

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

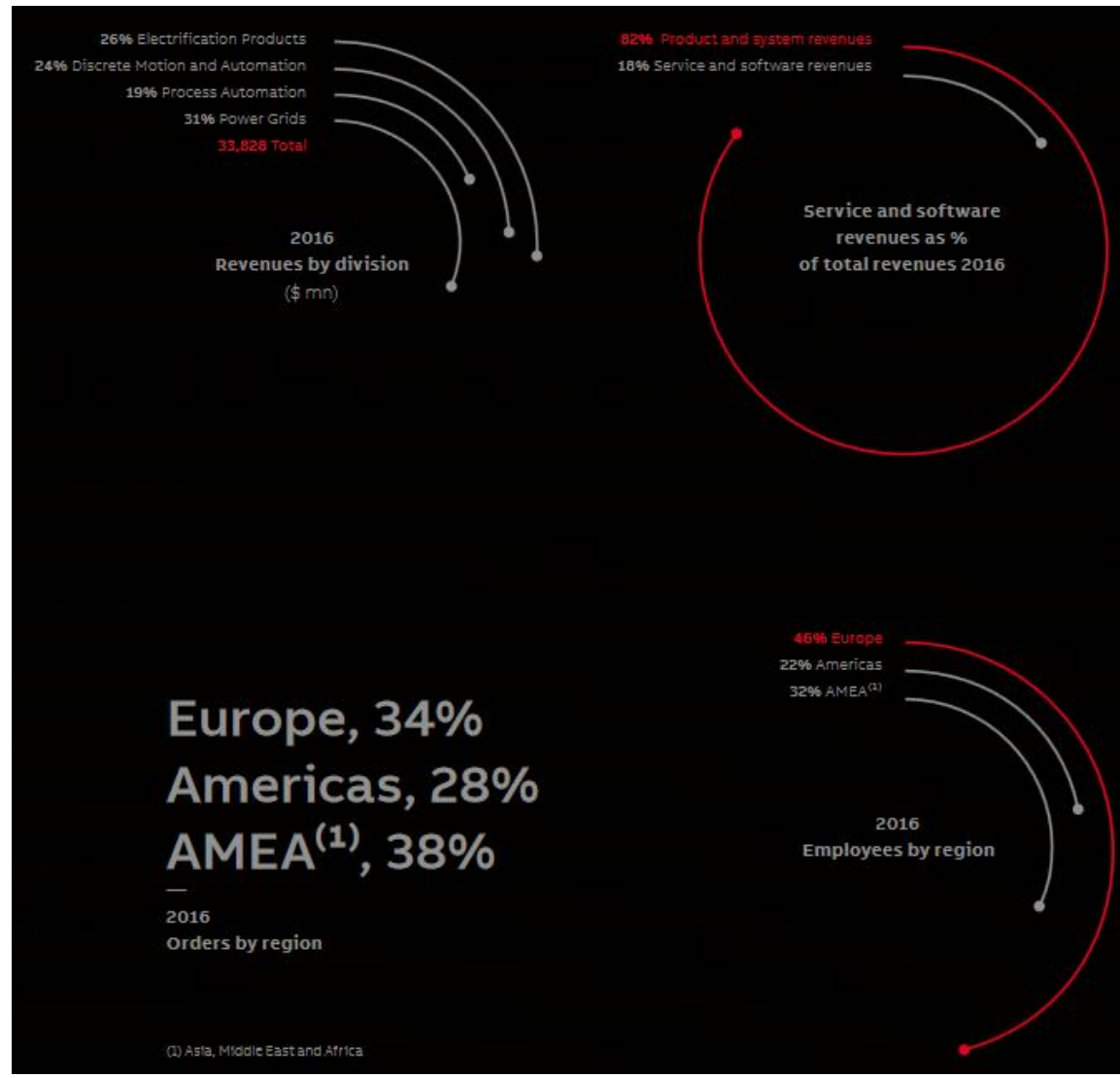
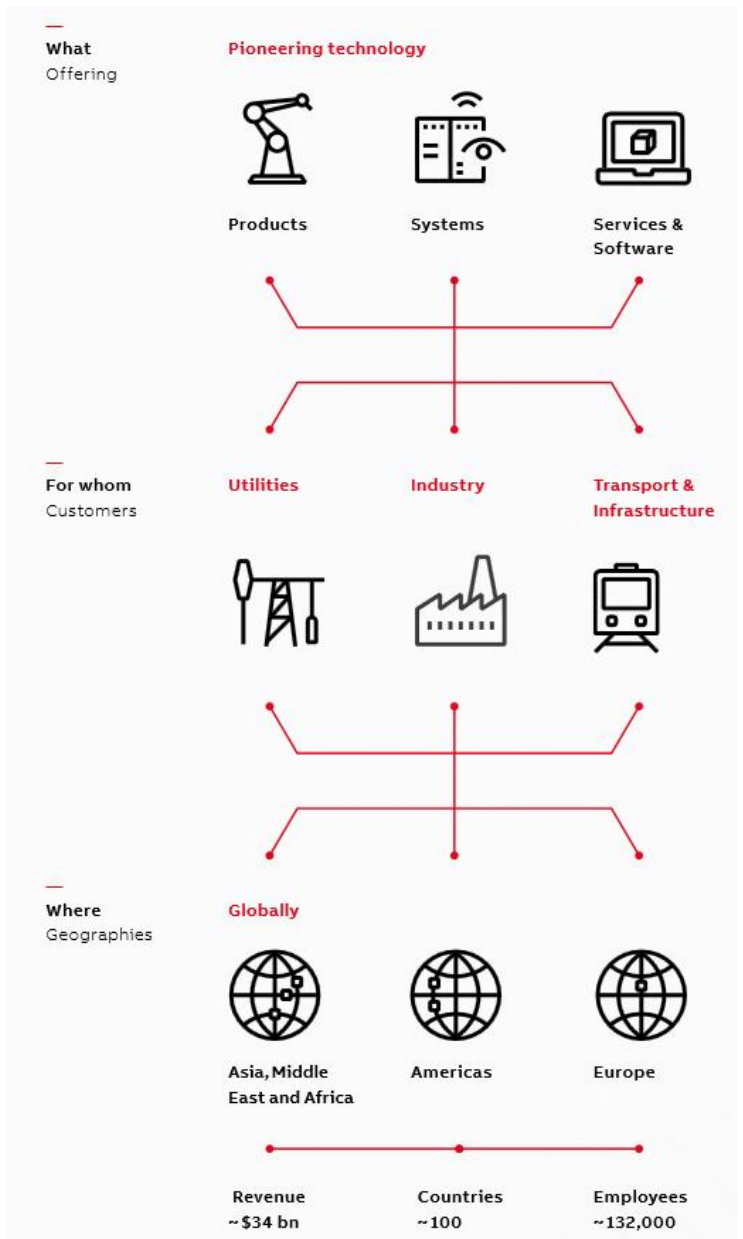


ABB IAOG - Oil, Gas and Chemicals

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
- Access & 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

FINANCIAL TIMES
 ft.com/global/economy
 September 23, 2010 7:39 pm
Stuxnet worm causes worldwide alarm
 By Joseph Menn and Mary Watkins
 No one knows the ultimate goal of the worm, which sends out instructions to machinery and factories. It could destroy gas pipelines, cause power plants and boilers to explode. Perhaps it already has.

Forbes
 New Posts
 +17 posts this hour
 INVESTING | 10/21/2011 | © 12:27 PM | 9,135 views
'Duqu' Virus Likely Handiwork Of Sophisticated Government, Kaspersky Lab Says

the guardian | The Observer
 News | Sport | Comment | Culture | Business | Money | Life & style
 News | Technology | The networker

Series: The networker
How Flame virus did everything for you
 The Flame virus went undetected for a long time. Now they're finding it on the world's PCs from malware.
 The Duqu Trojan probably a govt. What is it looking for? And which looking for it remains a mystery.
 regular threats, like botnets and Duqu, considered the of

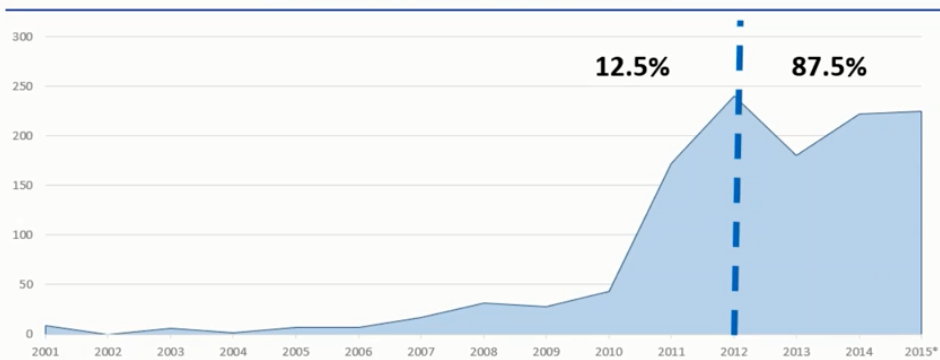
BBC NEWS TECHNOLOGY
 Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/Environment
 17 August 2012 Last updated at 14:22 GMT
Shamoon virus targets energy sector infrastructure
 A new threat targeting infrastructure in the energy industry has been uncovered by security specialists.
 The attack, known as Shamoon, is said to have hit "at least one organisation" in the sector.
 Shamoon is capable of wiping files and rendering several computers on a network unusable.
 On Wednesday, Saudi Arabia's national oil company said an attack had led to its own network being taken offline.
 Saudi Aramco is Saudi Arabia's national oil provider
 Related Stories

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

ICS (SCADA/DCS) disclosures per year



Since 2010 vulnerabilities in control system are increasing.
 "Never touch a running system" methodology does not work anymore

Source: <https://scadahacker.com/>

Electric Grids are Under Attacks!

American power plant shut down by cyber attack
Two U.S. power plants have been infected with computer viruses, and one was shut down by a malicious software in...

European renewable power grid rocked by cyber-attack [fr]
Published 10 December 2012, updated 20 December 2012
Tags cyber-attacks, cybersecurity, grid, power grid, renewables
4 comments

Infrastructure protection
U.S. power and water utilities face daily cyberattacks
Published 6 April 2012
American water and energy companies face a barrage of cyberattacks on a daily basis...

Cyber Incident Blamed for Nuclear Power Plant Shutdown
By Brian Krebs, June 04, 2008

Florida Utility Company Hit by Cyber Attack
A denial of service attack disabled JEA's Web site and automated phone system.
By Jeff Goldman | February 21, 2013
The Web site and automated phone system for Florida's JEA (formerly the Jacksonville Electric Authority) were hit by a denial-of-service attack that started on Sunday and continued on Wednesday morning.
"JEA is the seventh-largest community-owned electric utility in the United States, the largest water and sewer utilities in the nation providing electric, water and sewer services to residents and businesses in northeast Florida," writes Michael Clinton.

FBI: Smart Meter Hacks Likely to Spread
692 tweets
TOP +1K
retweet
A series of hacks perpetrated against so-called "smart meter" installations over the past several years may have cost a single U.S. electric utility hundreds of millions of dollars annually, the FBI said in a cyber intelligence bulletin obtained by KrebsOnSecurity. The law enforcement agency said this is the first known report of criminals compromising the hi-tech meters, and that it expects this type of fraud to spread across the country as more utilities deploy smart grid technology.
Smart meters are intended to improve efficiency, reliability, and allow the electric utility to charge different rates for...

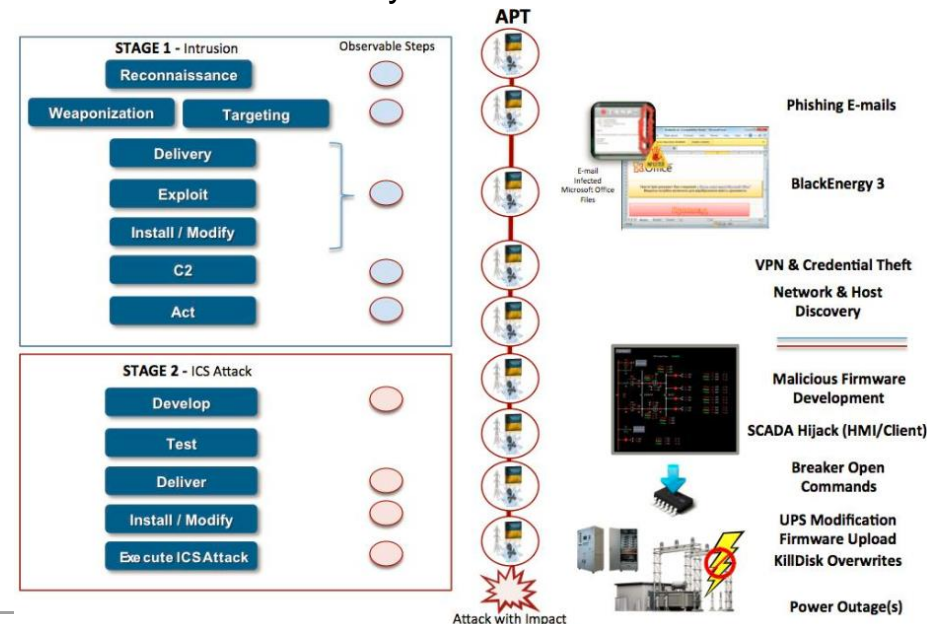
FEDERAL BUREAU OF INVESTIGATION
INTELLIGENCE BULLETIN
Cyber Intelligence Section
27 May 2010

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



Cyber Threats and Attacks in Nordic

The Threat is increasing and will not go away



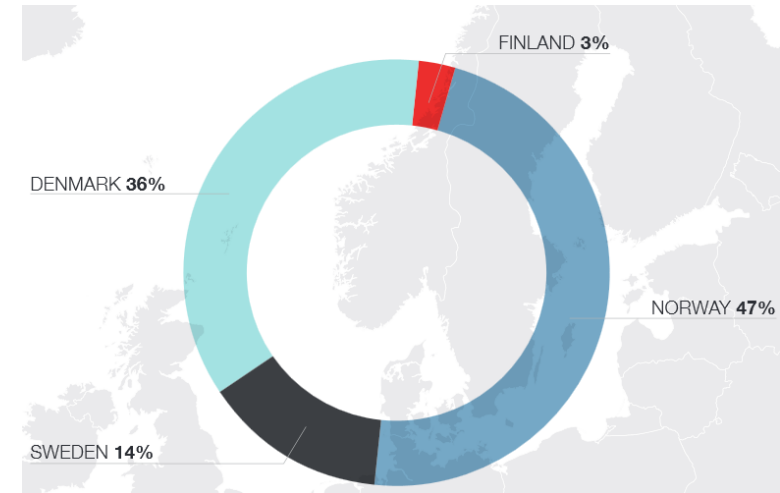
Hackers Launch All-Out Assault on Norway's Oil and Gas Industry

August 31, 2014 @ 05:17 PM EST

In what's being billed as the largest ever coordinated cyberattack in Norway, hackers have targeted some 300 different firms within the country's oil and energy industries. The attacks were revealed last week by the Nasjonal sikkerhetsmyndighet (National Security Authority Norway), which had been tipped off to the attacks by "International



- 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

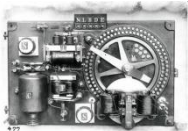
What are the threats?



Personal computer



Control System ?



Isolated devices

Point to point interfaces

Proprietary networks

Standard Ethernet/IP-based networks

Inter-connected systems

Distributed systems



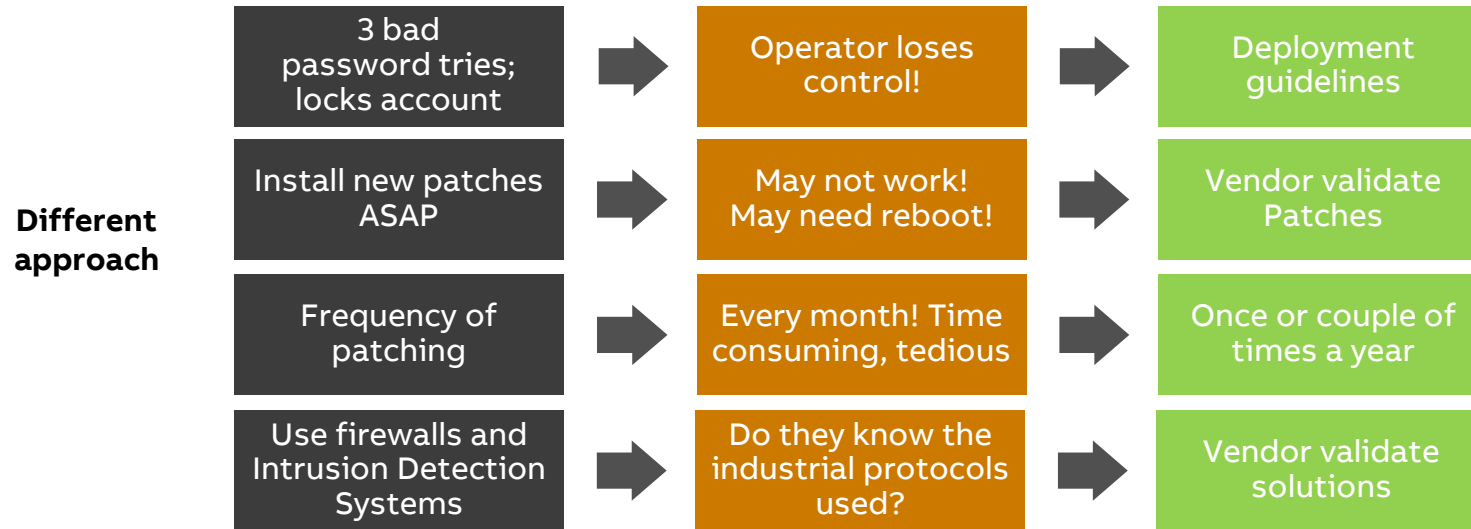
Hacking

Malicious software

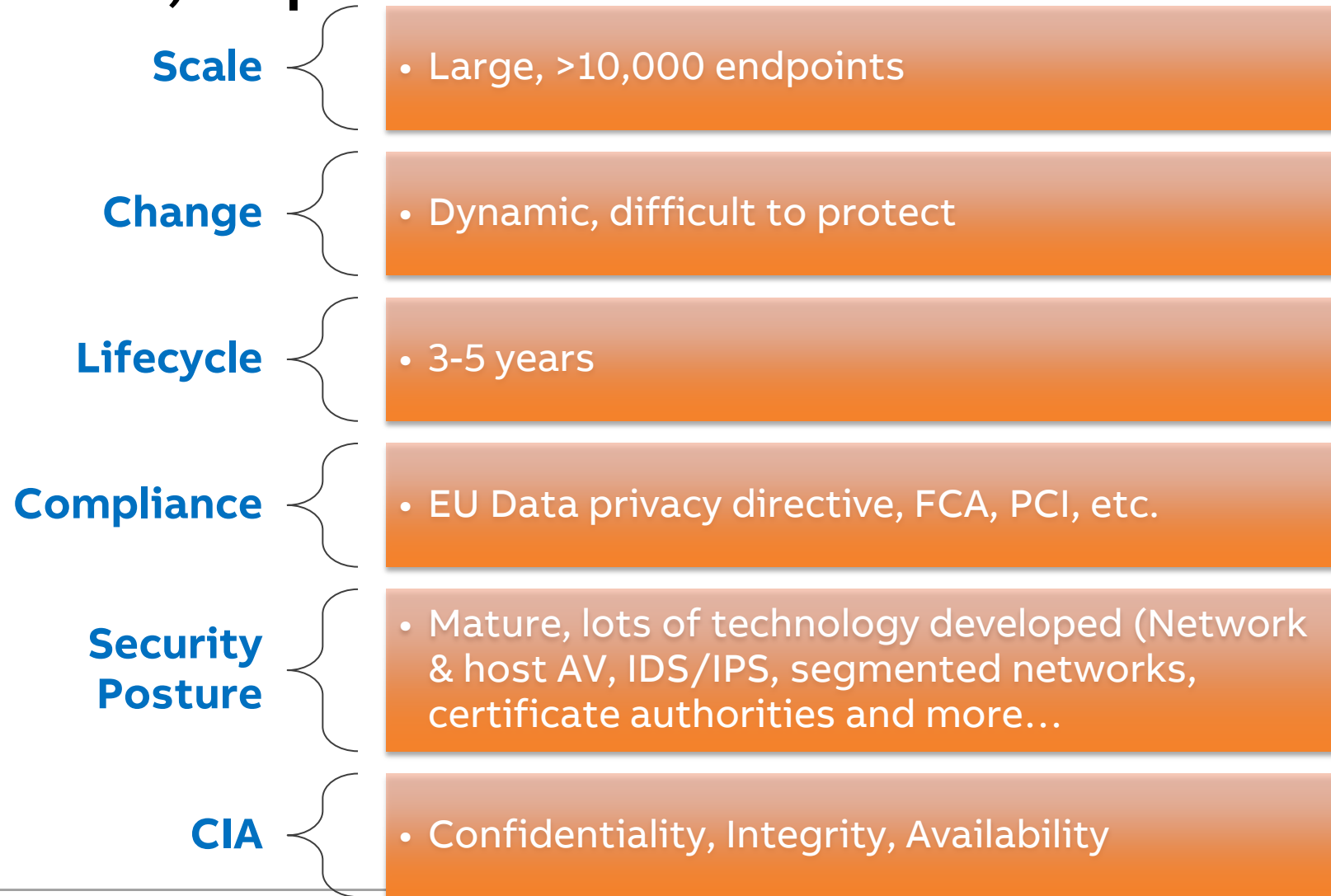
Mistakes

Cyber Security

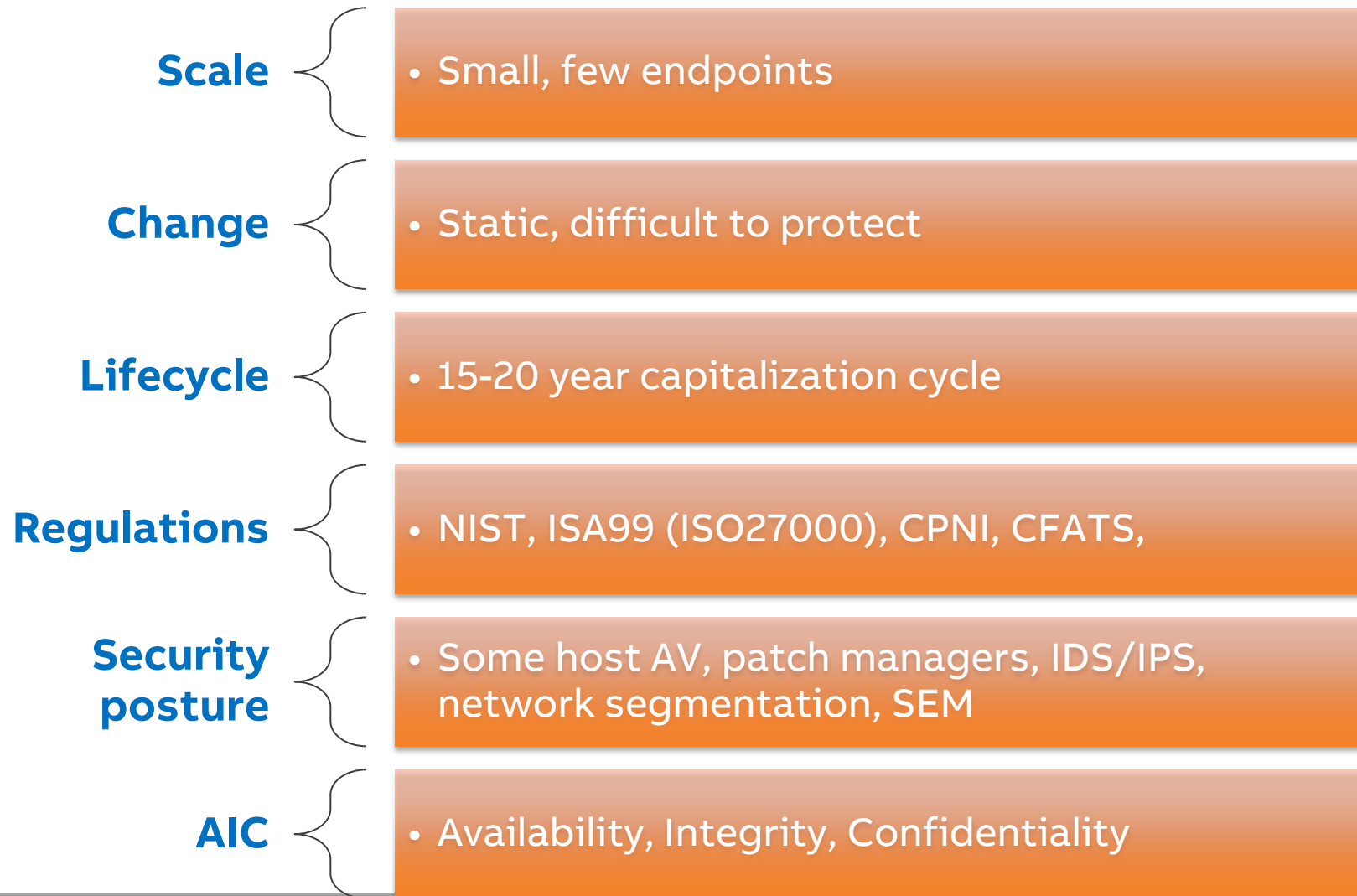
Traditional IT System vs DCS/SCADA Systems



Enterprise Networks, corporate IT



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.

Physical Security

Procedures and Policies

Firewalls and Architecture

Computer Policies

Account Management

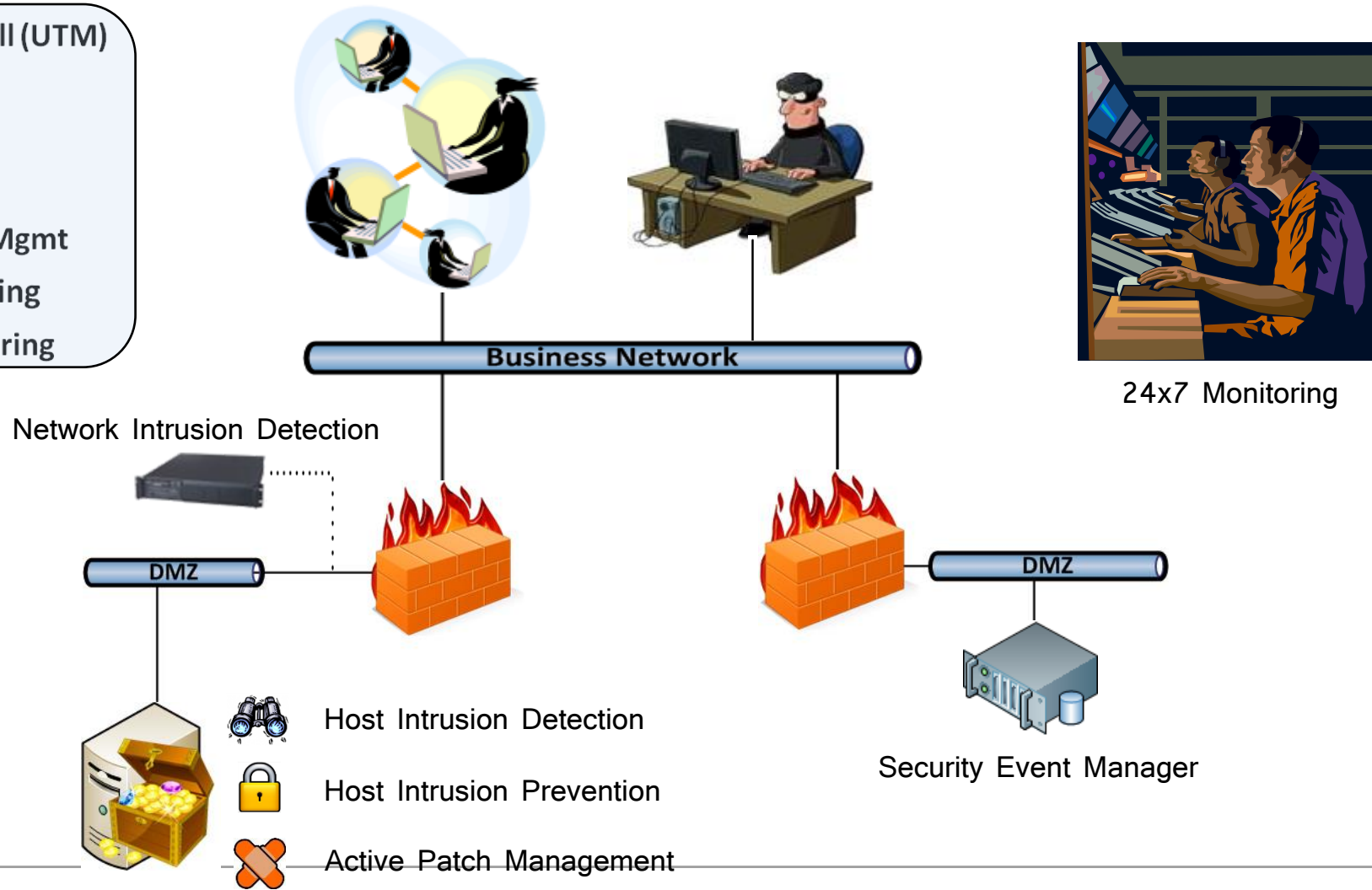
Security Updates

Antivirus Solutions



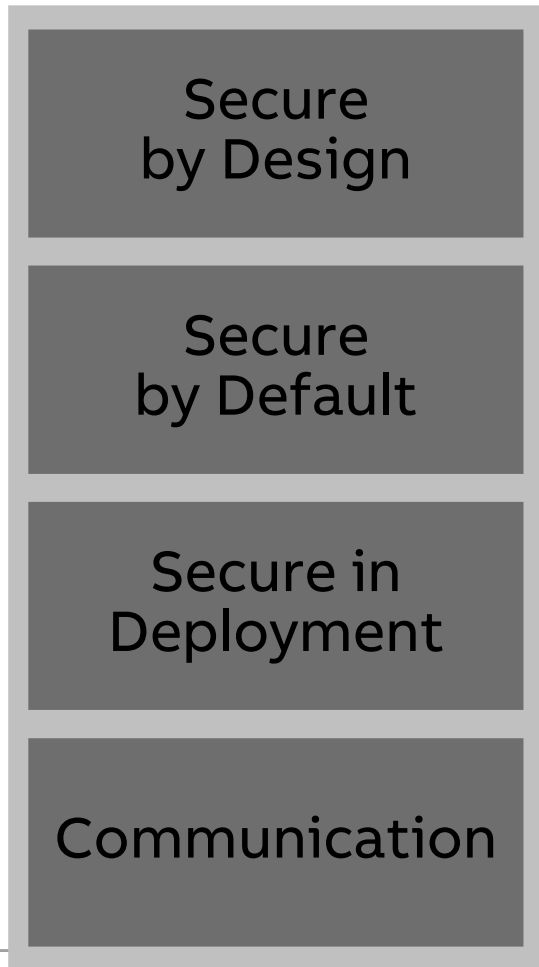
Putting it all together - "Defense-in-Depth"...

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



Security for System

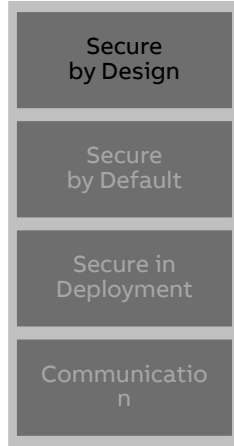
The Microsoft SD³+C Security Framework



- 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



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

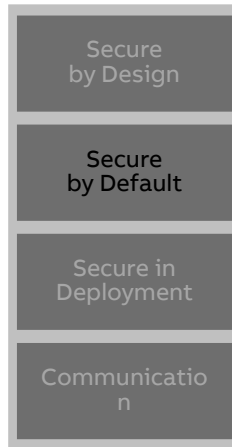
- Requirements verification
- Security testing
- 3rd party testing

Security requirements from International Standards

System Capability / System Design	Requirement ID	Requirement Description	Requirement Type	Requirement Status	Requirement Priority	Requirement Category	Requirement Sub-category	Requirement Detail	Requirement Reference	Requirement Source	Requirement Impact	Requirement Mitigation	Requirement Verification	Requirement Validation	Requirement Acceptance	Requirement Approval	Requirement Review	Requirement Change	Requirement History	Requirement Comments
System Capability / System Design	SP101	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP102	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP103	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP104	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP105	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP106	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP107	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP108	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP109	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control
System Capability / System Design	SP110	System shall be able to handle...	Functional	Active	High	Security	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control	Access Control

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

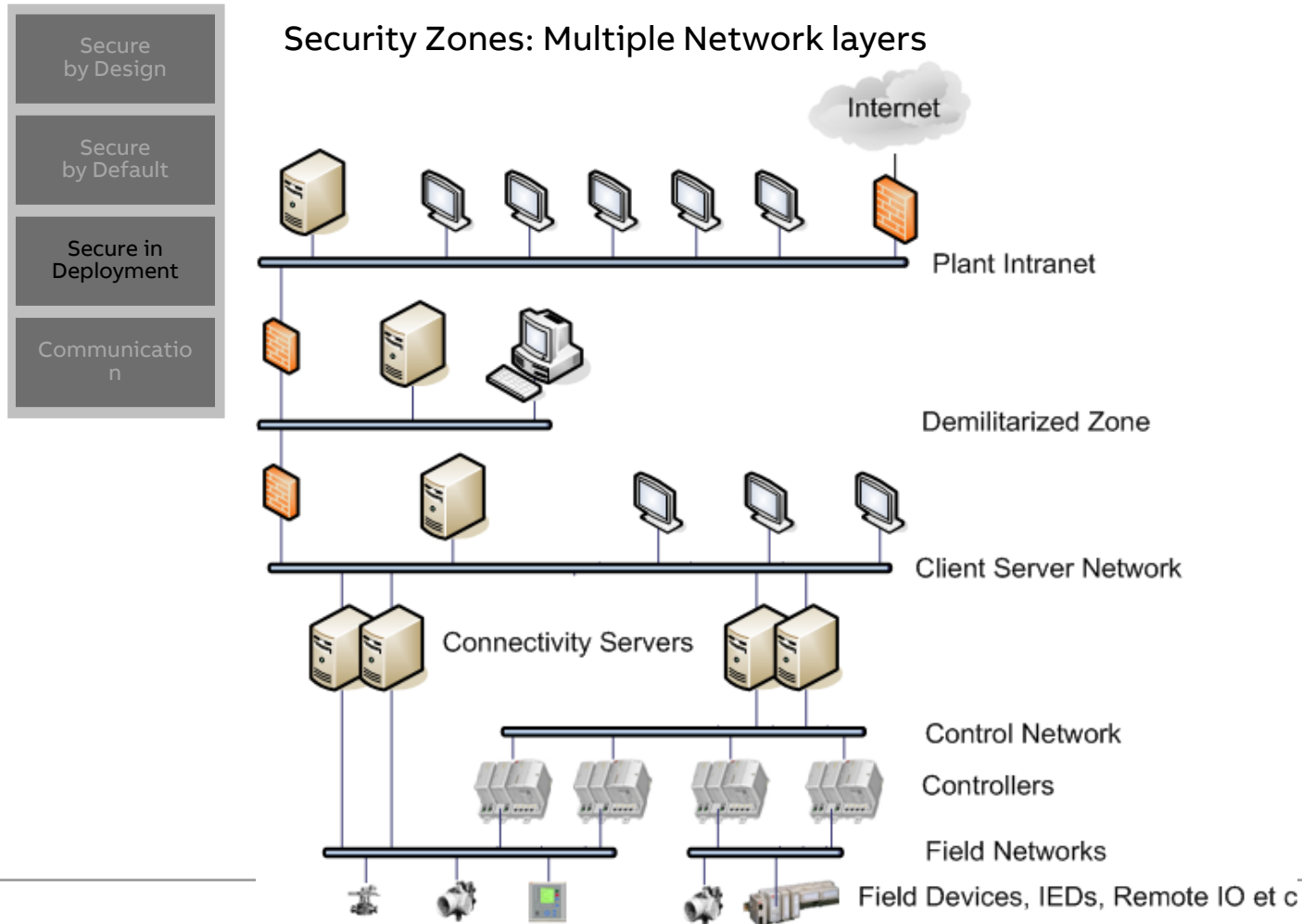
- Network segregation for different security levels
- Network redundancy
- Logical separation through Firewall
- Secure communication

Access Control

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

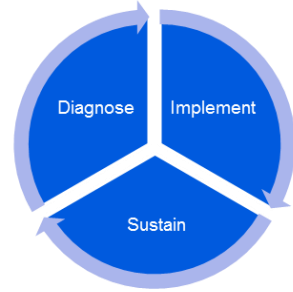
Secure in Deployment

Secure Architecture: Security Zones



Cyber Security Life Cycle Management

..how can we protect our systems? ->Multi-phase approach



Diagnose

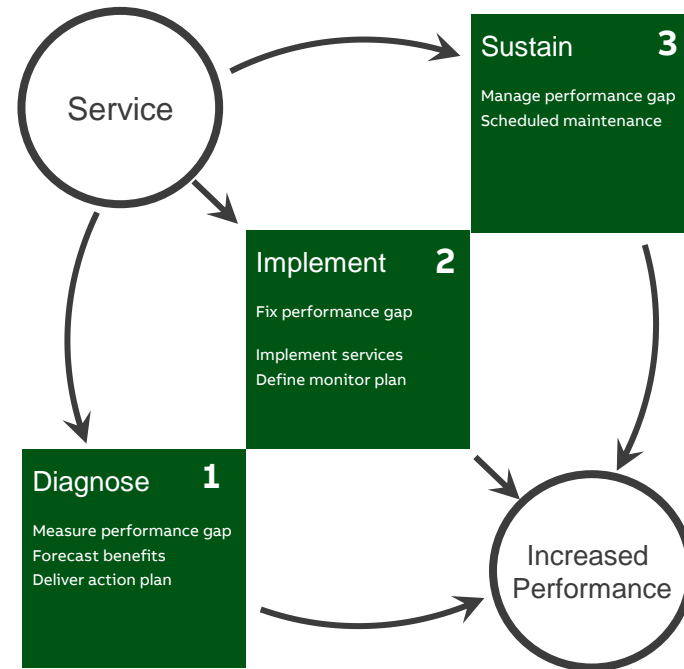
- Measure performance gap
- Forecast benefits
- Deliver action plan

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 frequent and high impact types of security 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

Wherever online

Wherever IT

Cyber Security - certification

- ISC(2): e.g. CISSP
- Ethical Hacking
- Penetration testing
- Information Security Auditor
- SANS/GIAC certification: <http://www.giac.org/>



ABB