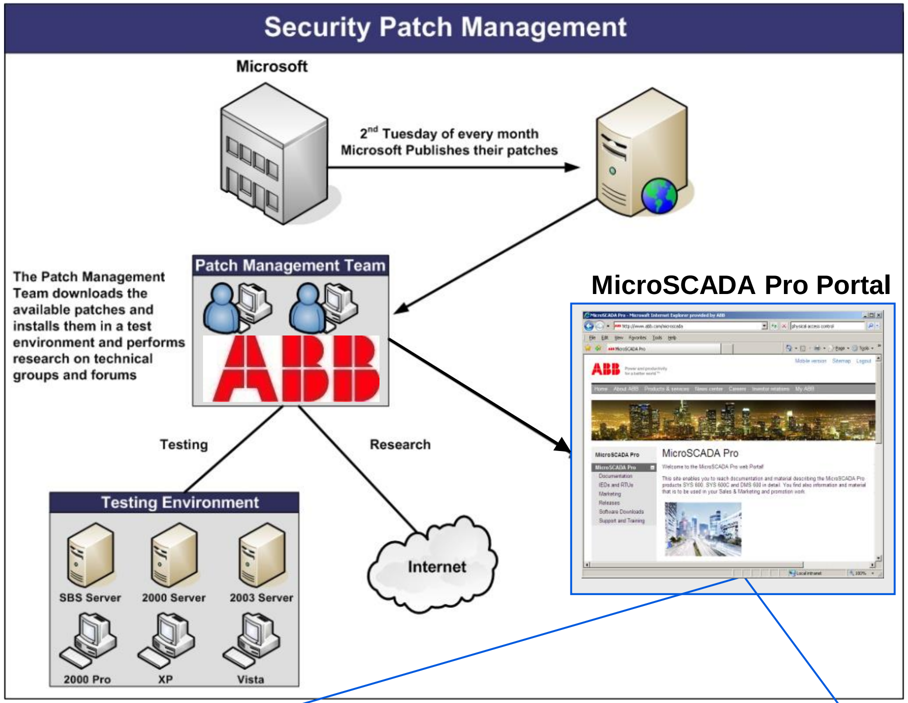
Forward security event logs to external system:

- Forwarding of all collected security event logs to max. 5 Syslog servers

PDF reports for security logs:

- Security events can be filtered and exported into pdf based reports

Cyber Security for Substation Automation
Security patch verification


Security Patch Management
Microsoft
2nd Tuesday of every month
Microsoft Publishes their patches
Patch Management Team
The Patch Management Team downloads the available patches and installs them in a test environment and performs research on technical groups and forums
MicroSCADA Pro Portal
MicroSCADA Pro
Welcome to the MicroSCADA Pro web Portal
Testing
Research
Testing Environment
SBS Server
2000 Server
2003 Server
2000 Pro
XP
Vista
Internet

Patch Compatibility Report

Microsoft

Security Bulletin	Comp. Status	Remarks	Windows XP	Windows 7	Windows Server 2003	Windows Server 2008	Windows Server 2008 R2
March 2011							
MS11-015	Q		x	x			x
MS11-016	N/A		-	-	-	-	-
MS11-017	Q		x	x	x	x	x
Restart required?	May need						

- Device Security Assurance Center (DSAC)
- Benefit
  - Reduce risk of vulnerability for windows based system components
- Features
  - Monthly security patch verification of software used as part of substation automation system
  - Computers are delivered with latest patches installed
- References
  - MicroSCADA Pro patch compatibility report

Defense in depth

Introduction

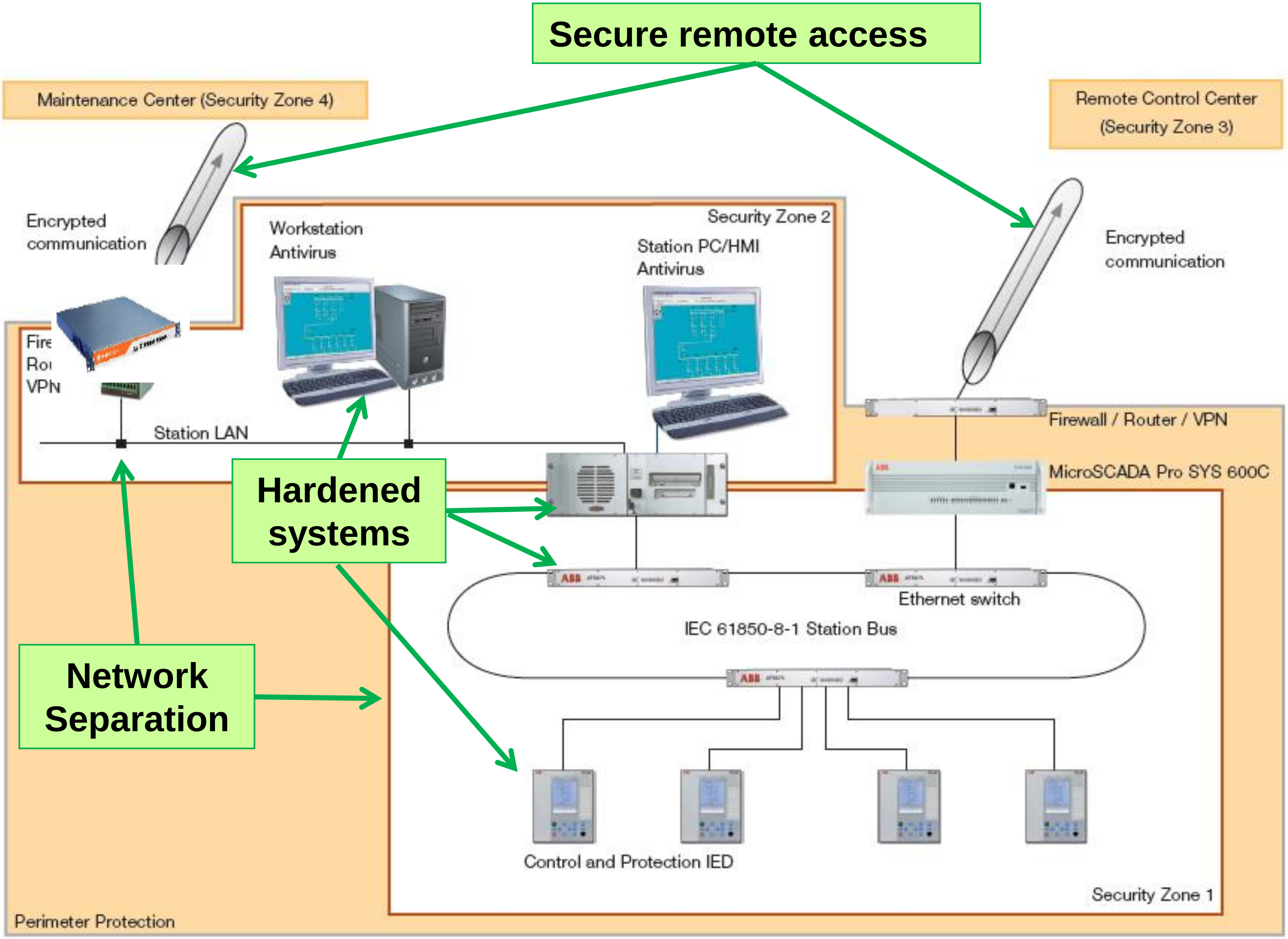
Main drivers

Discussion of risk

Challenges

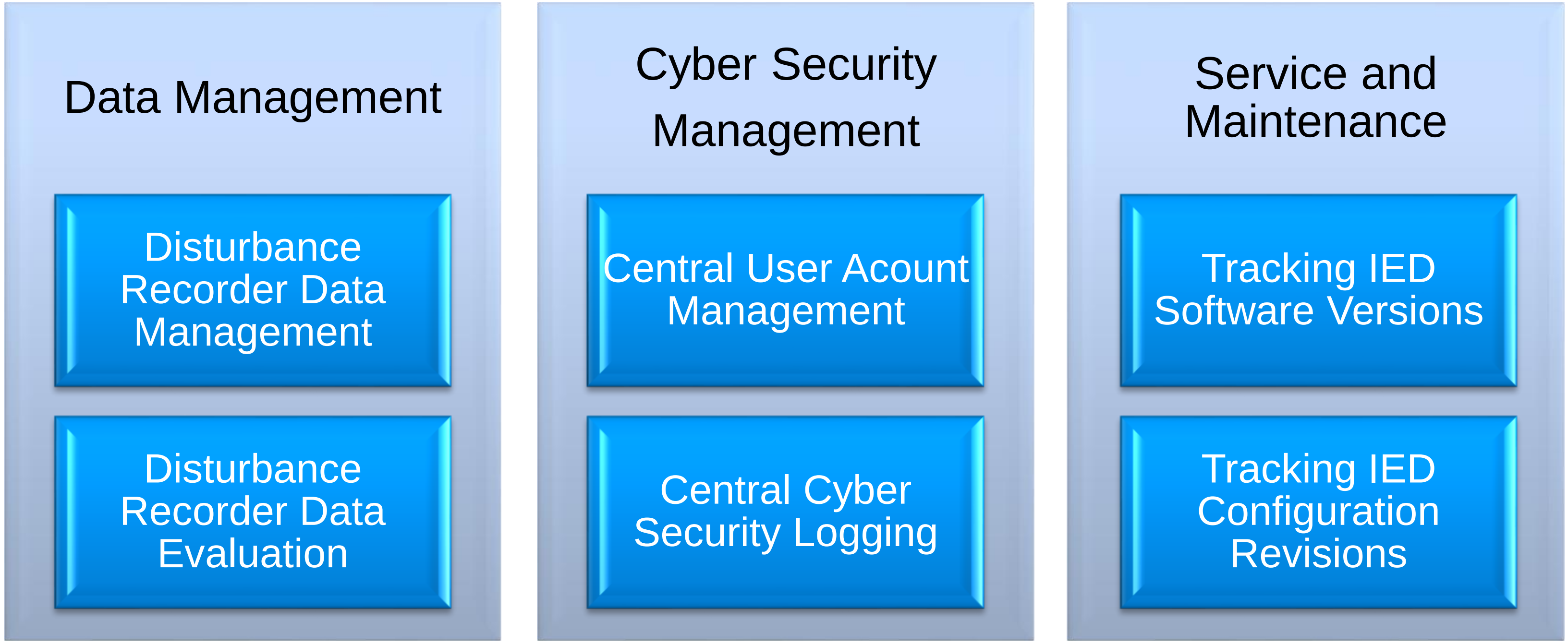
Solution approaches

Conclusions



Cyber Security for Substation Automation

System Data Monitor based Cyber security – System wide



Data Management

Disturbance Recorder Data Management

Disturbance Recorder Data Evaluation

Cyber Security Management

Central User Acount Management

Central Cyber Security Logging

Service and Maintenance

Tracking IED Software Versions

Tracking IED Configuration Revisions

Automatically collect, store and provide evaluation for disturbance recorder files.

Provide centralized User Account Management and security logging

Documentation of Firmware and configuration revisions of the supervised IEC 61850 IEDs

Cyber Security for Substation Automation
Cyber Security – Inventory Management

Introduction

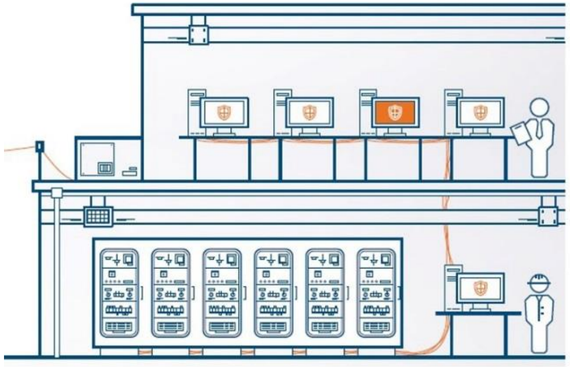
Main drivers

Discussion of risk

Challenges

Solution approaches

Conclusions

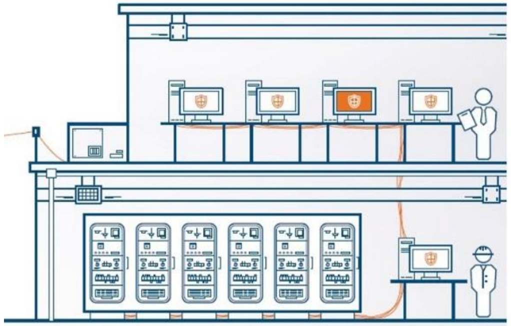


Collect service data

- Reading of service relevant data from supervised IEC 61850 IEDs
- Monitor deployed IED software versions and serial numbers*
- Track IED firmware versions
- Track IEC 61850 configuration revision information

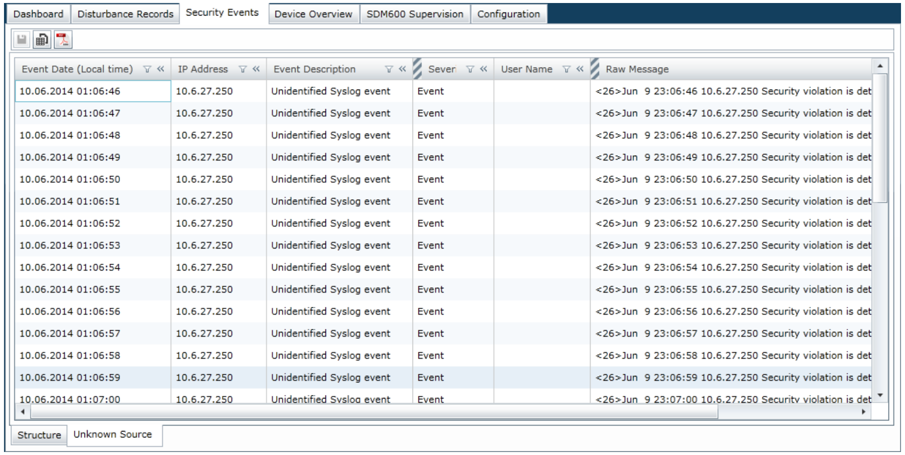
- Monitor deployed IED software versions
- Monitor Serial numbers if Provided by respective IED 9 ABB IED's provide this optional information)

Cyber Security for Substation Automation
Cyber Security – Configuration Change



Collect service data

- Reading of service relevant data from supervised IEC 61850 IEDs
- Monitor deployed IED software versions and serial numbers*
- Track IED firmware versions
- Track IEC 61850 configuration revision information



Event Date (Local time)	IP Address	Event Description	Sever	User Name	Raw Message
10.06.2014 01:06:46	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:46 10.6.27.250 Security violation is det
10.06.2014 01:06:47	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:47 10.6.27.250 Security violation is det
10.06.2014 01:06:48	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:48 10.6.27.250 Security violation is det
10.06.2014 01:06:49	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:49 10.6.27.250 Security violation is det
10.06.2014 01:06:50	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:50 10.6.27.250 Security violation is det
10.06.2014 01:06:51	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:51 10.6.27.250 Security violation is det
10.06.2014 01:06:52	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:52 10.6.27.250 Security violation is det
10.06.2014 01:06:53	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:53 10.6.27.250 Security violation is det
10.06.2014 01:06:54	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:54 10.6.27.250 Security violation is det
10.06.2014 01:06:55	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:55 10.6.27.250 Security violation is det
10.06.2014 01:06:56	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:56 10.6.27.250 Security violation is det
10.06.2014 01:06:57	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:57 10.6.27.250 Security violation is det
10.06.2014 01:06:58	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:58 10.6.27.250 Security violation is det
10.06.2014 01:06:59	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:06:59 10.6.27.250 Security violation is det
10.06.2014 01:07:00	10.6.27.250	Unidentified Syslog event	Event		<26>Jun 9 23:07:00 10.6.27.250 Security violation is det

System Data Manager

- Tracks IEC 61850 configuration revision information
- Managing service relevant data from IEDs:
  - IEC 61850 based IEDs (Ed.1 and Ed.2)
  - Reading all attributes from LLN0 and LPHD Logical Node
  - Tracking changes in the dashboard

Cyber Security for Substation Automation
User Activity and configuration changes

Introduction

Main drivers

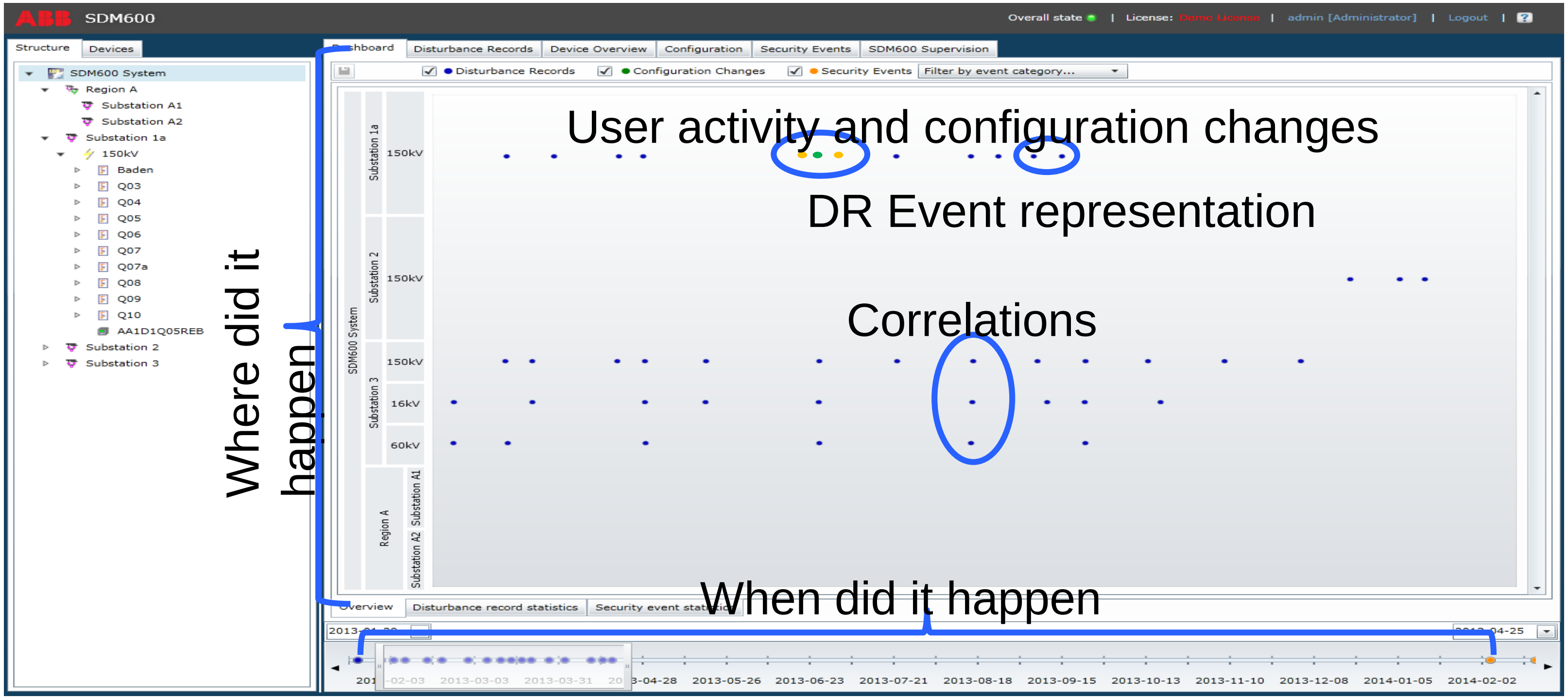
Discussion of risk

Challenges

Solution approaches

Conclusions

- System Data Manager – dashboard to consolidate all system events
- Cyber security event logging:
  - Collect cyber security related events from Syslog (RFC 5424, RFC 5426) compatible devices
  - Convert and collect security related Windows© Event Logs from PC's
  - Collect user activity from SDM600
  - Convert any Syslog message in predefined and categorized cyber security events



User activity and configuration changes

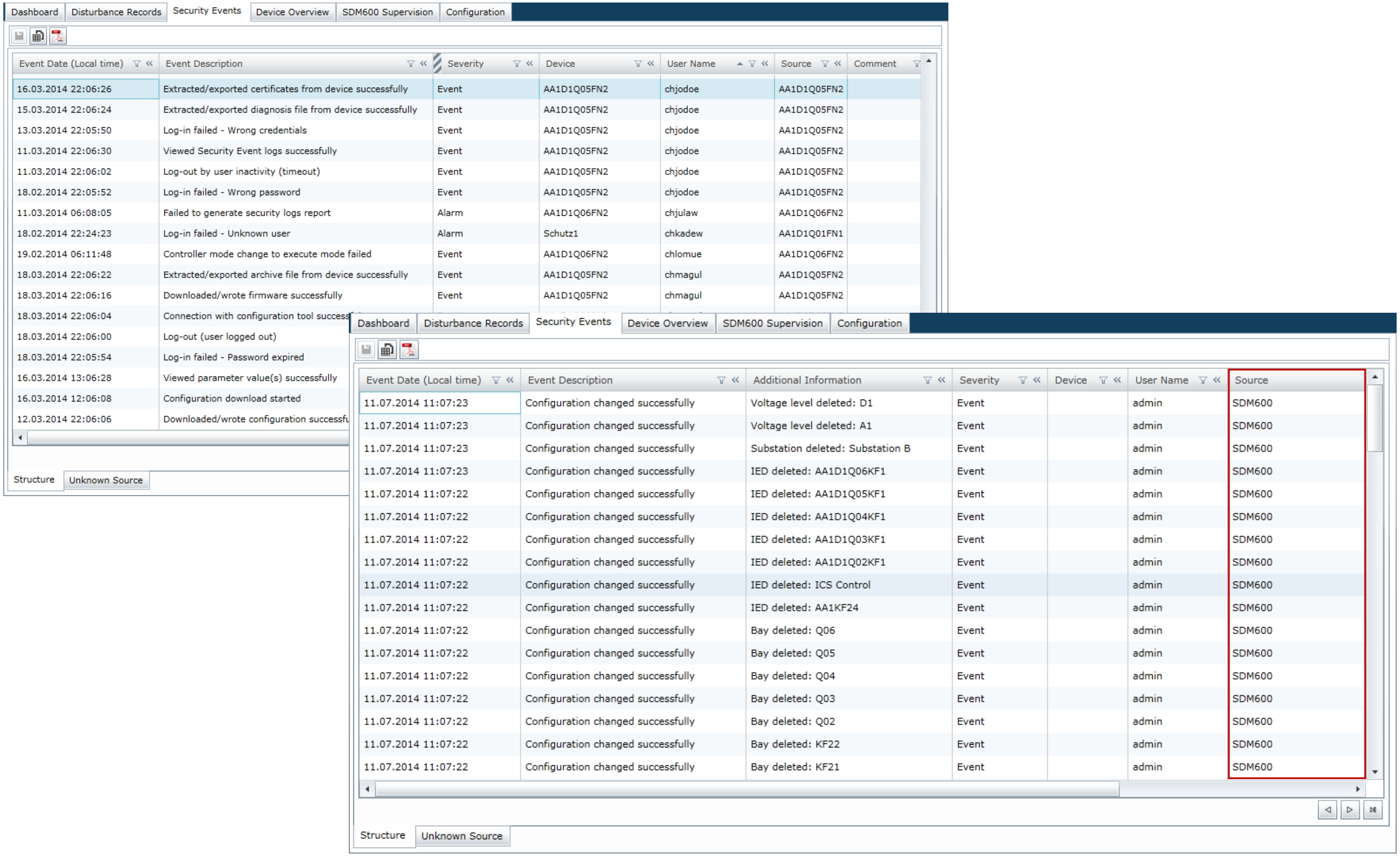
DR Event representation

Correlations

Where did it happen

When did it happen

Cyber Security for Substation Automation
Cyber Security – Alarm overview



Event Date (Local time)	Event Description	Severity	Device	User Name	Source	Comment
16.03.2014 22:06:26	Extracted/exported certificates from device successfully	Event	AA1D1Q05FN2	chjodoe	AA1D1Q05FN2	
15.03.2014 22:06:24	Extracted/exported diagnosis file from device successfully	Event	AA1D1Q05FN2	chjodoe	AA1D1Q05FN2	
13.03.2014 22:05:50	Log-in failed - Wrong credentials	Event	AA1D1Q05FN2	chjodoe	AA1D1Q05FN2	
11.03.2014 22:06:30	Viewed Security Event logs successfully	Event	AA1D1Q05FN2	chjodoe	AA1D1Q05FN2	
11.03.2014 22:06:02	Log-out by user inactivity (timeout)	Event	AA1D1Q05FN2	chjodoe	AA1D1Q05FN2	
18.02.2014 22:05:52	Log-in failed - Wrong password	Event	AA1D1Q05FN2	chjodoe	AA1D1Q05FN2	
11.03.2014 06:08:05	Failed to generate security logs report	Alarm	AA1D1Q06FN2	chjulaw	AA1D1Q06FN2	
18.02.2014 22:24:23	Log-in failed - Unknown user	Alarm	Schutz1	chkadew	AA1D1Q01FN1	
19.02.2014 06:11:48	Controller mode change to execute mode failed	Event	AA1D1Q06FN2	chlomue	AA1D1Q06FN2	
18.03.2014 22:06:22	Extracted/exported archive file from device successfully	Event	AA1D1Q05FN2	chmagul	AA1D1Q05FN2	
18.03.2014 22:06:16	Downloaded/wrote firmware successfully	Event	AA1D1Q05FN2	chmagul	AA1D1Q05FN2	
18.03.2014 22:06:04	Connection with configuration tool success					
18.03.2014 22:06:00	Log-out (user logged out)					
18.03.2014 22:05:54	Log-in failed - Password expired					
16.03.2014 13:06:28	Viewed parameter value(s) successfully					
16.03.2014 12:06:08	Configuration download started					
12.03.2014 22:06:06	Downloaded/wrote configuration successfu					

Event Date (Local time)	Event Description	Additional Information	Severity	Device	User Name	Source
11.07.2014 11:07:23	Configuration changed successfully	Voltage level deleted: D1	Event		admin	SDM600
11.07.2014 11:07:23	Configuration changed successfully	Voltage level deleted: A1	Event		admin	SDM600
11.07.2014 11:07:23	Configuration changed successfully	Substation deleted: Substation B	Event		admin	SDM600
11.07.2014 11:07:23	Configuration changed successfully	IED deleted: AA1D1Q06KF1	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	IED deleted: AA1D1Q05KF1	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	IED deleted: AA1D1Q04KF1	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	IED deleted: AA1D1Q03KF1	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	IED deleted: AA1D1Q02KF1	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	IED deleted: ICS Control	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	IED deleted: AA1KF24	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	Bay deleted: Q06	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	Bay deleted: Q05	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	Bay deleted: Q04	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	Bay deleted: Q03	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	Bay deleted: Q02	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	Bay deleted: KF22	Event		admin	SDM600
11.07.2014 11:07:22	Configuration changed successfully	Bay deleted: KF21	Event		admin	SDM600

Trends & Conclusions

Trends

- Introduction
- Main drivers
- Discussion of risk
- Challenges
- Solution approaches
- **Conclusions**

	Today	Trend
Regulation & Government initiatives	NERC CIP regulation for securing Bulk Electric System 🇺🇸🇨🇦	Additional security regulations expected for Smart Grid and will cover all voltage level 🇺🇸🇨🇦 Government organizations increase attention to securing critical infrastructure 🌍
Application focus	DCS, EMS, SCADA 🇺🇸🇨🇦	Focus on end-to-end security 🌍
Business aspects	Smart Grid stimulus funding tied to sound security approach 🇺🇸🇨🇦 Avoiding fines associated with non-compliance (end-users)	Reduction of risk (for both end-users and vendors) 🌍

Early CIP Committee position on Ethernet

- NERC CIP Committee Questions to Vendor Panel (Dec 2007):

"IEC 61850 (Ethernet based) is wide open communication that does not comply with CIP standards.

There are manufacturers planning to connect substation equipment together using control IED's connected with 61850. How will the 61850 substation of the future maintain compliance?"

"[We] have determined the best approach for our substation control IED's is to use [non-routable] serial communication

This removes the need for IP in the substation connected to control IED's, thus keeping the six walls of protection in the control and communication centers. [We] will only purchase control IED's that maintain the secure communication to maintain compliance. What are the manufacturers hearing from other customers with regards to serial or IP communication? Will all of the functions provided via IP communication be available using serial communications? Will serial interfaces continue to be provided for the foreseeable future?"

"R" in NERC stands for Reliability! Preventing real-time outflow of substation information will only be detrimental to the overall Grid Performance and Reliability

Grid Reliability - Intelligent Transmission Operations

Introduction

Main drivers

Discussion of risk

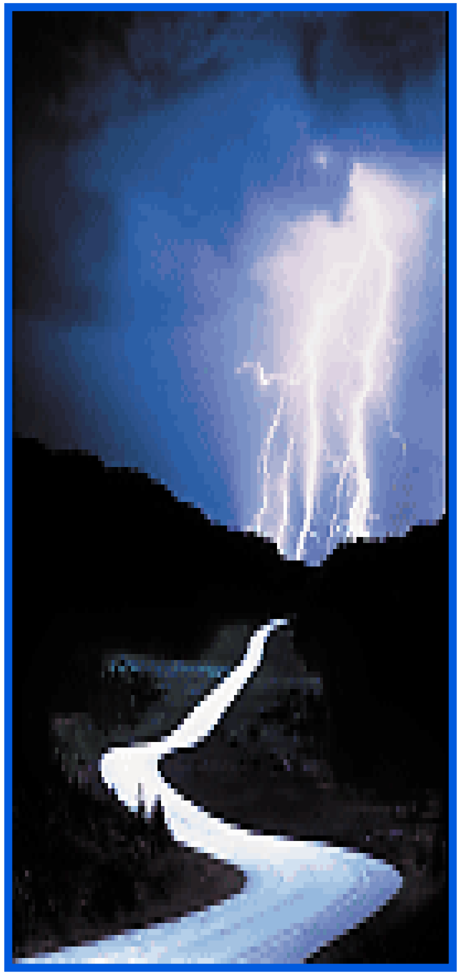
Challenges

Solution approaches

Conclusions

Power system functions and transmission operations requiring ultra high speed communications for monitoring and rapid response control

- Focus on Wide-Area Measurement and Control Systems
  - Automated Control Systems
  - Emergency Operations
  - Transmission System Contingency Analysis and Planning
  - Wide Area Monitoring and Control Advanced Auto Restoration
  - Power System Oscillation Damping
  - System-wide Automatic Voltage Control
  - Synchro-Phasor Applications
  - Self-Healing Grid (across both transmission and distribution)



Source Intelligrid Website: http://intelligrid.info/

Conclusions

Security is **not just a matter of technology**, it is primarily about people, relationships, organizations and processes working in tandem to prevent an attack

Effective security solutions require a **joint effort** by vendors, integrators, operating system providers and end users.

There is **no single solution** that is effective for all organizations and applications.

Security is a continuous process, not a product or a one-time investment

Security must be addressed with **multiple barriers** and requires both **protection** and **detection** mechanisms

Security is about risk management - perfect security is neither existent nor economically feasible

Thank you for your participation

Shortly, you will receive a link to an archive of this presentation.

To view a schedule of remaining webinars in this series, or for more information on ABB’s protection and control solutions, visit:

www.abb.com/relion

Power and productivity
for a better world™

ABB

NERC CIP release history

Effective Date	NERC CIP Version
July 1, 2008	Version 1
April 1, 2010	Version 2
October 1, 2010	Version 3
April 1, 2014	Version 4 (Now retired)
April 1, 2016	Version 5 (High & Medium)
April 1, 2017	Version 5/6 (Predicted)