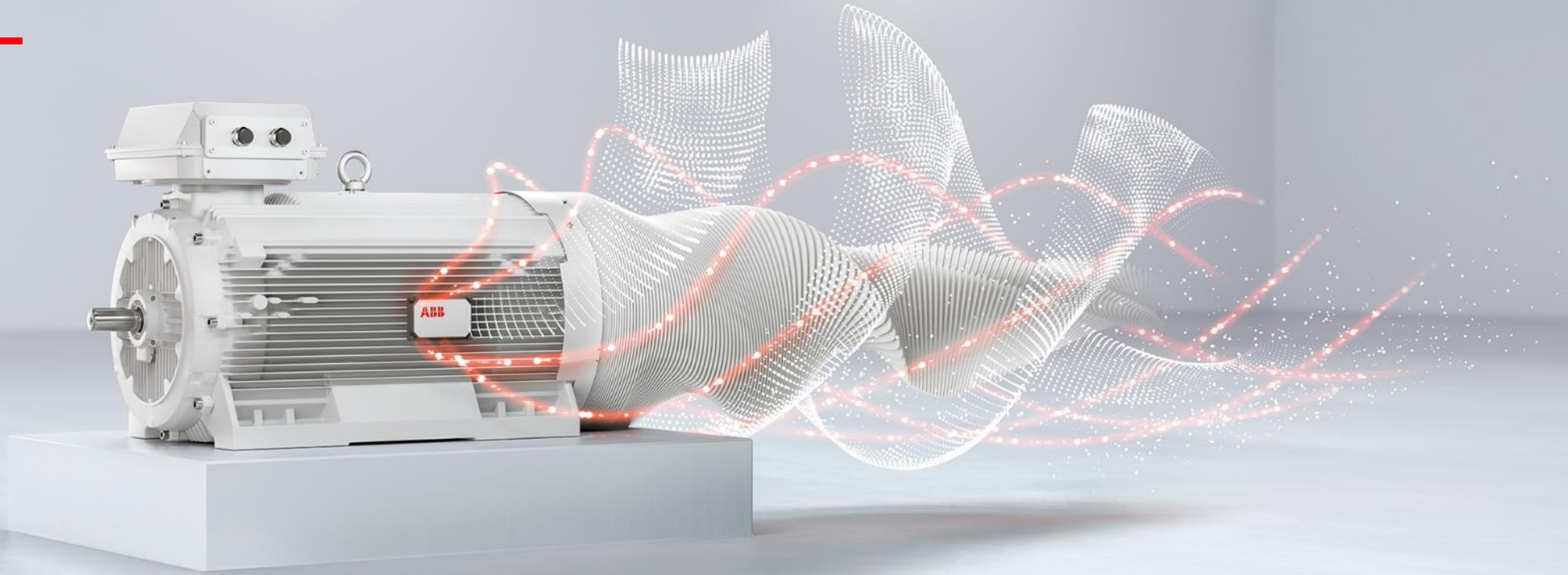




Industrial Control System (ICS) Security

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

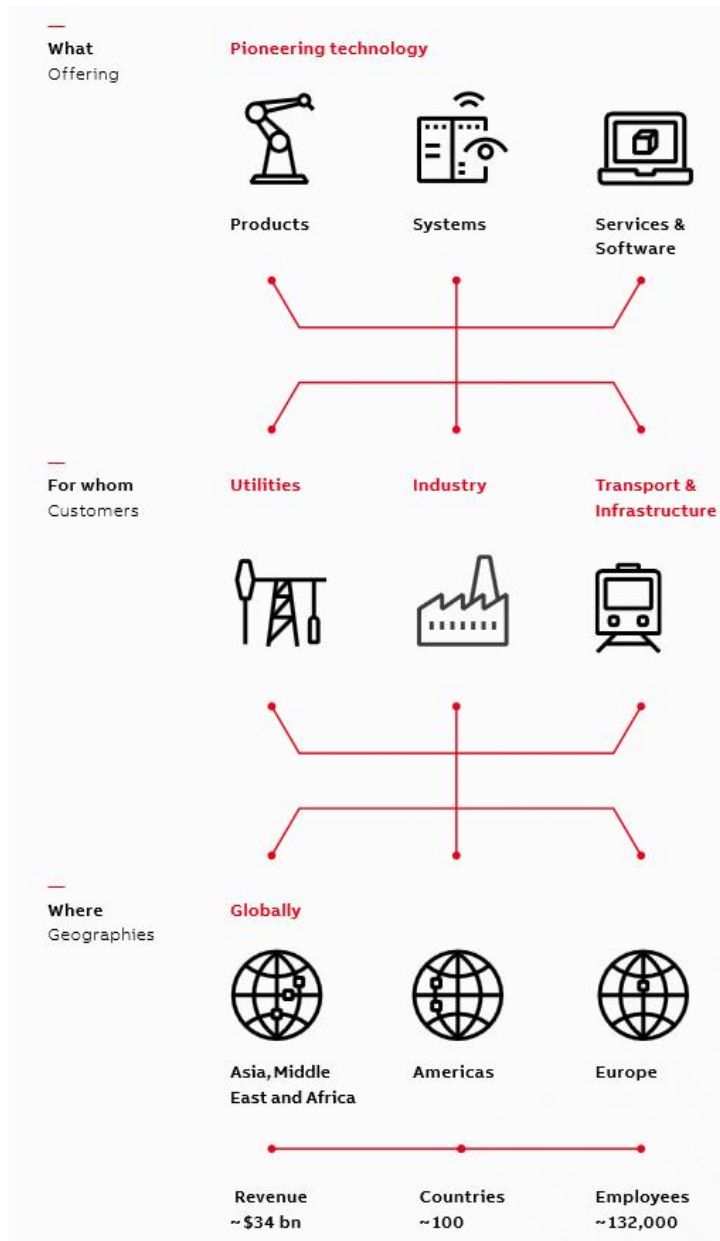


ABB IAOG - Oil, Gas and Chemicals

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](#)

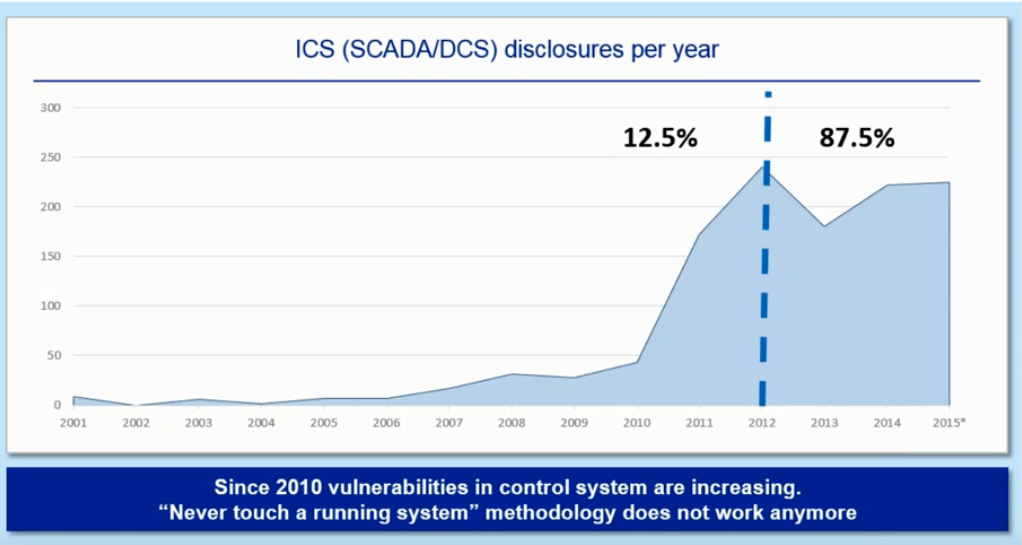
[Gina Krog](#)



[Goliat](#)

[Sadara](#)

ICS Trends/Incidences



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

FINANCIAL TIMES
ft.com/globaleconomy
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 Stuxnet worm, which sends out instructions to machinery and factories. It could destroy gas pipelines, cause power plants to explode. Perhaps it already has.

Forbes
New Posts
+37 posts this hour
INVESTING — 10/21/2011 @ 12:27PM — 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 went everything for o
The Flame virus went un security firm. Now they ne world's PCs from malware
regular threats, like bot Duqu, considered the o

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.
Here's a question: If you connect to the internet, how long will it take before it is infected by malicious software? The answer is: much more quickly than most lay users think. In 2003, the average time was 40 minutes. A year later it was 20 minutes. By 2008 an unpatched computer running Microsoft Windows XP could only expect five to 16 minutes of freedom. The Internet Storm Centre (ISC) provides a useful chart of what it calls "survival time" for Windows machines. It suggests that a PC currently can expect between 40 and 200 minutes of freedom before an automated probe searches it to determine whether it can
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



Electric Grids are Under Attacks!

The collage features several news snippets:

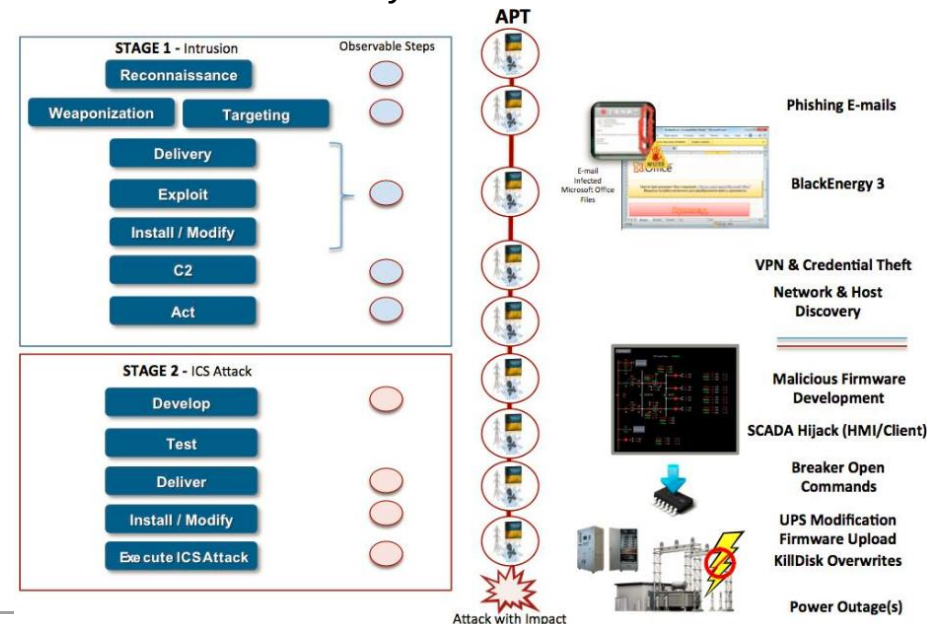
- American power plant shut down by cyber attack**
Two U.S. power plants have been infected with computer viruses, and one was shut down by a malicious software in...
- European renewable power grid rocked by cyber-attack**
Published 10 December 2012, updated 20 December 2012
Tags: cyber-attacks, cybersecurity, grid, power grid, renewables
4 comments
- U.S. power and water utilities face daily cyberattacks**
Published 6 April 2012
Infrastructure protection
- 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 Authority) were hit by a denial-of-service attack that started on Sunday and 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 residents and businesses in northeast Florida," writes The Jacksonville Evening News 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



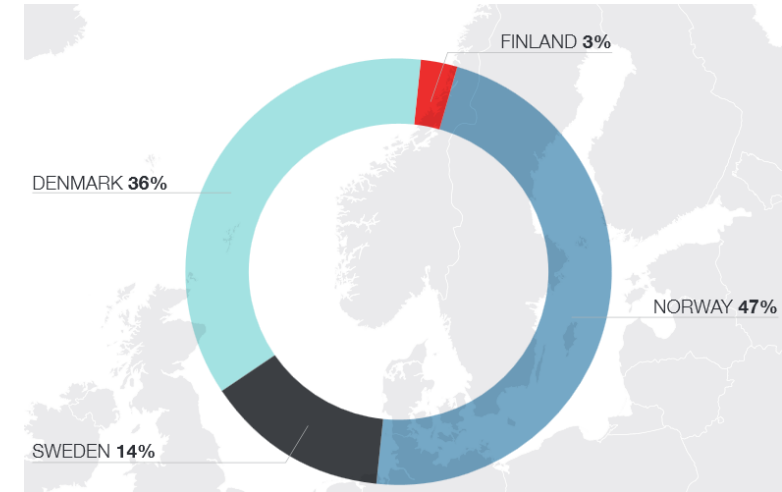
Hackers Launch All-Out Assault on Norway's Oil and Gas Industry

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

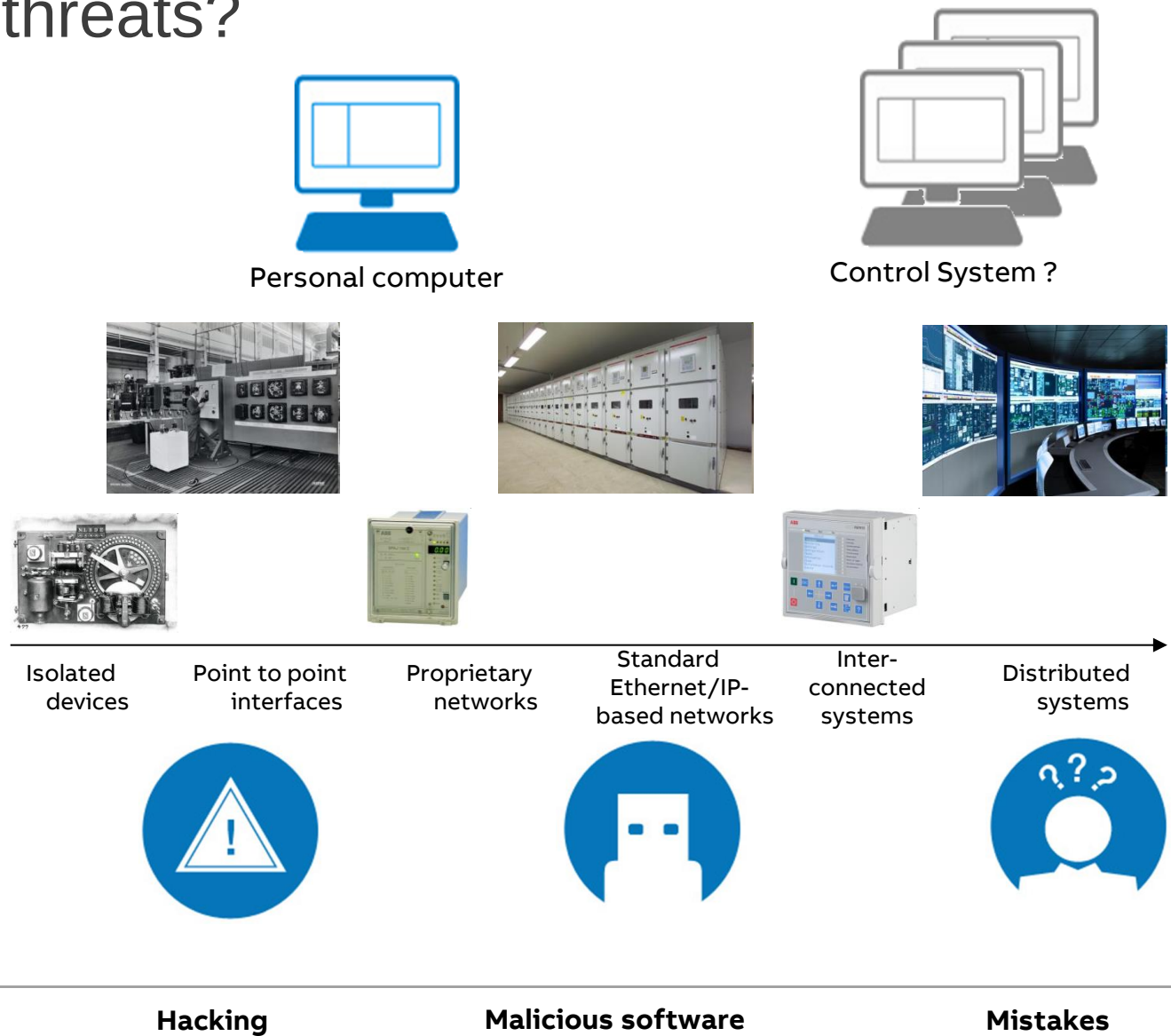
- Loss of life & personal injury
- Loss of property including data
- Damage to environment

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

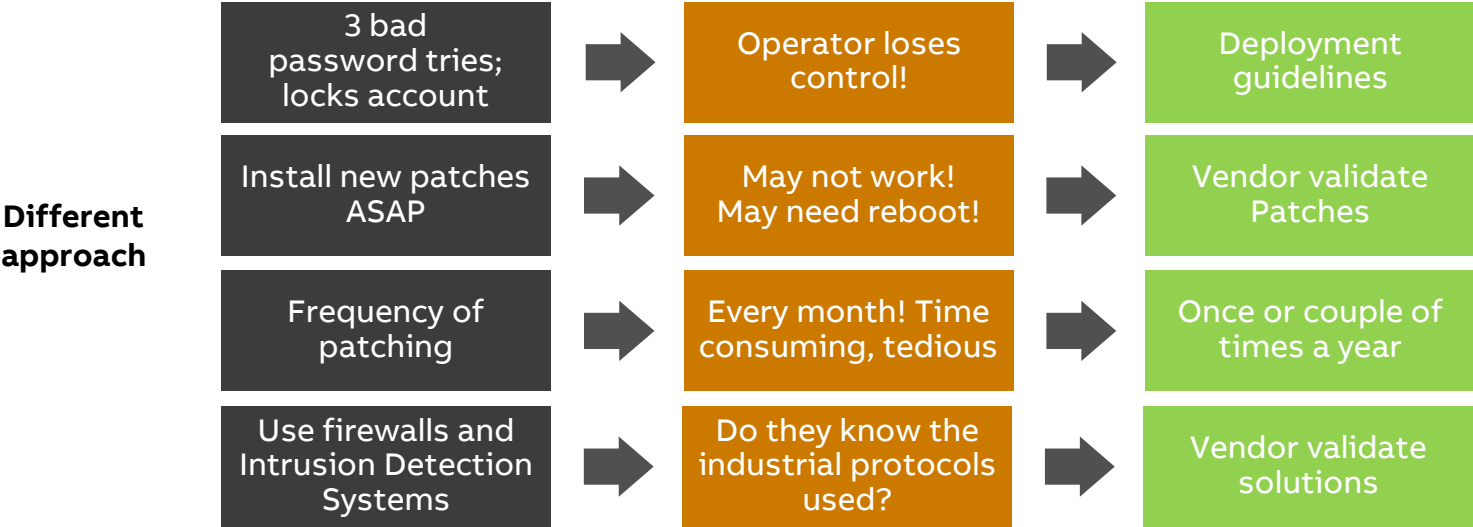
Cyber Security

What are the threats?

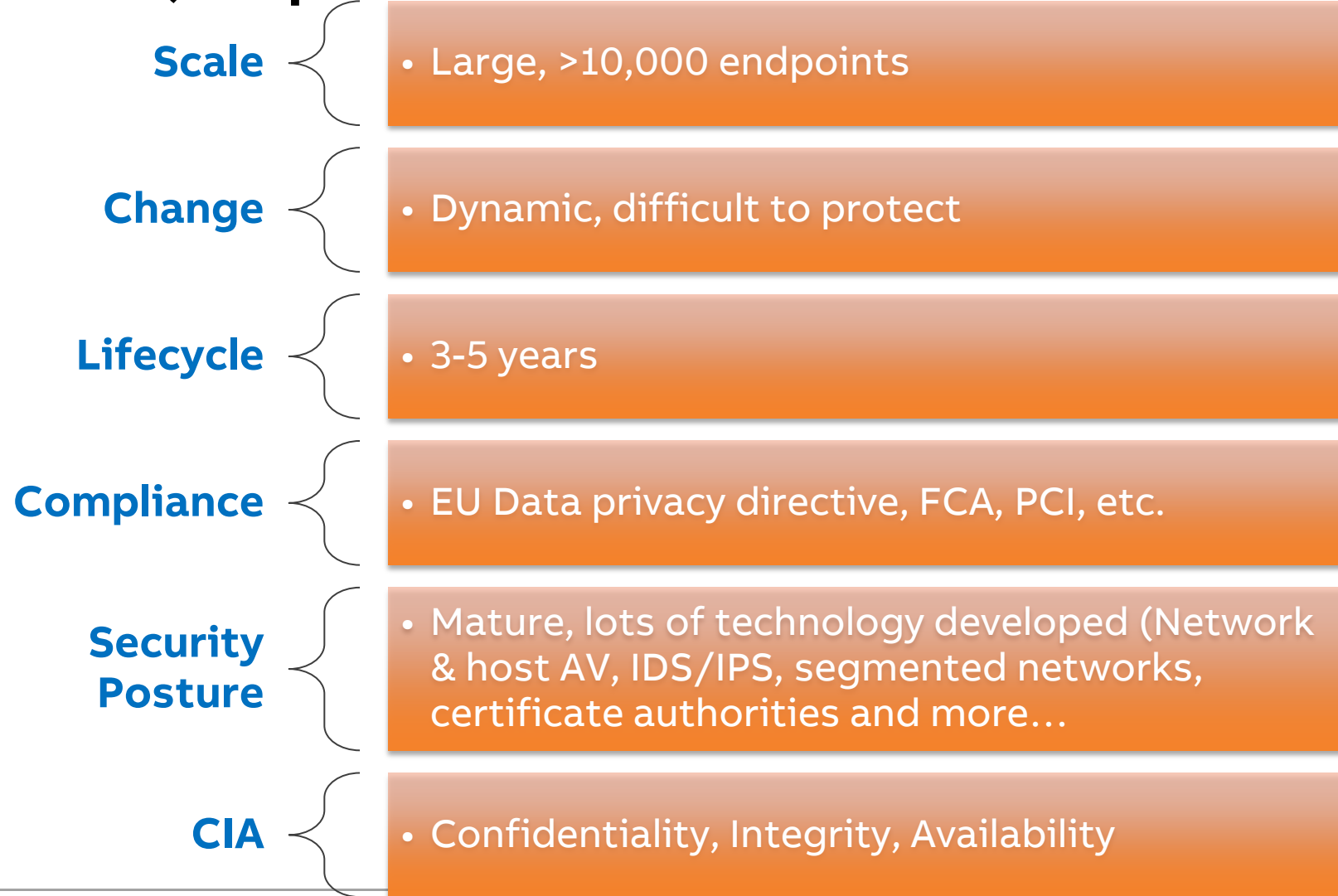


Cyber Security

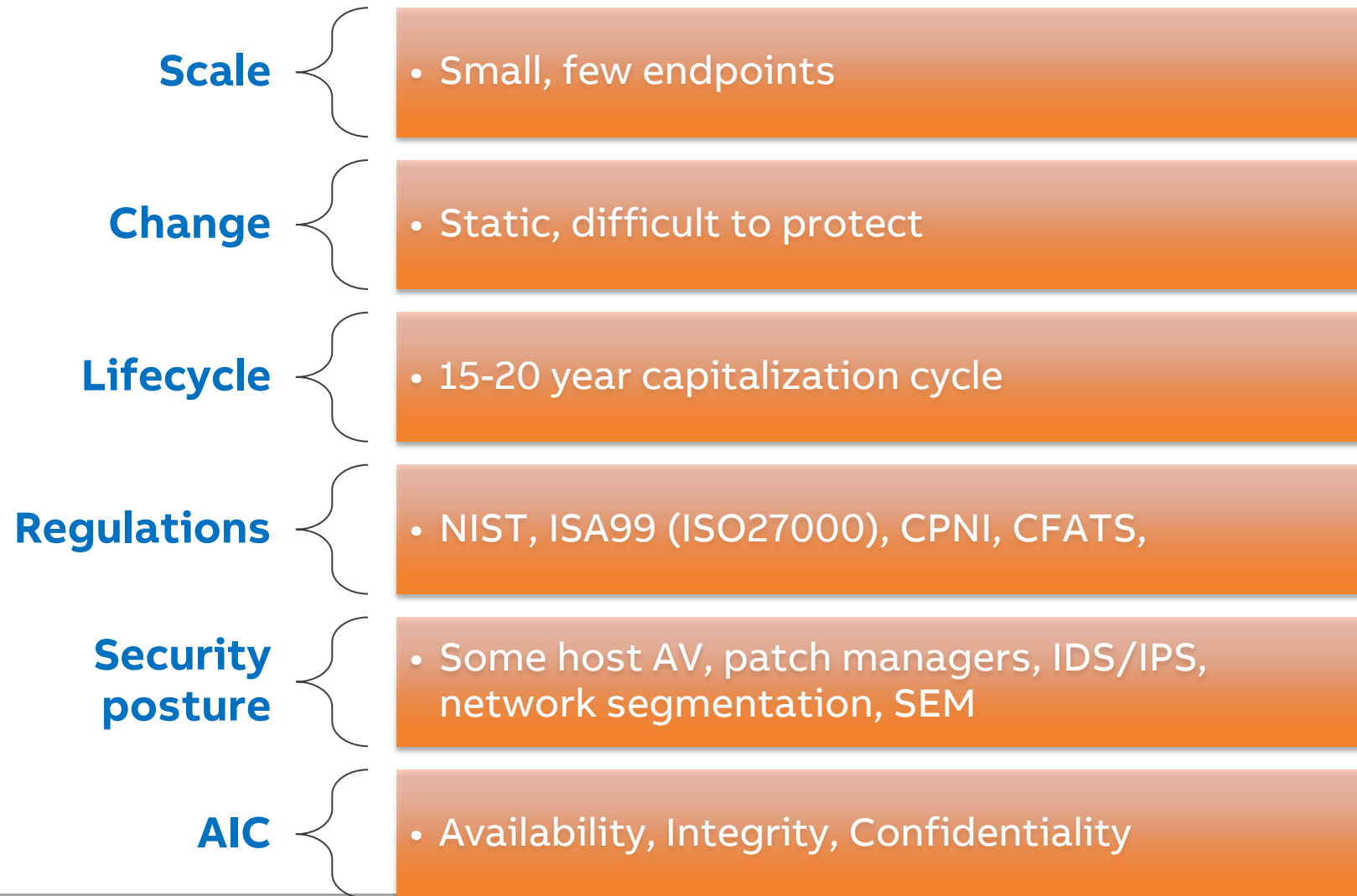
Traditional IT System vs DCS/SCADA Systems



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

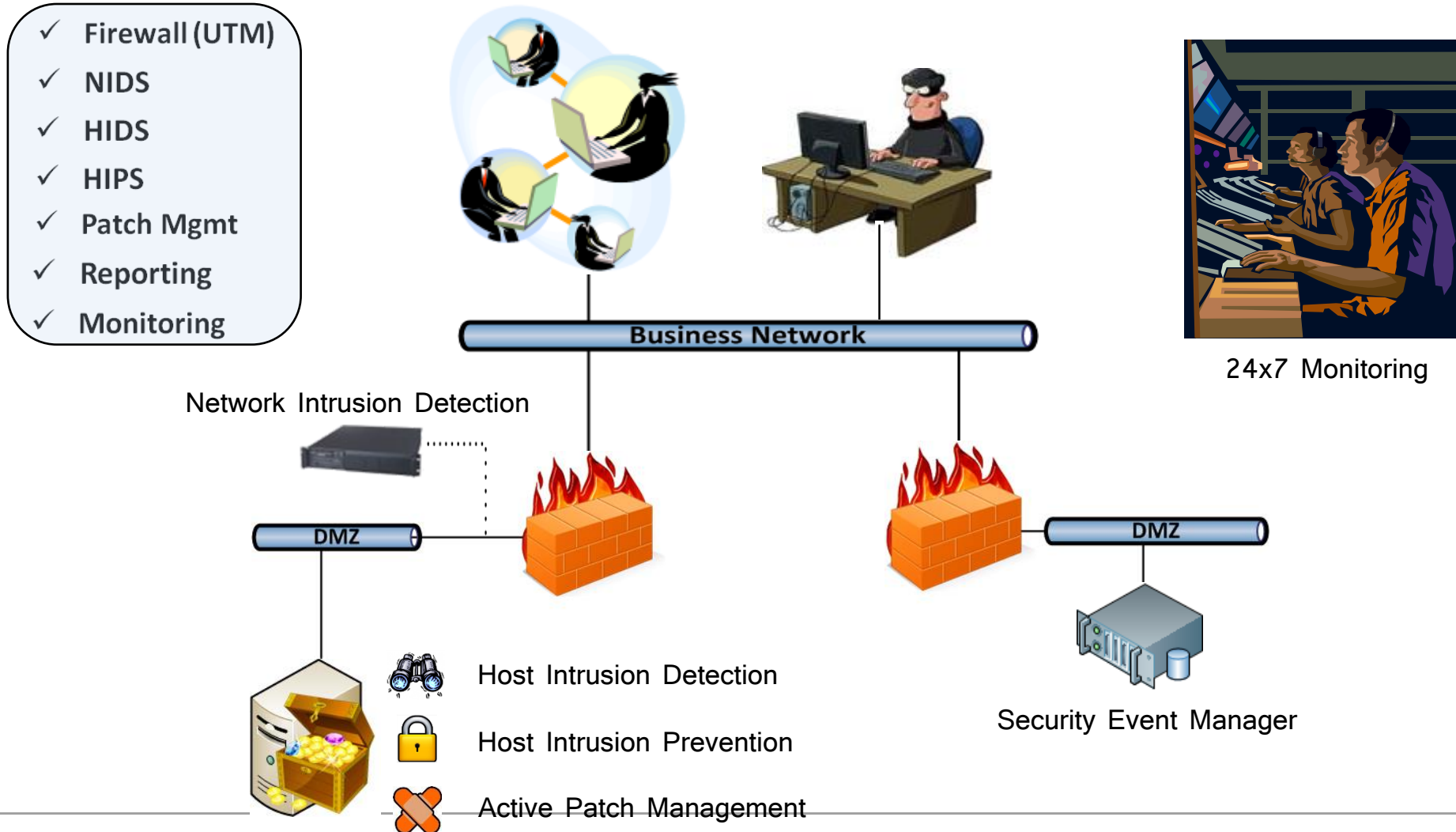
Account Management

Security Updates

Antivirus Solutions

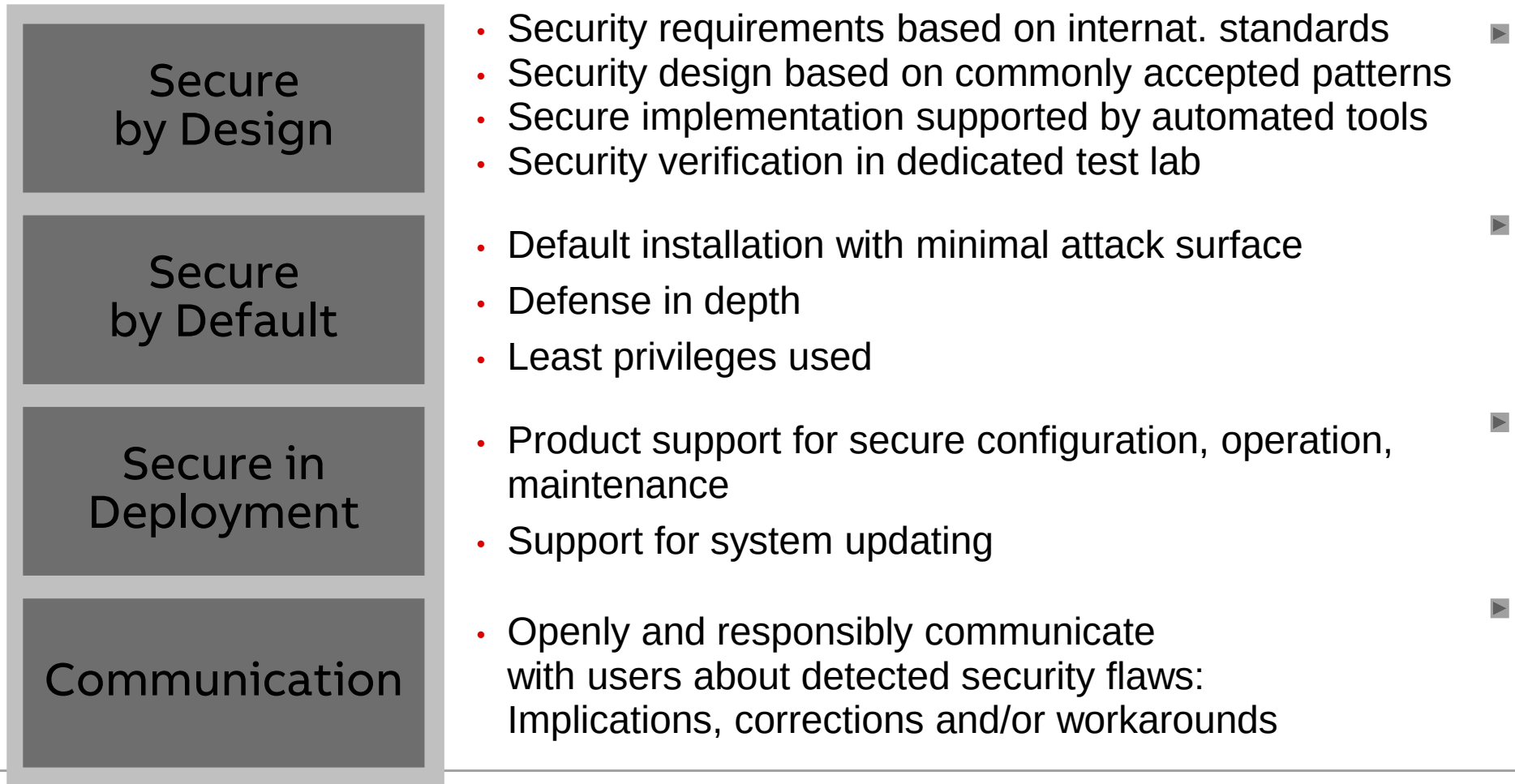


Putting it all together - “Defense-in-Depth”...



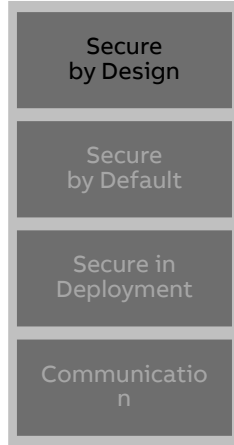
Security for System

The Microsoft SD³+C Security Framework



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

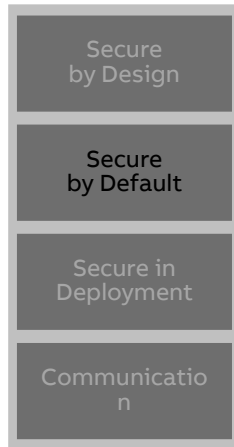
- Requirements verification
- Security testing
- 3rd party testing

Security requirements from International Standards

Standard	Clause	Requirement	Mapping
ISO 27001	5.1	Information security policy	ISO 27001:2015 5.1
ISO 27001	5.2	Information security objectives	ISO 27001:2015 5.2
ISO 27001	5.3	Information security risk assessment	ISO 27001:2015 5.3
ISO 27001	5.4	Information security risk treatment	ISO 27001:2015 5.4
ISO 27001	5.5	Information security risk monitoring	ISO 27001:2015 5.5
ISO 27001	5.6	Information security risk review	ISO 27001:2015 5.6
ISO 27001	5.7	Information security risk communication	ISO 27001:2015 5.7
ISO 27001	5.8	Information security risk reporting	ISO 27001:2015 5.8
ISO 27001	5.9	Information security risk documentation	ISO 27001:2015 5.9
ISO 27001	5.10	Information security risk management	ISO 27001:2015 5.10
ISO 27001	5.11	Information security risk assessment	ISO 27001:2015 5.11
ISO 27001	5.12	Information security risk treatment	ISO 27001:2015 5.12
ISO 27001	5.13	Information security risk monitoring	ISO 27001:2015 5.13
ISO 27001	5.14	Information security risk review	ISO 27001:2015 5.14
ISO 27001	5.15	Information security risk communication	ISO 27001:2015 5.15
ISO 27001	5.16	Information security risk reporting	ISO 27001:2015 5.16
ISO 27001	5.17	Information security risk documentation	ISO 27001:2015 5.17
ISO 27001	5.18	Information security risk management	ISO 27001:2015 5.18
ISO 27001	5.19	Information security risk assessment	ISO 27001:2015 5.19
ISO 27001	5.20	Information security risk treatment	ISO 27001:2015 5.20
ISO 27001	5.21	Information security risk monitoring	ISO 27001:2015 5.21
ISO 27001	5.22	Information security risk review	ISO 27001:2015 5.22
ISO 27001	5.23	Information security risk communication	ISO 27001:2015 5.23
ISO 27001	5.24	Information security risk reporting	ISO 27001:2015 5.24
ISO 27001	5.25	Information security risk documentation	ISO 27001:2015 5.25
ISO 27001	5.26	Information security risk management	ISO 27001:2015 5.26
ISO 27001	5.27	Information security risk assessment	ISO 27001:2015 5.27
ISO 27001	5.28	Information security risk treatment	ISO 27001:2015 5.28
ISO 27001	5.29	Information security risk monitoring	ISO 27001:2015 5.29
ISO 27001	5.30	Information security risk review	ISO 27001:2015 5.30
ISO 27001	5.31	Information security risk communication	ISO 27001:2015 5.31
ISO 27001	5.32	Information security risk reporting	ISO 27001:2015 5.32
ISO 27001	5.33	Information security risk documentation	ISO 27001:2015 5.33
ISO 27001	5.34	Information security risk management	ISO 27001:2015 5.34
ISO 27001	5.35	Information security risk assessment	ISO 27001:2015 5.35
ISO 27001	5.36	Information security risk treatment	ISO 27001:2015 5.36
ISO 27001	5.37	Information security risk monitoring	ISO 27001:2015 5.37
ISO 27001	5.38	Information security risk review	ISO 27001:2015 5.38
ISO 27001	5.39	Information security risk communication	ISO 27001:2015 5.39
ISO 27001	5.40	Information security risk reporting	ISO 27001:2015 5.40
ISO 27001	5.41	Information security risk documentation	ISO 27001:2015 5.41
ISO 27001	5.42	Information security risk management	ISO 27001:2015 5.42
ISO 27001	5.43	Information security risk assessment	ISO 27001:2015 5.43
ISO 27001	5.44	Information security risk treatment	ISO 27001:2015 5.44
ISO 27001	5.45	Information security risk monitoring	ISO 27001:2015 5.45
ISO 27001	5.46	Information security risk review	ISO 27001:2015 5.46
ISO 27001	5.47	Information security risk communication	ISO 27001:2015 5.47
ISO 27001	5.48	Information security risk reporting	ISO 27001:2015 5.48
ISO 27001	5.49	Information security risk documentation	ISO 27001:2015 5.49
ISO 27001	5.50	Information security risk management	ISO 27001:2015 5.50
ISO 27001	5.51	Information security risk assessment	ISO 27001:2015 5.51
ISO 27001	5.52	Information security risk treatment	ISO 27001:2015 5.52
ISO 27001	5.53	Information security risk monitoring	ISO 27001:2015 5.53
ISO 27001	5.54	Information security risk review	ISO 27001:2015 5.54
ISO 27001	5.55	Information security risk communication	ISO 27001:2015 5.55
ISO 27001	5.56	Information security risk reporting	ISO 27001:2015 5.56
ISO 27001	5.57	Information security risk documentation	ISO 27001:2015 5.57
ISO 27001	5.58	Information security risk management	ISO 27001:2015 5.58
ISO 27001	5.59	Information security risk assessment	ISO 27001:2015 5.59
ISO 27001	5.60	Information security risk treatment	ISO 27001:2015 5.60
ISO 27001	5.61	Information security risk monitoring	ISO 27001:2015 5.61
ISO 27001	5.62	Information security risk review	ISO 27001:2015 5.62
ISO 27001	5.63	Information security risk communication	ISO 27001:2015 5.63
ISO 27001	5.64	Information security risk reporting	ISO 27001:2015 5.64
ISO 27001	5.65	Information security risk documentation	ISO 27001:2015 5.65
ISO 27001	5.66	Information security risk management	ISO 27001:2015 5.66
ISO 27001	5.67	Information security risk assessment	ISO 27001:2015 5.67
ISO 27001	5.68	Information security risk treatment	ISO 27001:2015 5.68
ISO 27001	5.69	Information security risk monitoring	ISO 27001:2015 5.69
ISO 27001	5.70	Information security risk review	ISO 27001:2015 5.70
ISO 27001	5.71	Information security risk communication	ISO 27001:2015 5.71
ISO 27001	5.72	Information security risk reporting	ISO 27001:2015 5.72
ISO 27001	5.73	Information security risk documentation	ISO 27001:2015 5.73
ISO 27001	5.74	Information security risk management	ISO 27001:2015 5.74
ISO 27001	5.75	Information security risk assessment	ISO 27001:2015 5.75
ISO 27001	5.76	Information security risk treatment	ISO 27001:2015 5.76
ISO 27001	5.77	Information security risk monitoring	ISO 27001:2015 5.77
ISO 27001	5.78	Information security risk review	ISO 27001:2015 5.78
ISO 27001	5.79	Information security risk communication	ISO 27001:2015 5.79
ISO 27001	5.80	Information security risk reporting	ISO 27001:2015 5.80
ISO 27001	5.81	Information security risk documentation	ISO 27001:2015 5.81
ISO 27001	5.82	Information security risk management	ISO 27001:2015 5.82
ISO 27001	5.83	Information security risk assessment	ISO 27001:2015 5.83
ISO 27001	5.84	Information security risk treatment	ISO 27001:2015 5.84
ISO 27001	5.85	Information security risk monitoring	ISO 27001:2015 5.85
ISO 27001	5.86	Information security risk review	ISO 27001:2015 5.86
ISO 27001	5.87	Information security risk communication	ISO 27001:2015 5.87
ISO 27001	5.88	Information security risk reporting	ISO 27001:2015 5.88
ISO 27001	5.89	Information security risk documentation	ISO 27001:2015 5.89
ISO 27001	5.90	Information security risk management	ISO 27001:2015 5.90
ISO 27001	5.91	Information security risk assessment	ISO 27001:2015 5.91
ISO 27001	5.92	Information security risk treatment	ISO 27001:2015 5.92
ISO 27001	5.93	Information security risk monitoring	ISO 27001:2015 5.93
ISO 27001	5.94	Information security risk review	ISO 27001:2015 5.94
ISO 27001	5.95	Information security risk communication	ISO 27001:2015 5.95
ISO 27001	5.96	Information security risk reporting	ISO 27001:2015 5.96
ISO 27001	5.97	Information security risk documentation	ISO 27001:2015 5.97
ISO 27001	5.98	Information security risk management	ISO 27001:2015 5.98
ISO 27001	5.99	Information security risk assessment	ISO 27001:2015 5.99
ISO 27001	6.00	Information security risk treatment	ISO 27001:2015 6.00

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

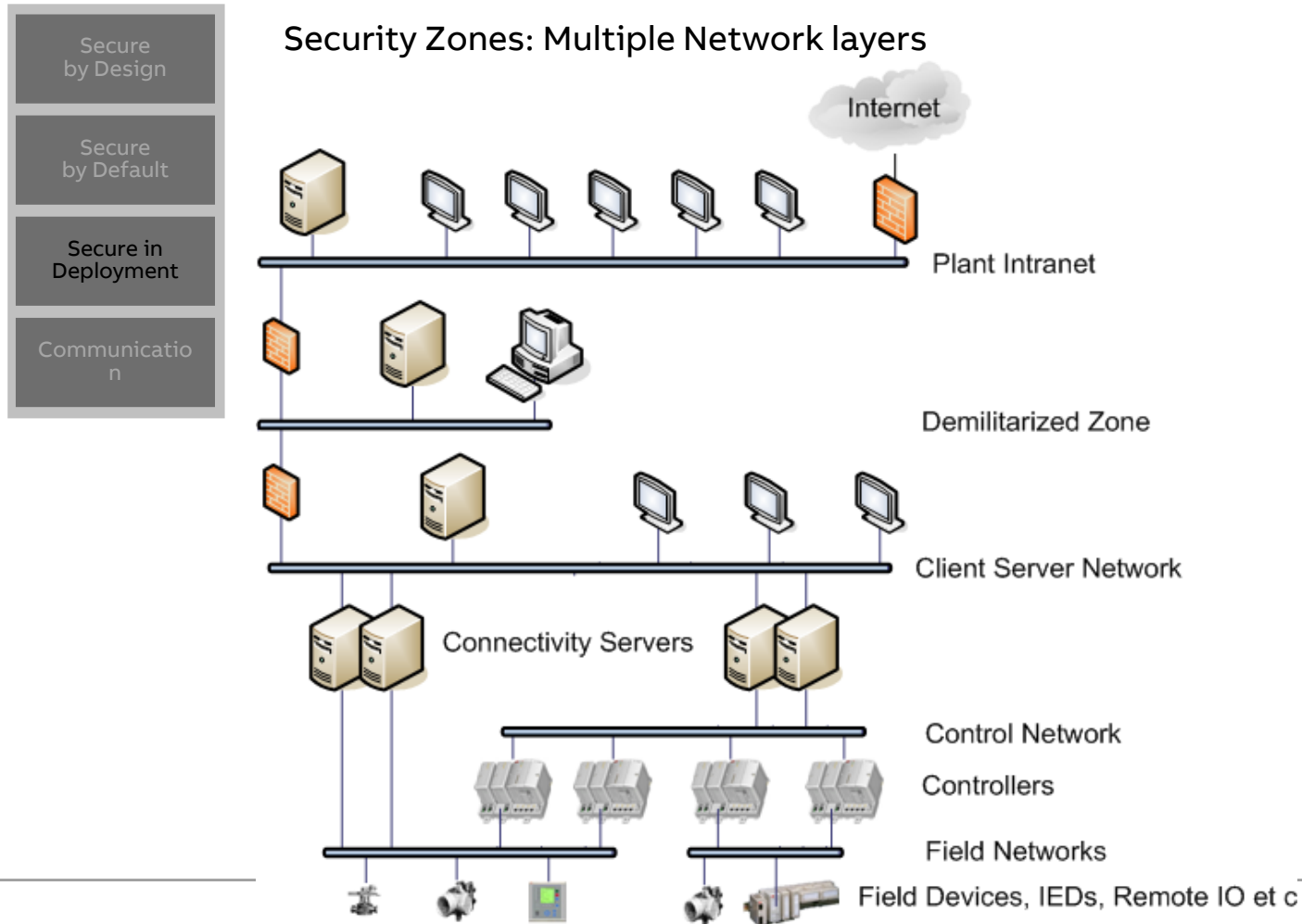
- Network segregation for different security levels
- Network redundancy
- Logical separation through Firewall
- Secure communication

Access Control

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

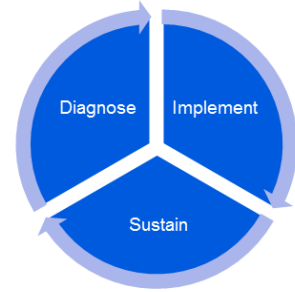
Secure in Deployment

Secure Architecture: Security Zones



Cyber Security Life Cycle Management

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



Diagnose

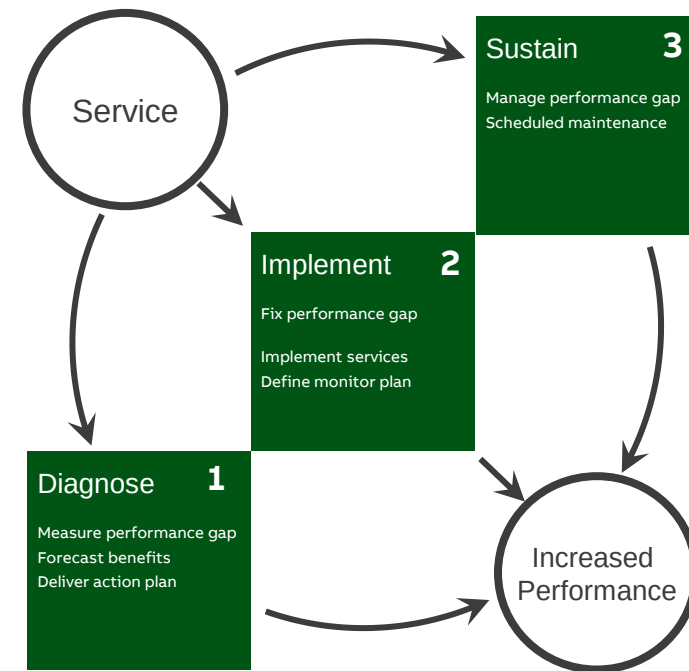
- Measure performance gap
- Forecast benefits
- Deliver action plan

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