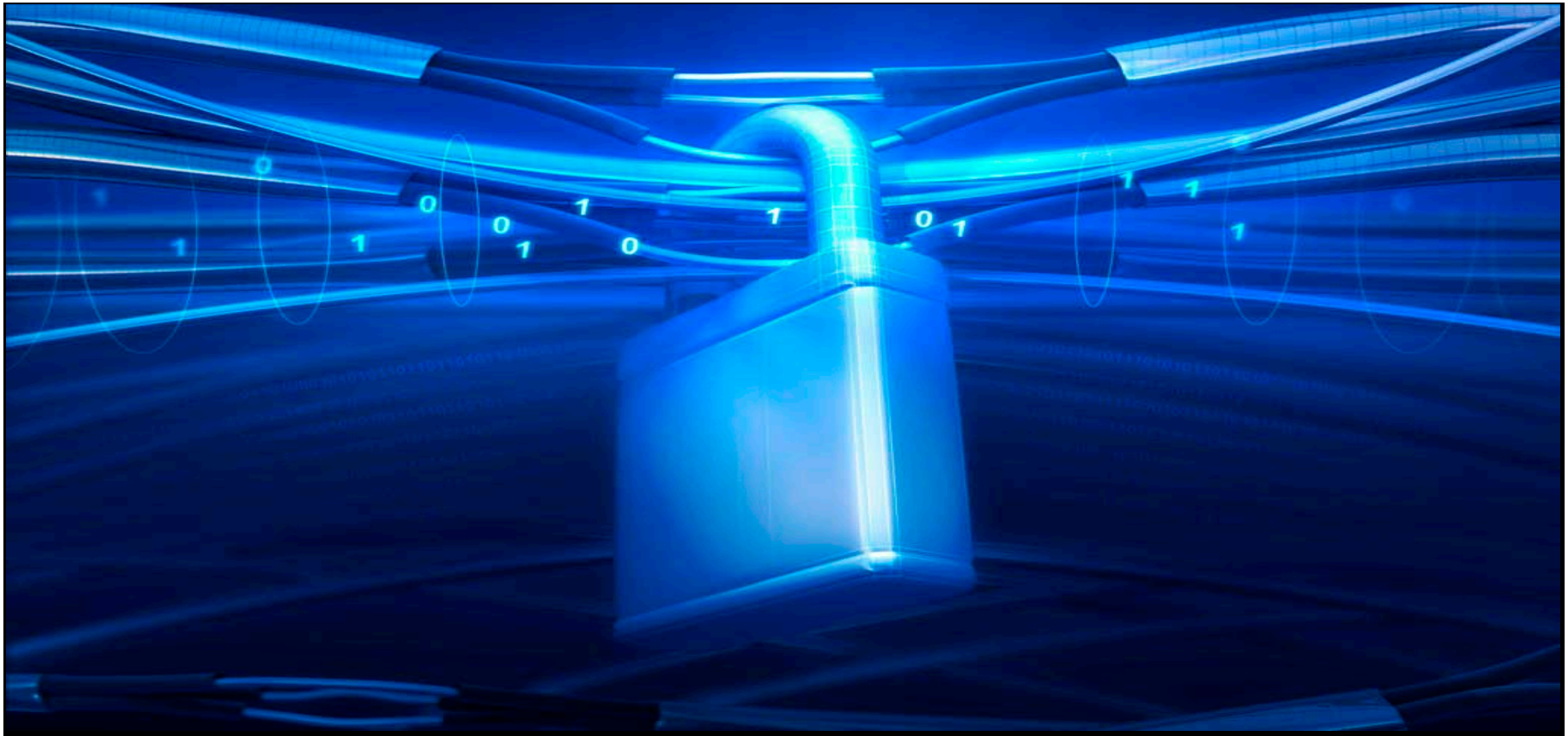


March 25-27, 2014 Steven A. Kunsman

i-PCGRID Workshop 2015
Cyber Security for Substation Automation
The Jagged Line between Utility and Vendors

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

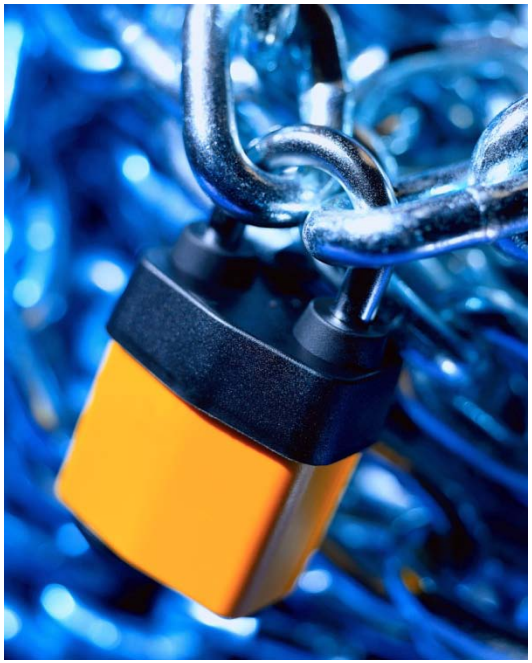
Cyber security has become an issue **by introducing Ethernet (TCP/IP) based communication protocols** to industrial automation and control systems. e.g. IEC60870-5-104, DNP 3.0 via TCP/IP or IEC61850

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

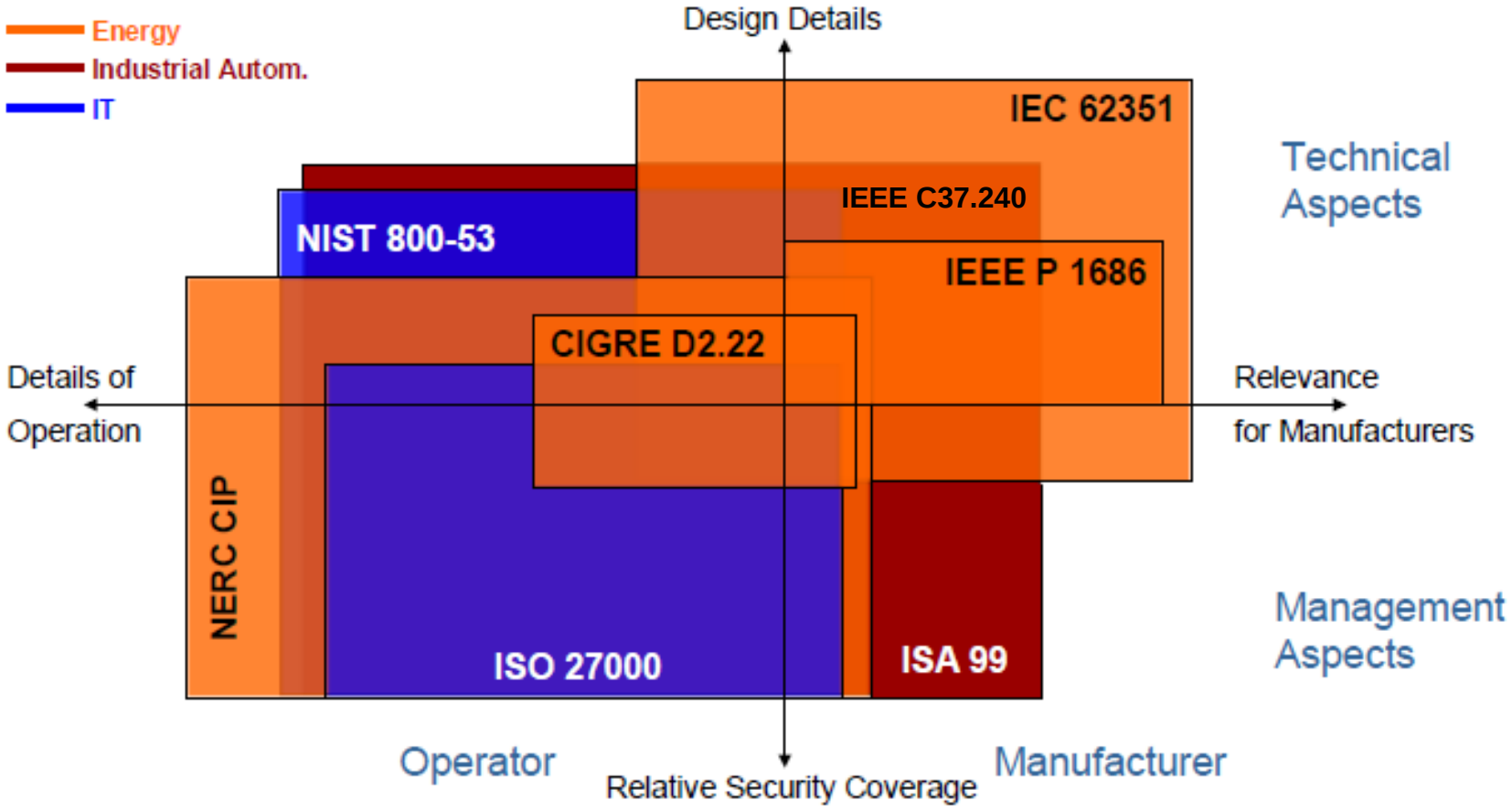
Utilities need to avoid penalties due to non-compliance with regulatory directives or industry best practices

Cyber Security for Substation Automation
Back to the basics



- Security is about awareness, policy and process
- Ignore compliance - at least at first
  - Focus on risk mitigation and management
  - Assess your maturity model and then improve
- There is no such thing as 100% security
  - Actors and threats constantly changing
- Deploy Defense in Depth
  - Deter, Detect and Delay the bad guys
- Security does not come for free

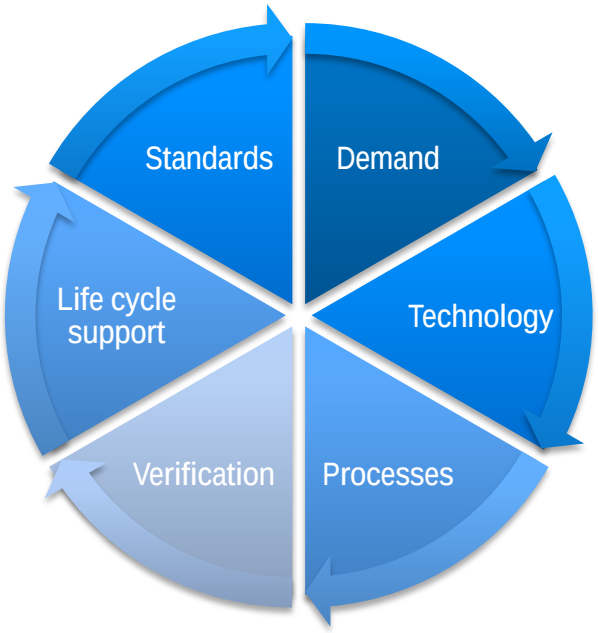
Cyber Security for Substation Automation
Standards and scope



Representation of scope and completeness of selected standards

Source DTS IEC 62351-10 : Security architecture guidelines

Cyber security initiatives
Security organization & institutionalization

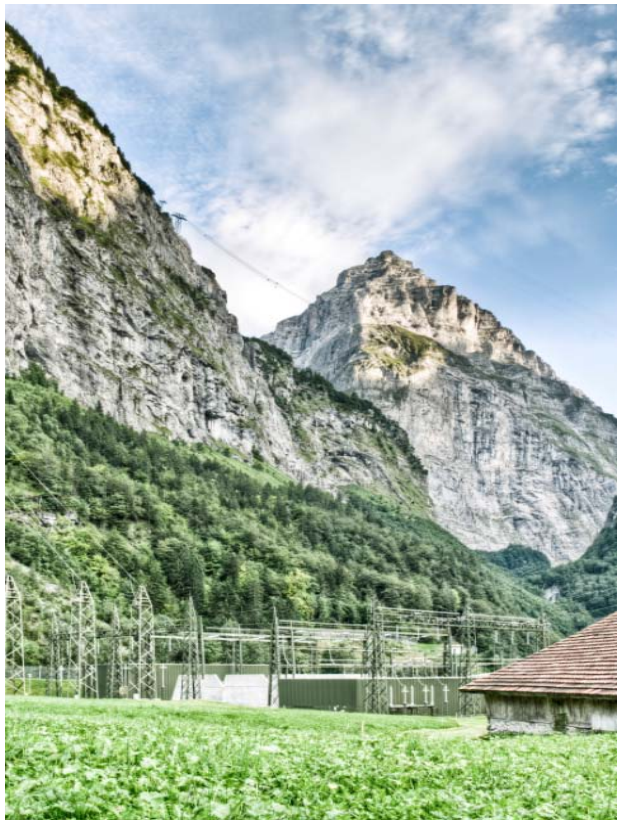


- Security Need
  - High level of security for products & solutions
  - Fast response and reliable partner in case of a cyber security incident
- Vendor responsibility
  - Cross-functional cyber security organization
    - Institutionalize security culture
    - Active participation in security standards
  - Established security processes
    - Security assessment in R&D
    - Security baked into the technology
    - Robustness and validation testing
    - Patch management process

Device Security Assurance Center (DSAC)
Product and System Hardening

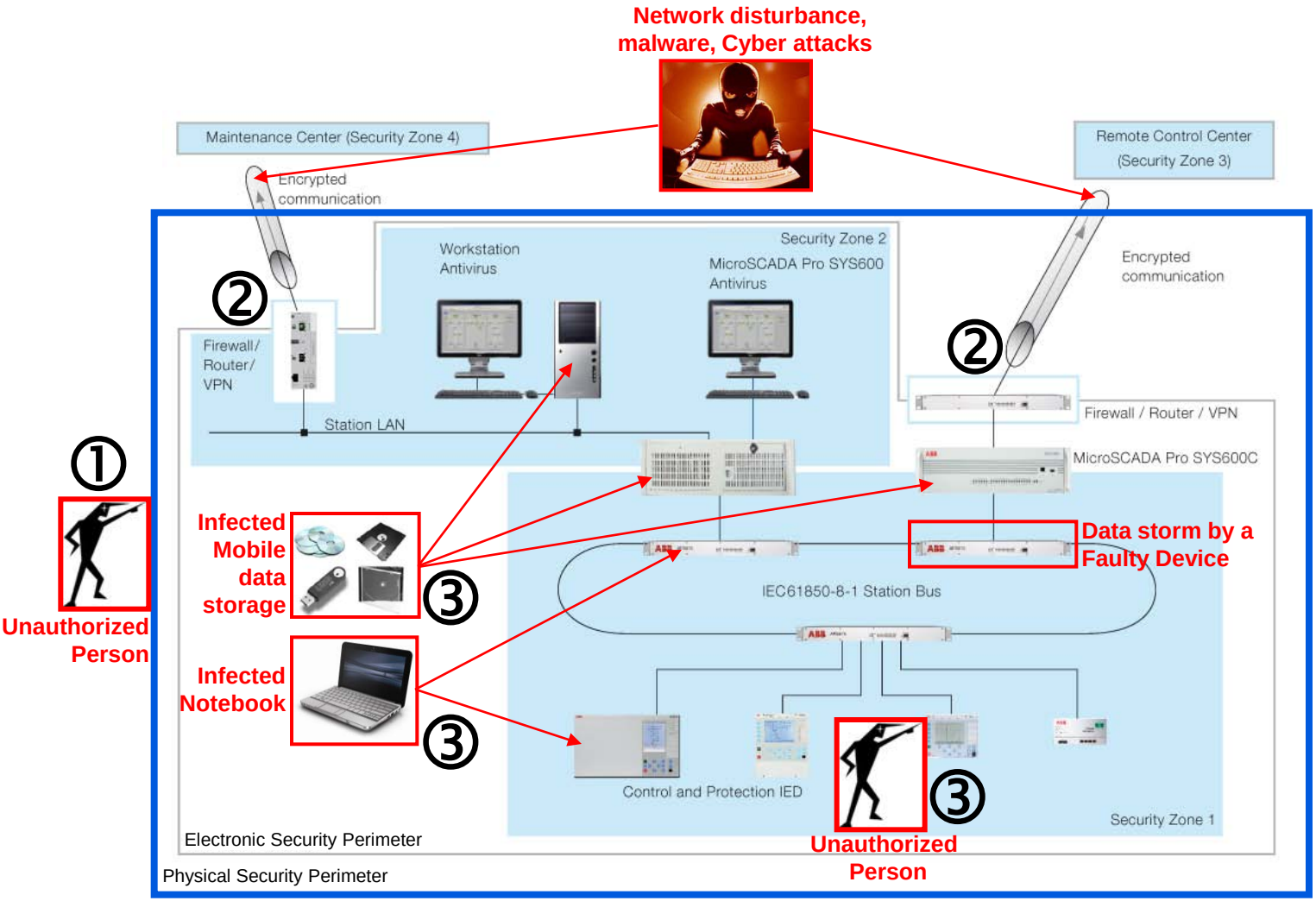
- Security Need
  - Robust and reliable products and solutions
- Vendor Responsibility
  - Security testing center guarantees a common and best practice robustness testing
  - Continuous regression tests on products and systems ensuring a high level of robustness against cyber security attacks

Protect
Is my system protected against an attack?



- Security Needs
  - Ensure reliable system operation (availability and performance)
- Utility Responsibility
  - Malware Protection: Prevent, detect, and remove malware, e.g. viruses, worm, …
  - Perimeter Protection: Restrict access by blocking / filtering inbound and outbound connections
  - Secure Communication: Encryption to prevent unauthorized users from reading and manipulating data

Protect
Cyber security and robustness threats



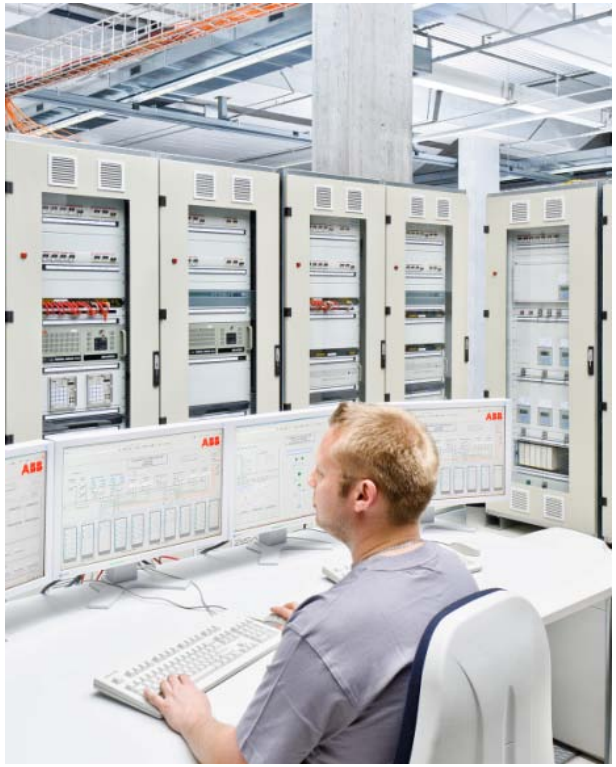
Security measures

① Physical perimeter protection

② Electronic perimeter protection

③ Defense in depth

Monitor
Do I know what happens on my system?



- Security Need
  - Alert about critical security alarms in real-time to enable fast corrective actions
- Utility Responsibility
  - Logging & Alarming: All security related events are recorded, sever events are alarmed to the remote center
  - Reporting & Auditing: Produce necessary data, reports and documentation for an audit

Monitor
Security events logging / Audit trail

Archive Information - Security Events

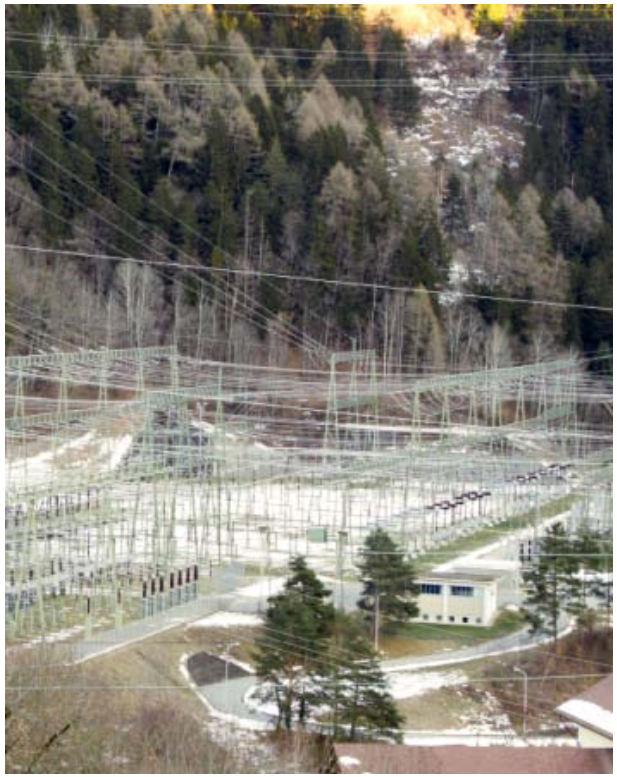
Max. entries: 961 Displayed entries: 912 - 961

Seq. No.	Date yy.mm.dd	Time hh:mm:ss.mss	Time invalid	User name	Event id	Severity	Source	Event text
912	10.03.30	14:35:56.655		JohnSmith	1320	Event	RTU560 Server AA1E1Q01A	Download configuration files succ
913	10.03.30	14:36:07.943		JohnSmith	1210	Event	RTU560 Server AA1E1Q01A	User logged out
914	10.03.30	14:36:30.353		TommyAtkins	1110	Event	RTU560 Server AA1E1Q01A	User log in successful
915	10.03.30	14:36:34.694		TommyAtkins	6110	Event	RTU560 Server AA1E1Q01A	Test mode started (control allowe
916	10.03.30	14:36:43.589		TommyAtkins	1210	Event	RTU560 Server AA1E1Q01A	User logged out
917	10.03.30	14:36:57.022		Admin	1110	Event	RTU560 Server AA1E1Q01A	User log in successful
918	10.03.30	14:37:00.268		Admin	1210	Event	RTU560 Server AA1E1Q01A	User logged out
919	10.03.30	14:37:00.840		JohnSmith	1110	Event	RTU560 Server AA1E1Q01A	User log in successful
920	10.03.30	14:37:40.191		JohnSmith	1210	Event	RTU560 Server AA1E1Q01A	User logged out
921	10.03.30	14:37:54.298		JohnSmith	1140	Event	RTU560 Server AA1E1Q01A	User log in failed - Wrong passwc
922	10.03.30	14:38:04.514		JohnSmith	1110	Event	RTU560 Server AA1E1Q01A	User log in successful
923	10.03.30	14:38:07.379		JohnSmith	1370	Event	RTU560 Server AA1E1Q01A	Viewed security event list succes
924	10.03.30	14:38:59.496		JohnSmith	1210	Event	RTU560 Server AA1E1Q01A	User logged out
925	10.03.30	14:39:13.010		JohnDoe	1120	Event	RTU560 Server AA1E1Q01A	User log in failed - Unknown user
926	10.03.30	14:39:29.138		MaryMajor	1110	Event	RTU560 Server AA1E1Q01A	User log in successful
927	10.03.30	14:39:51.517		MaryMajor	1210	Event	RTU560 Server AA1E1Q01A	User logged out
928	10.03.30	14:40:05.690		JohnSmith	1110	Event	RTU560 Server AA1E1Q01A	User log in successful
929	10.03.30	14:40:42.116		JohnSmith	1330	Event	RTU560 Server AA1E1Q01A	Upload configuration files succes
930	10.03.30	14:40:51.957		JohnSmith	1330	Event	RTU560 Server AA1E1Q01A	Upload configuration files succes
931	10.03.30	14:41:01.716		JohnSmith	1330	Event	RTU560 Server AA1E1Q01A	Upload configuration files succes
932	10.03.30	14:41:57.711		JohnSmith	6510	Event	RTU560 Server AA1E1Q01A	PLC debug mode started

```
Download configuration files succ
User logged out
User log in successful
Test mode started (control allowe
User logged out
User log in successful
User logged out
User log in successful
User logged out
User log in failed - Wrong passwc
```

- Security Need
  - Alert about critical security alarms in real-time to enable fast corrective actions
- Vendor Responsibility
  - Event logs are securely retained
  - Security event logs displayable via device tools
  - Ability disseminate security events to external security log clients using syslog

Manage
Can I sustain the security of my system?



- Security Need
  - Keep the security of the system up to date
- Utility Responsibility
  - Patch Management
    - Reduce risk of vulnerability for windows based system components
  - Backup & Restoration
    - Ensures complete data security and enables fast restoration in case of data loss /manipulation
  - Accounts & Authentication
    - Restrict access to intended users only, protected by high password complexity

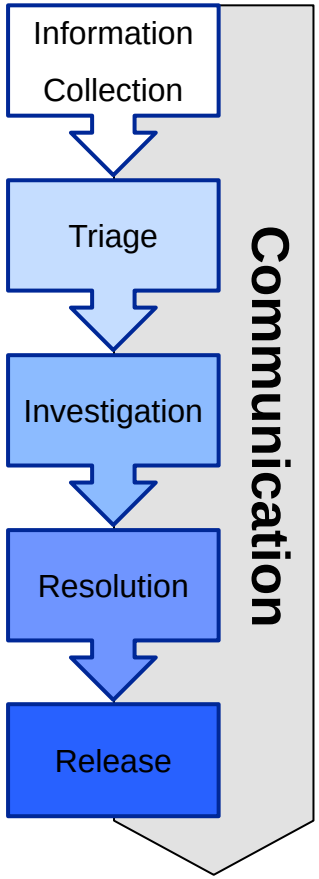
Manage
Vulnerability handling & Incident response

Minimize risk

Vendor Responsibility

- **Cultural change**: Accept that vulnerabilities exist (having a vulnerability is acceptable, improperly handling them is not!)
- Formal processes and policies
- Proper communication at the right time

Must establish a formal process and vulnerability resolution with urgency



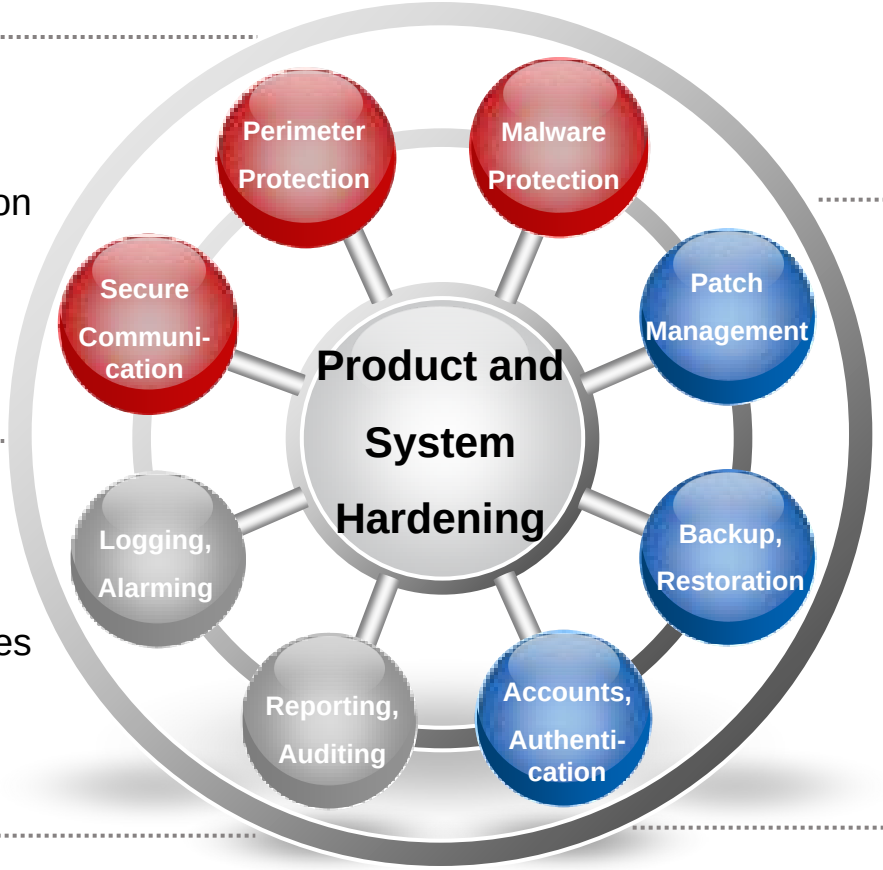
Cyber Security for Substation Automation
Summary

Protecting

against threats to substation automation systems

Monitoring

security and health activities in real-time



Managing

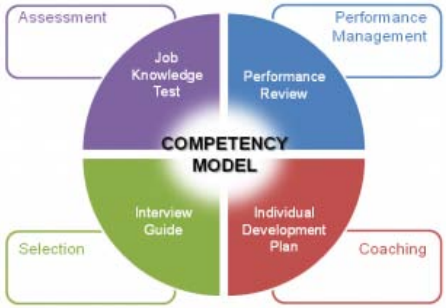
critical activities, such as configurations, changes and patches

The Challenges
Organizational

Risk Management

Awareness

Competence Management



Disruptive Changes

Images: www.guardianconsultants.co.uk wegilant.com www.floris-cm.nl blogpool4tool.com

Enterprise IT vs. Control Systems
A different set of challenges

	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
A definition *in the context of power and automation technology*

*Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack**

translates into

Measures taken to protect the reliability, integrity and availability of power and automation technologies against unauthorized access or attack

**Merriam-Webster's dictionary*

Wrap up

- Security is **not just a matter of technology**, it is primarily about people, relationships, organizations and processes working in tandem to prevent or recover from an attack
- Effective security solutions require a **joint effort** by vendors, integrators, operating system providers and utilities
- 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 **protection, deferral** and **detection** mechanisms
- **Security is about risk management** - perfect security is non existent nor economically feasible

Power and productivity
for a better world™