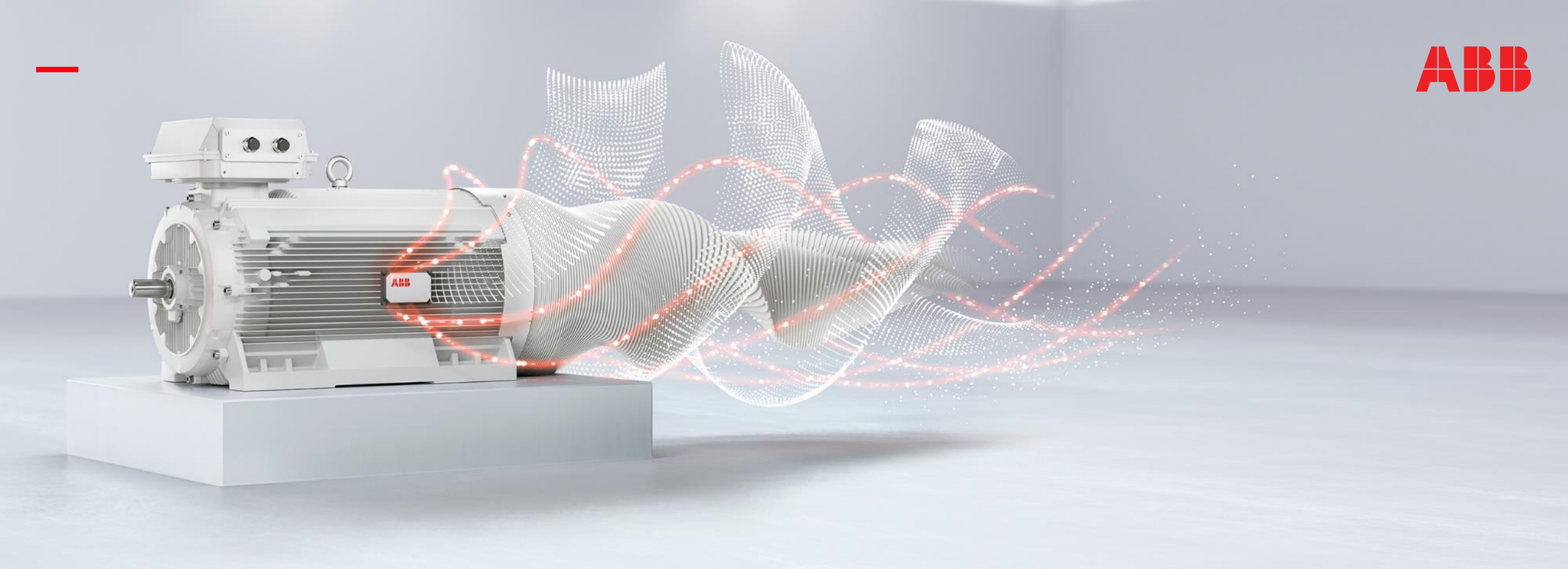


Industrial Control System (ICS) Security

Mohammad M R Chowdhury, 22 March 2017

About me

ABB OGC, ABB AS

ITS, UIO

UNIK 4740/0740

Thesis supervision

ABB CRC

UNIK/UIO

Telenor/GrameenPhone

UIO

HUT/
Aalto

ABB - at a glance

ABB – 125 Years of Innovation

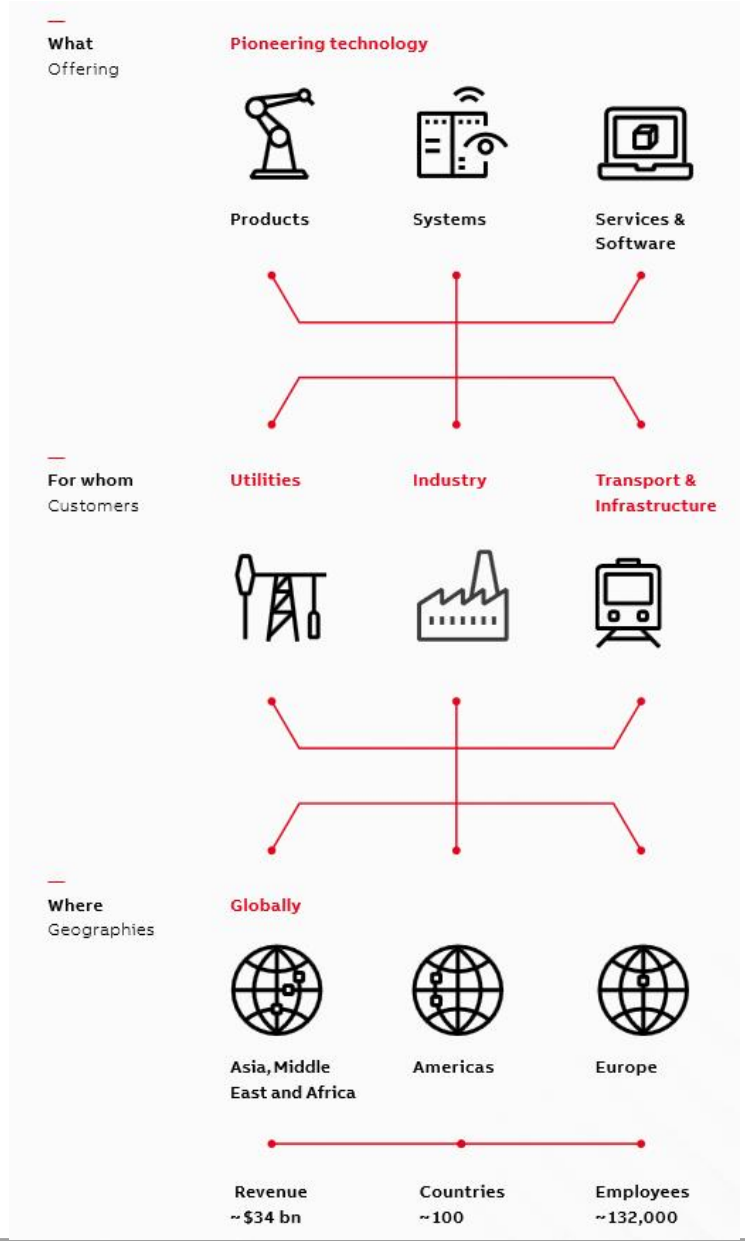


ABB IAOG - Oil, Gas and Chemicals

Four divisions:

Electrification Products

EP - divisjonsportal

EPMV - Mellomspenningsprodukter

Global portal

Robotics and Motion

RMRO - Robotics

Global portal

Industrial Automation

IAMP - Marine and Ports

IAOG - Oil, Gas and Chemicals

IATU - Turbocharging

Global portal

Power Grids

Global portal

Advanced Service And Products

>> Cyber Security and Infrastructure (~22 @ Oslo/Bergen/Czech)

IAOG major operation centers:

- Norway – Oslo, Bergen, Stavanger, Hammerfest
- US – Houston
- UK
- UAE
- Saudi Arabia

Customers:

- Aibel Norway
- ConocoPhillips
- ENI Norge
- ExxonMobil
- Engie E&P Norge AS
- Lundin
- Norske Shell
- Statoil Norway

Our work areas:

- System integration: Automation (ABB's system 800xA, Condition Monitoring, Power Management System)
- OGC products
- OGC Services

CSI scopes:

- Virtual and physical servers/clients
- Networks: Firewall/IDPS, Enterprise/Industrial Switches
- Acccess & Account Management
- System Hardening
- Centralized antimalware, patch management and backup solution
- SIEM
- Security Assessment
- Risk Assessments

Some projects

Johan Sverdrup

Aasta Hansteen

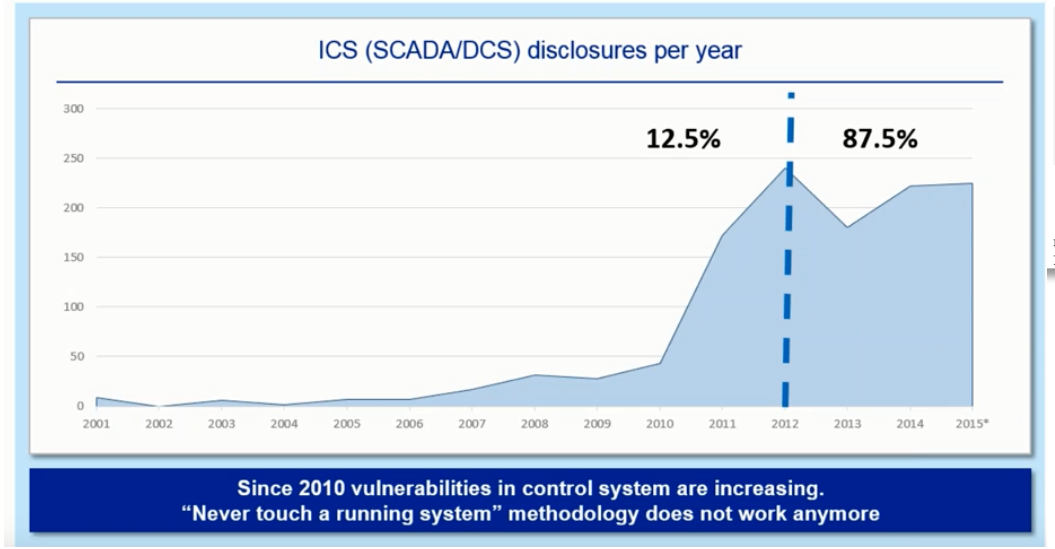
Valemon

Gina Krog

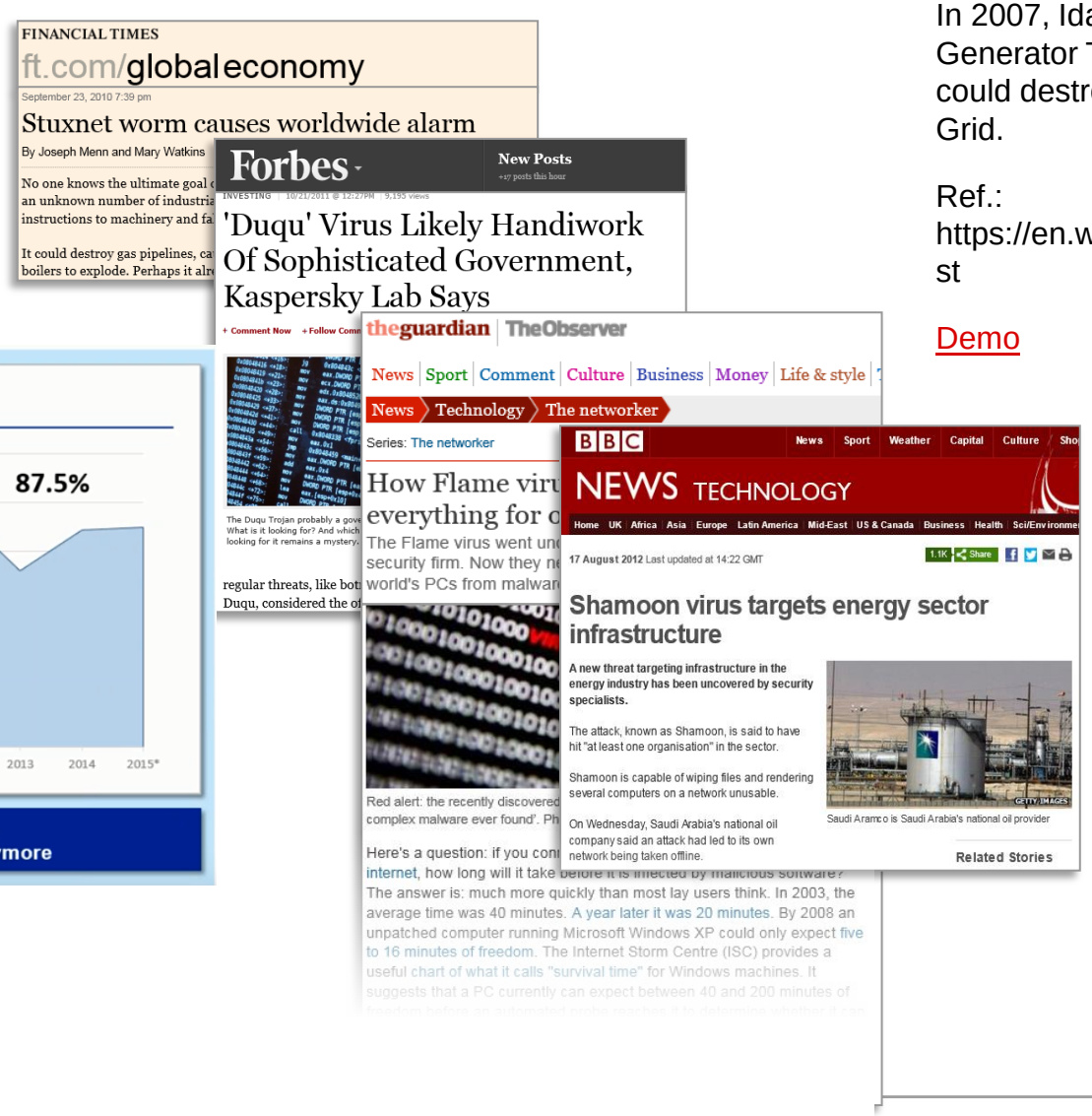
Goliat

Sadara

ICS Trends/Incidences



Source: https://scadahacker.com/



In 2007, Idaho National Laboratory ran the Aurora Generator Test to demonstrate how a cyber attack could destroy physical components of the electric Grid.

Ref.: https://en.wikipedia.org/wiki/Aurora_Generator_Test

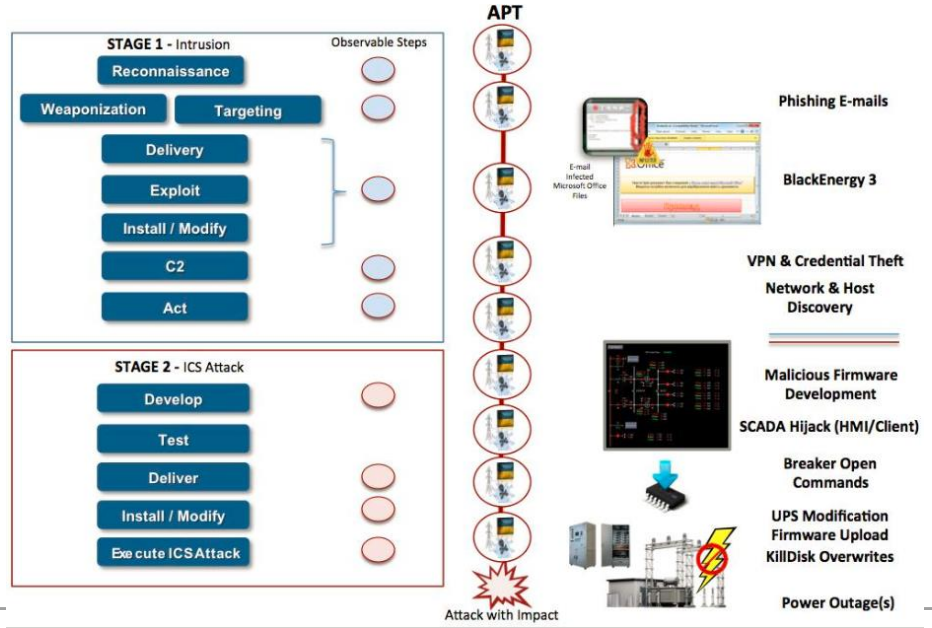
Demo

Electric Grids are Under Attacks!

Black Energy Attack

- November 2015
  - During the presidential election in Ukraine, BlackEnergy module killdisk infected several media agencies.
- December 2015
  - BlackEnergy 3 found in all of the three power plants in Ukraine have power outage

- Highly synchronized, multi-staged, multi-site attack
- Weaponized microsoft office doc embedding Blackenergy 3 malware, spread by phishing emails
- Open the doc > ask for enabling macro that drops malware component > is just the initial access
- Harvest > Take over the system

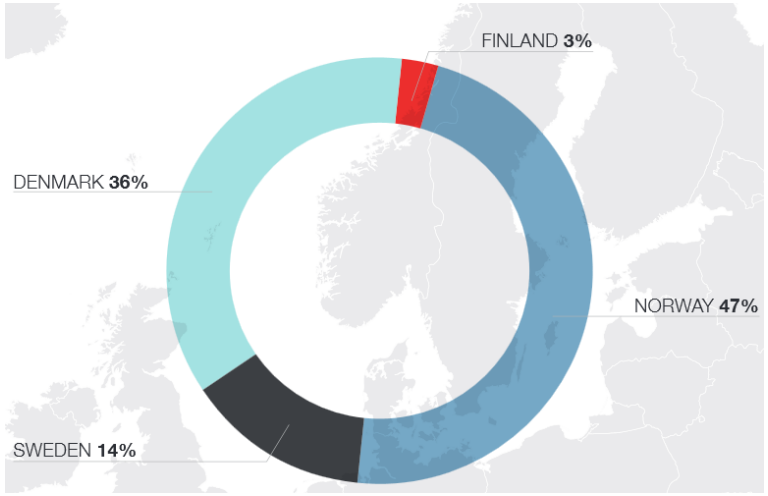


Source: SANS ICS, E-ISAC, March 18, 2016

Cyber Threats and Attacks in Nordic

The Threat is increasing and will not go away

- In August 2015, NSM announced threat actors compromised upto 50 Norwegian Oil companies.
- NSM advised 250 energy companies to check their networks
  - Phishing email with malicious attachment to employees
    - Havex family/Energetic Bear or Dragonfly malware found [source: FireEye]
- BlackEnergy2 found on ICS networks in Sweden [source: Kaspersky Lab]



Advanced persistent threat (APT) and Targeted Malware Alerts in the Nordics by FireEye products [Source: Cyber Threats to the Nordic Region, May 2015, FireEye]

What are potential consequences?

Social Impacts

- Loss of public confidence on organization, e.g. if nuclear accidents occur due to cyber security breach

Others

- Impact on national security
- Loss of sensitive information

Physical Impacts

- Loss of life & personal injury
- Loss of property including data
- Damage to environment

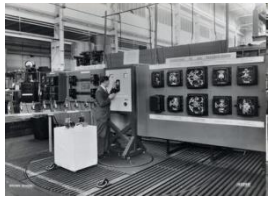
Economic Impacts

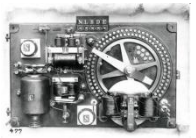
- Economic loss to the facility or organization
- Economic loss to a nation or even great, to global economy
- Loss of brand images
- Legal liabilities

Cyber Security
What are the threats?

Personal computer

Control System ?

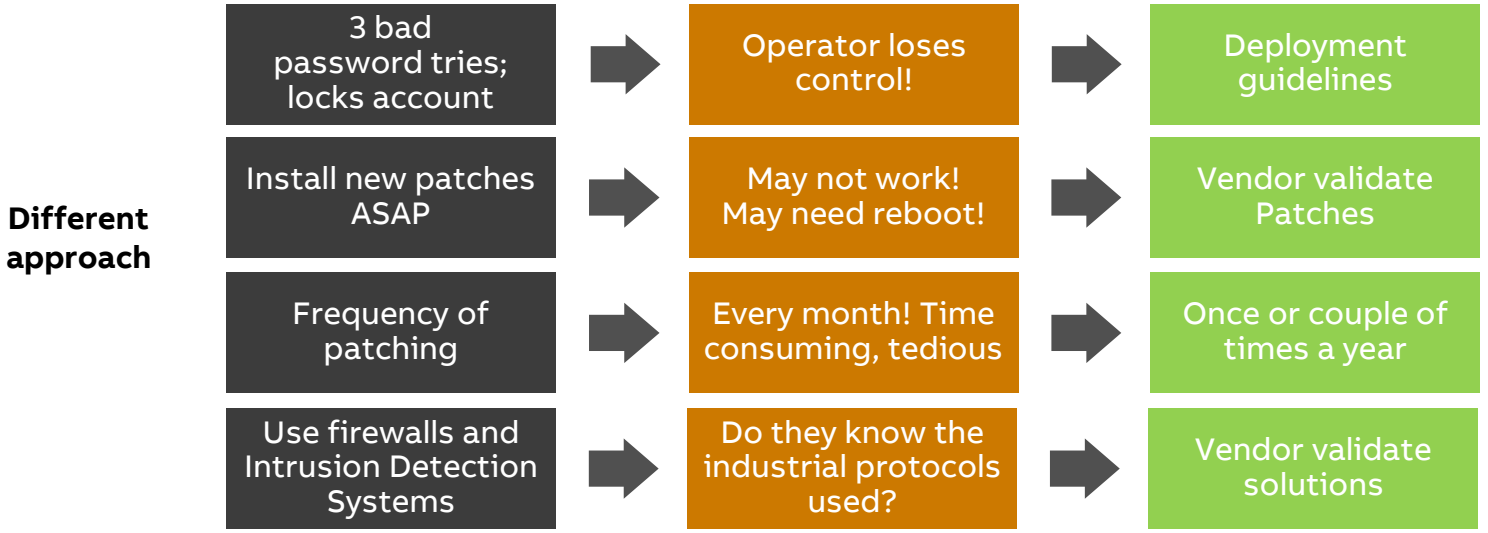




Isolated devices | Point to point interfaces | Proprietary networks | Standard Ethernet/IP-based networks | Inter-connected systems | Distributed systems

Hacking **Malicious software** **Mistakes**

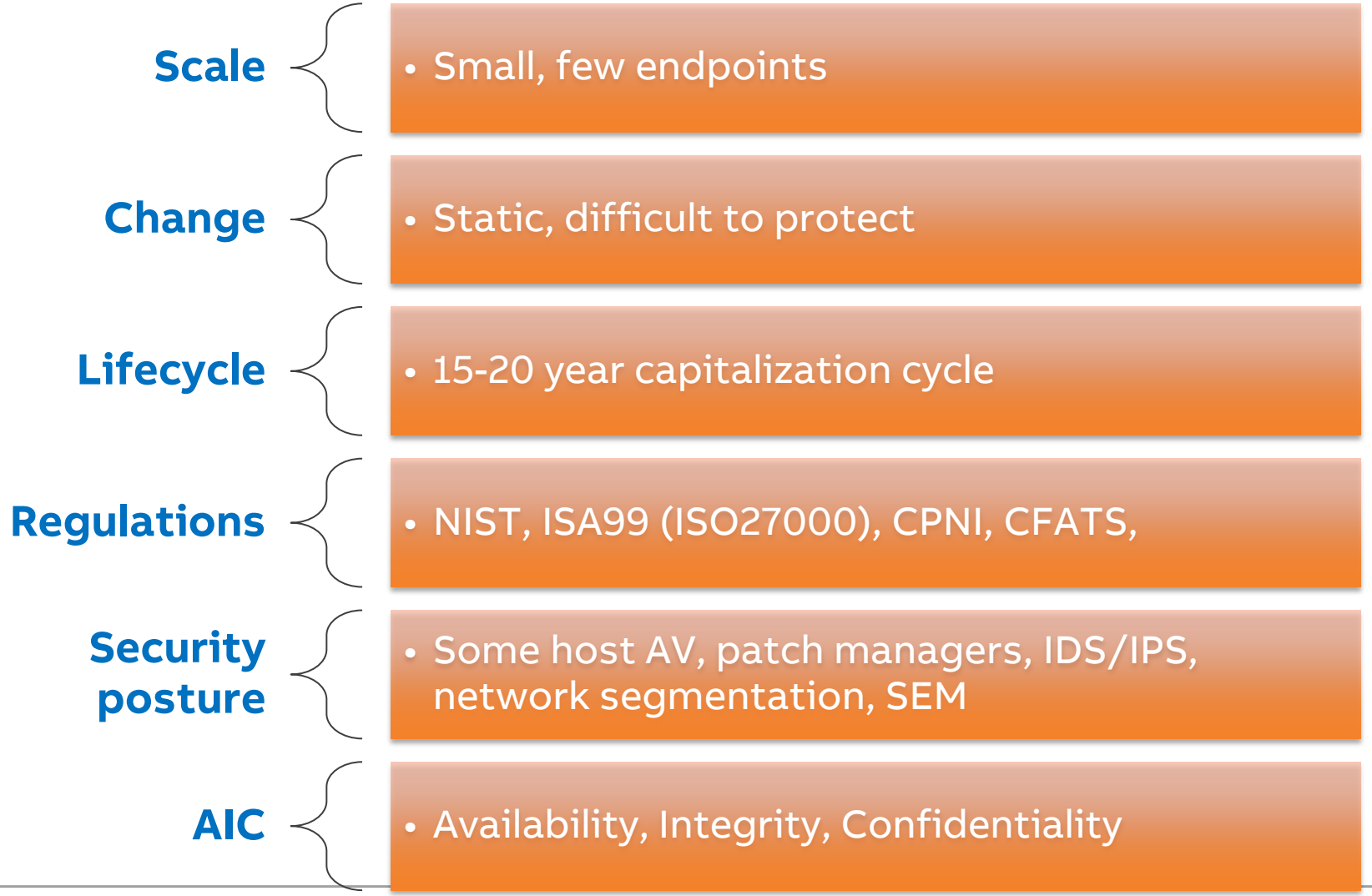
Cyber Security
Traditional IT System vs DCS/SCADA Systems



Enterprise Networks, corporate IT

Scale	• Large, >10,000 endpoints
Change	• Dynamic, difficult to protect
Lifecycle	• 3-5 years
Compliance	• EU Data privacy directive, FCA, PCI, etc.
Security Posture	• Mature, lots of technology developed (Network & host AV, IDS/IPS, segmented networks, certificate authorities and more…
CIA	• Confidentiality, Integrity, Availability

Automation Networks



Mitigation strategies

Prevention:

- Forsee the exploitation of vulnerabilities
- Measures in place to avoid the exploitation
- First line of defense

Detection:

- Monitors the network or system
- Detect the exploit
- Trigger alarms
- Second line of defense

Reaction/Recovery:

- Trigger actions to compromise
- Minimize the impact of exploitation
- Third line of defense

Cyber security best practices
Defense in Depth

The coordinated use of multiple security measures, addressing people, technology, and operations.

Putting it all together - “Defense-in-Depth”…

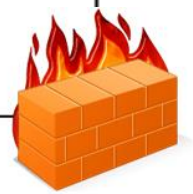
- ✓ Firewall (UTM)
- ✓ NIDS
- ✓ HIDS
- ✓ HIPS
- ✓ Patch Mgmt
- ✓ Reporting
- ✓ Monitoring

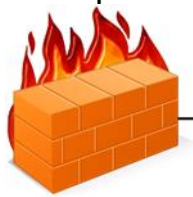
Business Network

24x7 Monitoring

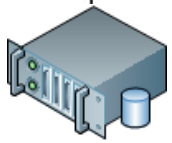
Network Intrusion Detection

DMZ





DMZ



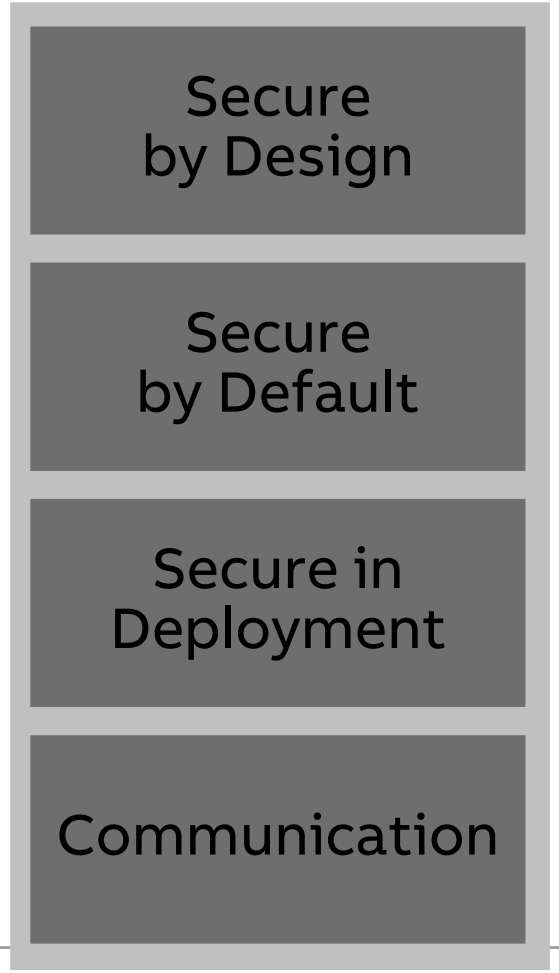
Security Event Manager

Host Intrusion Detection

Host Intrusion Prevention

Active Patch Management

Security for System
The Microsoft SD³+C Security Framework



- Security requirements based on internat. standards
- Security design based on commonly accepted patterns
- Secure implementation supported by automated tools
- Security verification in dedicated test lab

- Default installation with minimal attack surface
- Defense in depth
- Least privileges used

- Product support for secure configuration, operation, maintenance
- Support for system updating

- Openly and responsibly communicate with users about detected security flaws: Implications, corrections and/or workarounds

Secure by Design

Security in the Product Development Process

Secure by Design

Secure by Default

Secure in Deployment

Communication

Product development

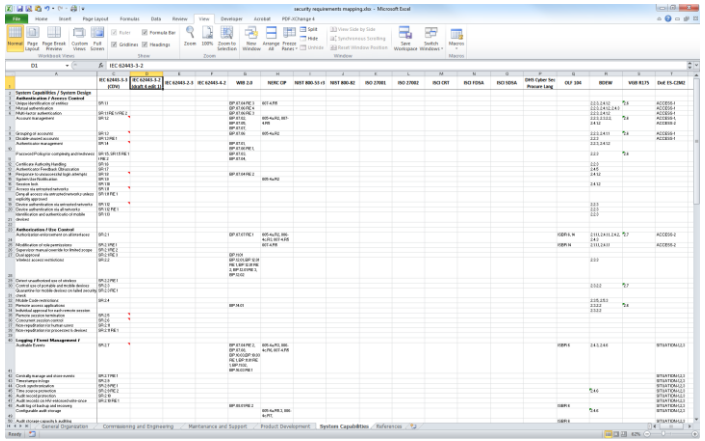
Security integrated in the Quality Management System

- Security check points at Project Execution Levels
- Threat modeling
- Secure coding guidelines

Testing in product development

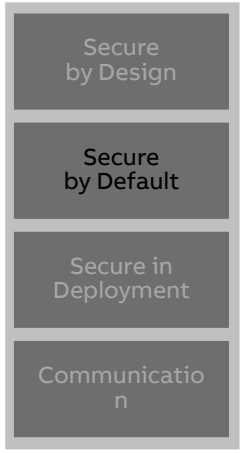
- Requirements verification
- Security testing
- 3rd party testing

Security requirements from International Standards



Secure by Default

Secure Default settings out of the box



Secure default settings

- Automated installation – consistent & repeatable
- Secure default settings and hardening

Defense-in-depth: Hosts

- Windows Firewall @ Hosts
- Network filters @ Controllers
- Network loop protection
- System supervision & monitoring

Defense-in-depth: Network

- Network segregation for different security levels
- Network redundancy
- Logical separation through Firewall
- Secure communication

Access Control

- Active Directory
- RBAC
- Special authentication functions: re-/double authentication, log over, audit trail, digital signatures

Secure in Deployment

Secure Architecture: Security Zones

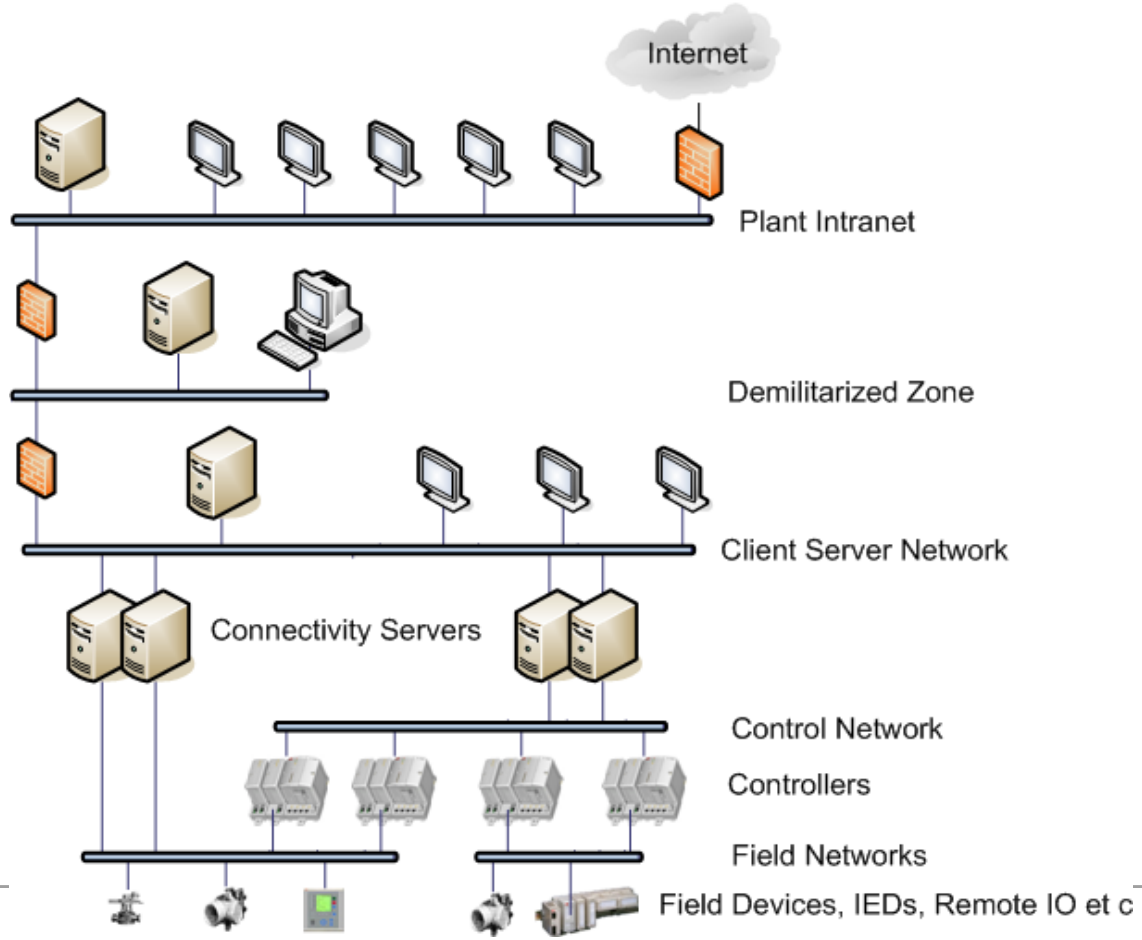
Secure by Design

Secure by Default

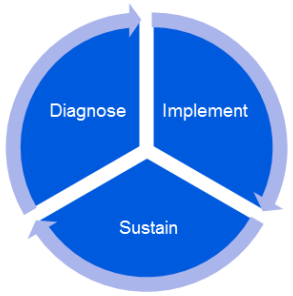
Secure in Deployment

Communication

Security Zones: Multiple Network layers



Cyber Security Life Cycle Management
..how can we protect our systems? ->Multi-phase approach



Diagnose

Measure performance gap

Forecast benefits

Deliver action plan

Implement

Fix performance gap

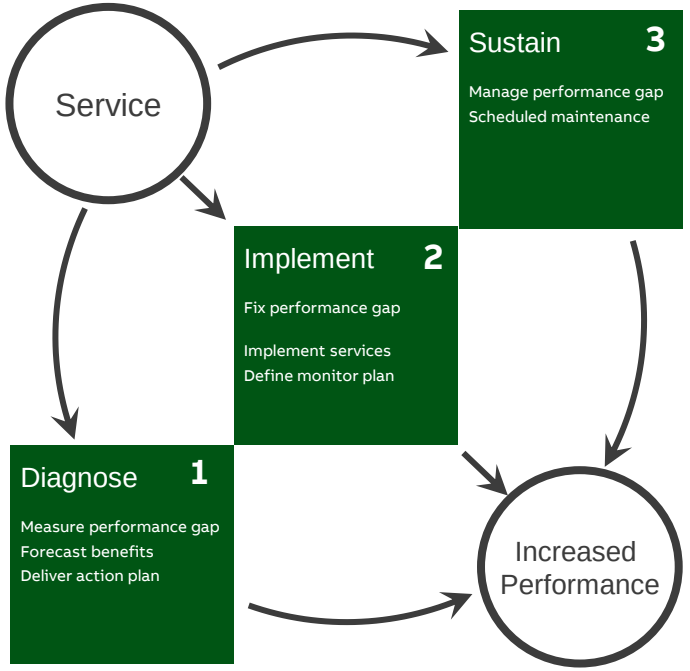
Implement services

Define monitor plan

Sustain

Manage performance gap

Scheduled maintenance – ABB Care



Organizations

Computer Emergency Response Team (CERT): e.g. US-CERT, NorCERT

- Vulnerability or Attacks/Incidences Report to CERT
- Issue alerts or summary report of most frequenct and high impact types of secutity incidences
- Website: http://www.us-cert.gov/; https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- works to reduce risks within and across all critical infrastructure sectors
- ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures
- Website: http://ics-cert.us-cert.gov/

European CERT: http://cert.europa.eu/

Asia Pacific CERT: http://www.apcert.org/

National Institute of Standards and Technology (NIST): http://csrc.nist.gov/

European Network and Information Security Agency (ENISA): http://www.enisa.europa.eu/

- European 'hub' for exchange of information on Cyber Security

Cyber Security – skills/technologies

- Intrusion Detection/Intrusion Prevention: Network-based and host-based
- Risk assessment/analysis/mitigations; Threat modeling: methodologies, tools (e.g. Microsoft STRIDE), interviews, standards
- Security in the cloud
- SIEM solutions, Security Analysis
- Access Control: e.g. Windows base - AD DS, RBAC
- Ethical Hacking
- Penetration Testing
- Security Scanning, Vulnerability Scanner
- Specific solutions: e.g. Firewall, Windows Security, Virtualization Security (e.g. Vmware security)
- Networking: Firewall, Switch, IP addressing
- OSI Layers
- Different Protocols: HTTPS, TLS, IPSec
- Hardware: Servers, Firewall, Ethernet Switch, Workstations
- Software: OS, Antivirus, Backup, Patch Management

Need of Cyber Security Professionals

In every industry

IT

Automation

Utility

Finance

Consulting

Wherver online

Wherver IT

Cyber Security - certification

- ISC(2): e.g. CISSP
- Ethical Haching
- Penetration testing
- Information Security Auditor
- SANS/GIAC cetification: http://www.giac.org/