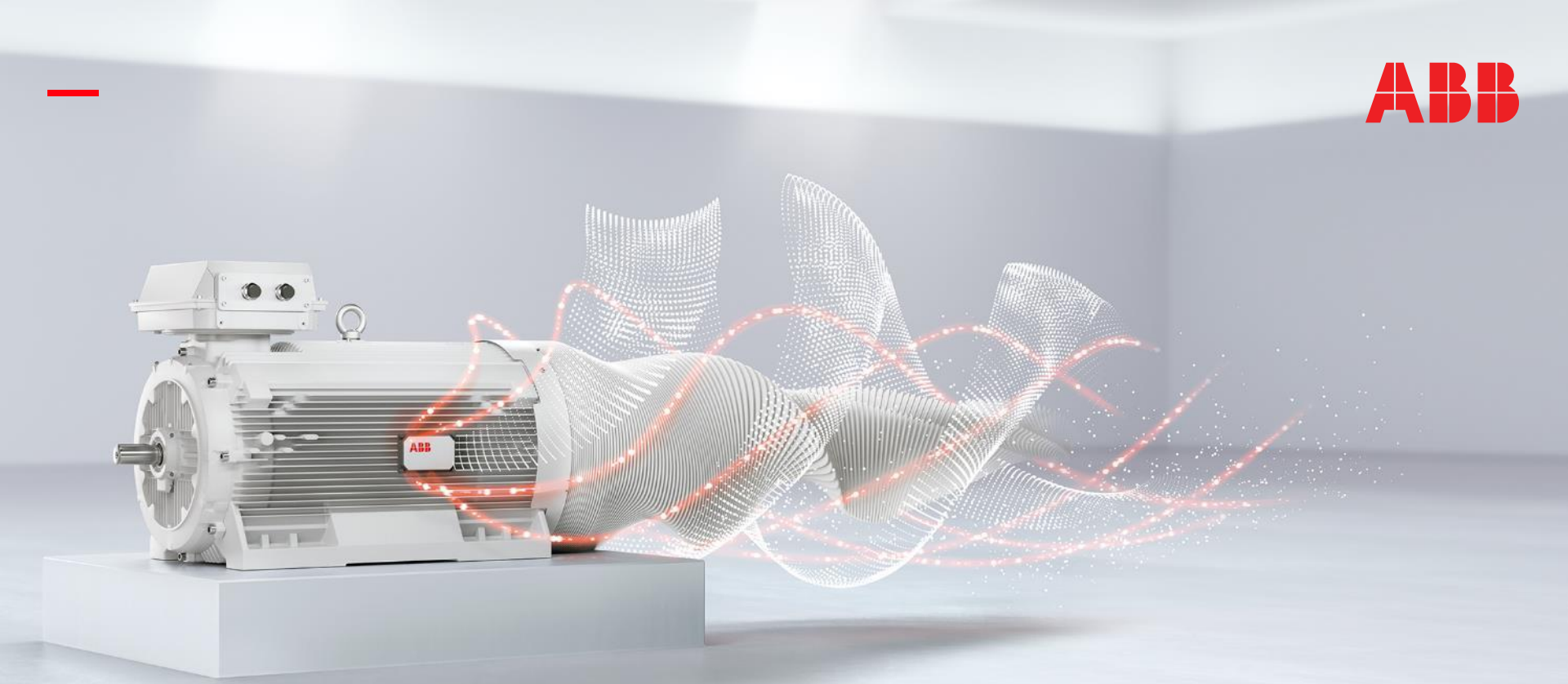


NEK ELSIKKERHETSKONFERANSE, 22. NOV 2017

Cyber Security – med vekt på industrielle løsninger

Managing Cyber Security in Power and Automation

Judith Rossebø, Cyber Security Specialist, Member of NK65

Focus of presentation

Topics covered

- Cyber Security in Power and Automation
  - Why is Cyber Security an Issue?
  - Cyber Security Trends
- What are the Challenges?
- How Should the Challenges be Addressed?
- Industry Approach - ISA/IEC 62443 Standards

Cyber security in power and automation

Why is cyber security an issue?

Power and Automation Today

Modern automation, protection, and control systems are highly specialized IT systems

- Leverage commercial off the shelf IT components
- Use standardized, Ethernet-based communication protocols
- Are distributed and highly interconnected
- Use mobile devices and storage media
- Based on software (> 50% of manufacturers offerings are software-related)
- IT/OT Convergence

Cyber Security Issues

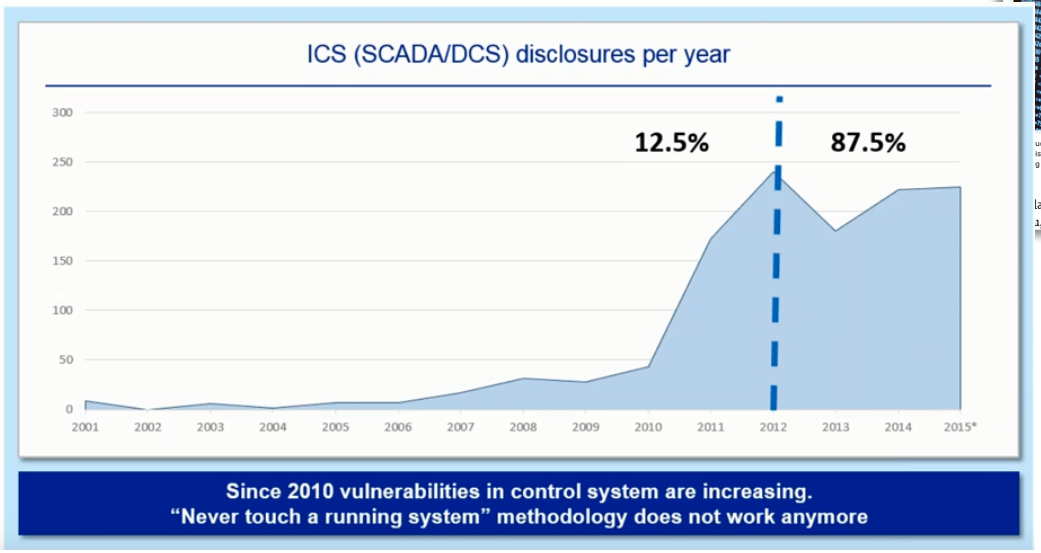
- Increased attack surface as compared to legacy, isolated systems
- Communication with external (non-OT) systems
- Attacks from/over the IT world

Attacks are real and have an actual safety, health, environmental, and financial impact

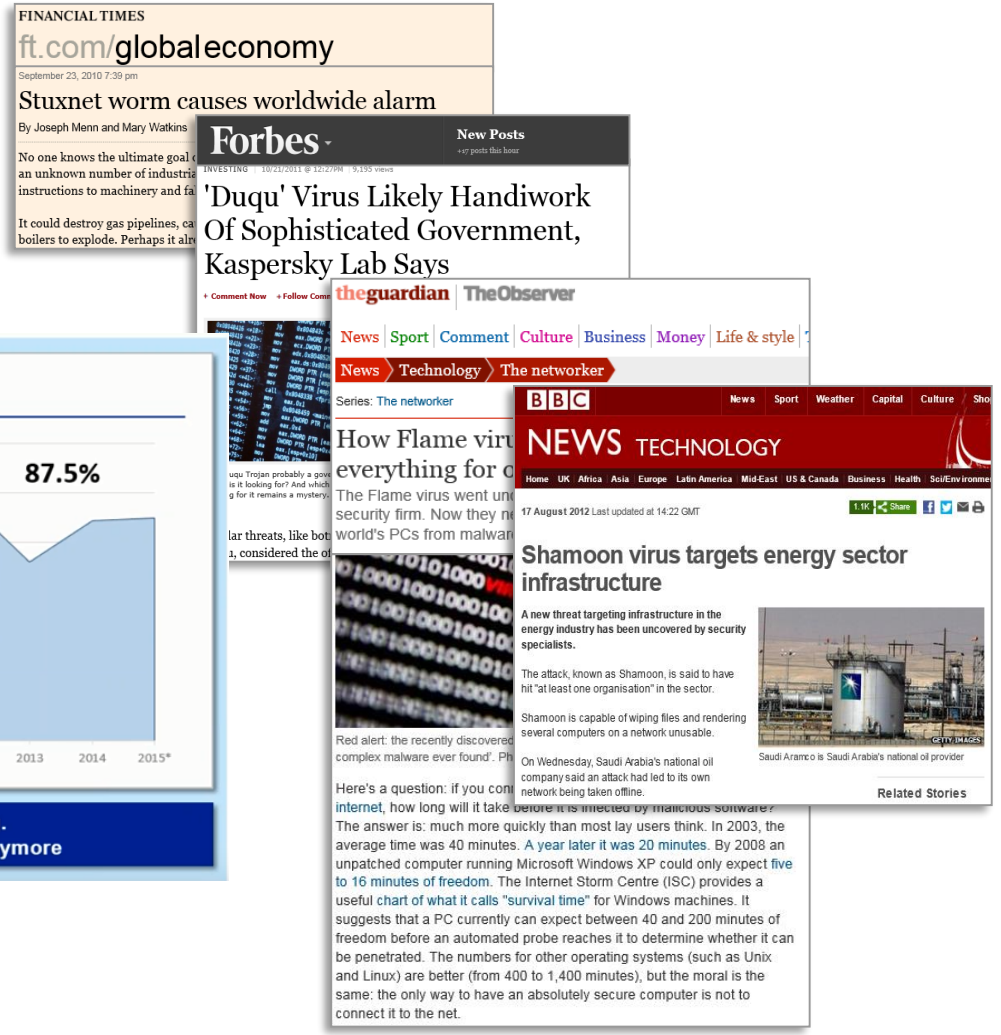
Cyber security in power and automation

Trends

Examples of recent events



Source: https://scadahacker.com/



Images: www.ft.com, www.forbes.com, www.theguardian.com, www.bbc.com

Cyber Attack on the Ukrainian Electricity Grid

Example in 2015

CNET › Security › Ukraine blackout is a cyberattack milestone

Ukraine blackout is a cyberattack milestone

Hundreds of thousands of homes were left in the dark in what security experts say was a first for hackers with ill intent.

Security

by **Katie Collins**

January 5, 2016 1:55 PM PST

@katiecollins

Some cyberattacks are about stealing data, some about monkeying with someone else's machines. This one left innocent bystanders in the dark.

A massive power outage in Ukraine last month has been attributed to hackers targeting the electricity grid with malware. Security researchers say it is the first known instance of a blackout being credibly linked to the actions of malicious hackers.

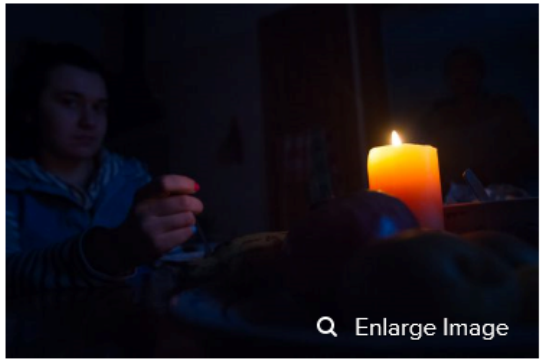
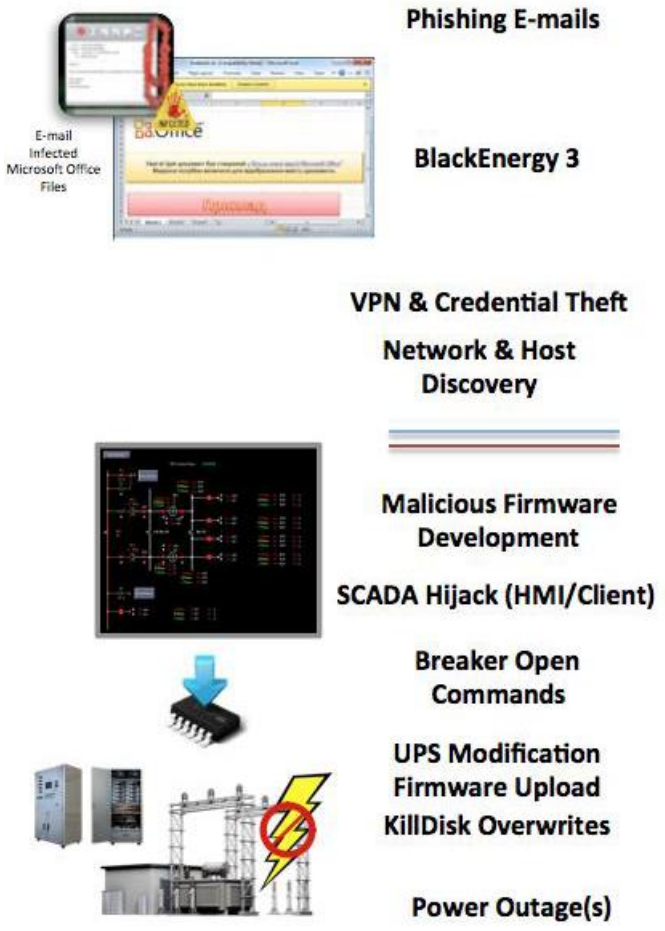


Image:www.cnet.com

Attack on the Ukrainian Electricity Grid

Technical components involved in the attack:

- Spear phishing to get malware on workstation(s) in the office network
- Theft of user credentials using malware on workstation in the IT domain (office network)
- Access SCADA workstation from IT domain (office network) over VPN
- Use of standard SCADA dialogues in SCADA workstation
- Open breakers at multiple substations to disconnect power
- Wipe disks using Killdisk
  Modify UPS to interfere with restoration efforts
  Denial of service on Call- Centers



Reference: SANS ICS, E-ISAC, March, 2016

What are the Main Cyber Security Challenges ?

Challenges

Organizational

Risk Management

Awareness

Competence Management

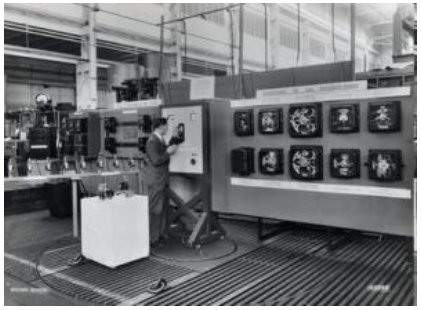
Disruptive Changes

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

Challenges

Technical

Installed Base



Sustaining Security

Situational Awareness

Heterogeneity

Compliance

Vulnerabilities

Images: www.zazzle.co.nz, www.zoho.com, blog.monitorscout.com, www.leadthefish.com, nl.123rf.com, www.ccure.it

How Should the Challenges be Addressed?

How should the challenges be addressed?

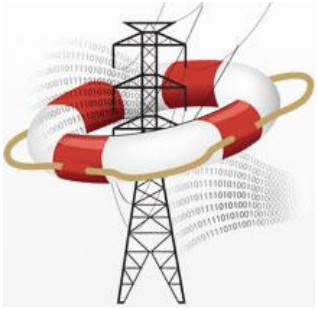
4 key questions should be addressed:

Can we really defend ourselves?

Do we know our infrastructure and systems?

Can we identify potentially malicious activities?

Can we recover from any incident?



Images: www.techieapps.com, technorati.com, www.calibersecurity.com, cert.org

How should the challenges be addressed?

Proper preparation:

Requires a change from all of us!

Make an inventory of what you have

Know the behavior of your infrastructure and systems

Compare your actual with your baseline

Monitor vulnerability disclosures

Patch your systems and stay up to date

Images: howstuffworks.com blog.optimizely.com lisagroup.com.au dhs.org cve.mitre.org securityfocus.com www.marketingzen.com

Industial Approach – IEC 62443 Standardization

Cyber Security Standards

ISA/IEC 62443 : Industrial Automation and Control System Security

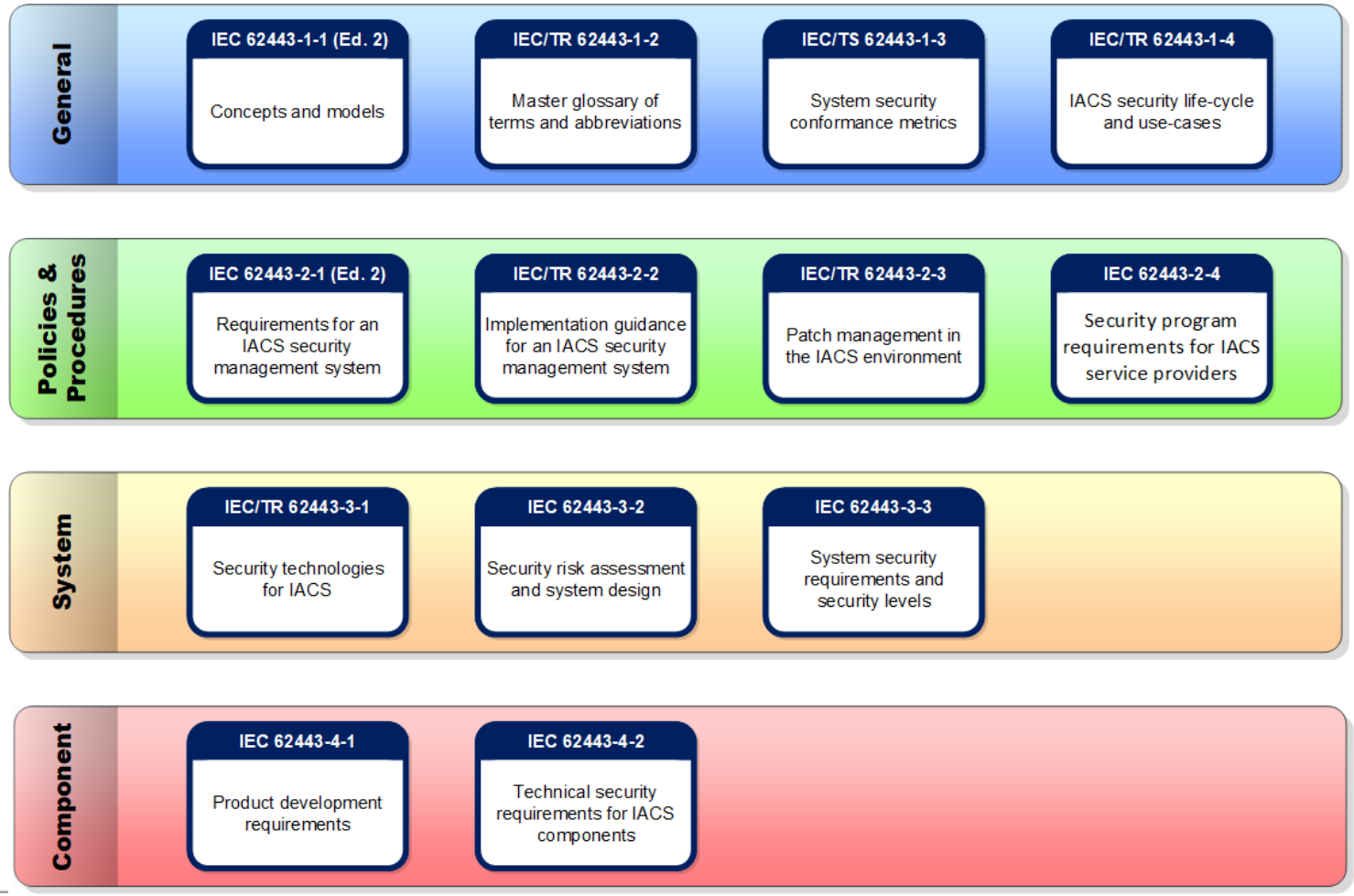


Image: ISA 99 Committee

Zones and Conduits

A network & system segmentation technique:

- Prevents the spread of an incident
- Provides a front-line set of defenses
- The basis for risk assessment in system design

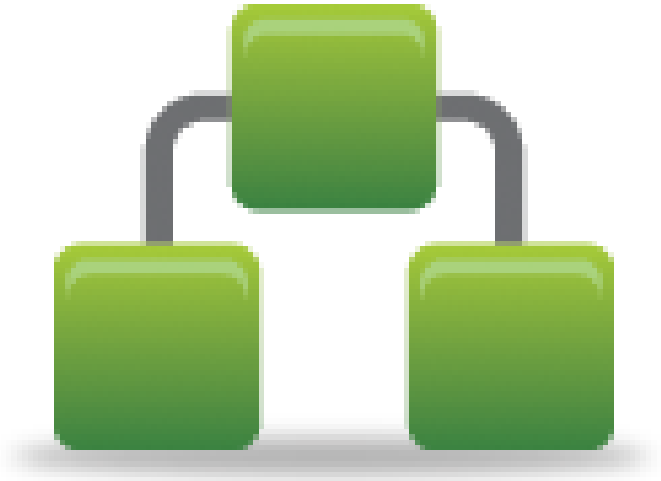


Image: ISA-62443-1-1, 2nd Edition (Under development)

Foundational Requirements

System and component capability requirements

- FR 1 – Identification & authentication control
- FR 2 – Use control
- FR 3 – System integrity
- FR 4 – Data confidentiality
- FR 5 – Restricted data flow
- FR 6 – Timely response to events
- FR 7 – Resource availability

Image: ISA-62443-1-1, 2nd Edition (Under development)

Security Levels

For component and system capabilities

Protection against attacks:

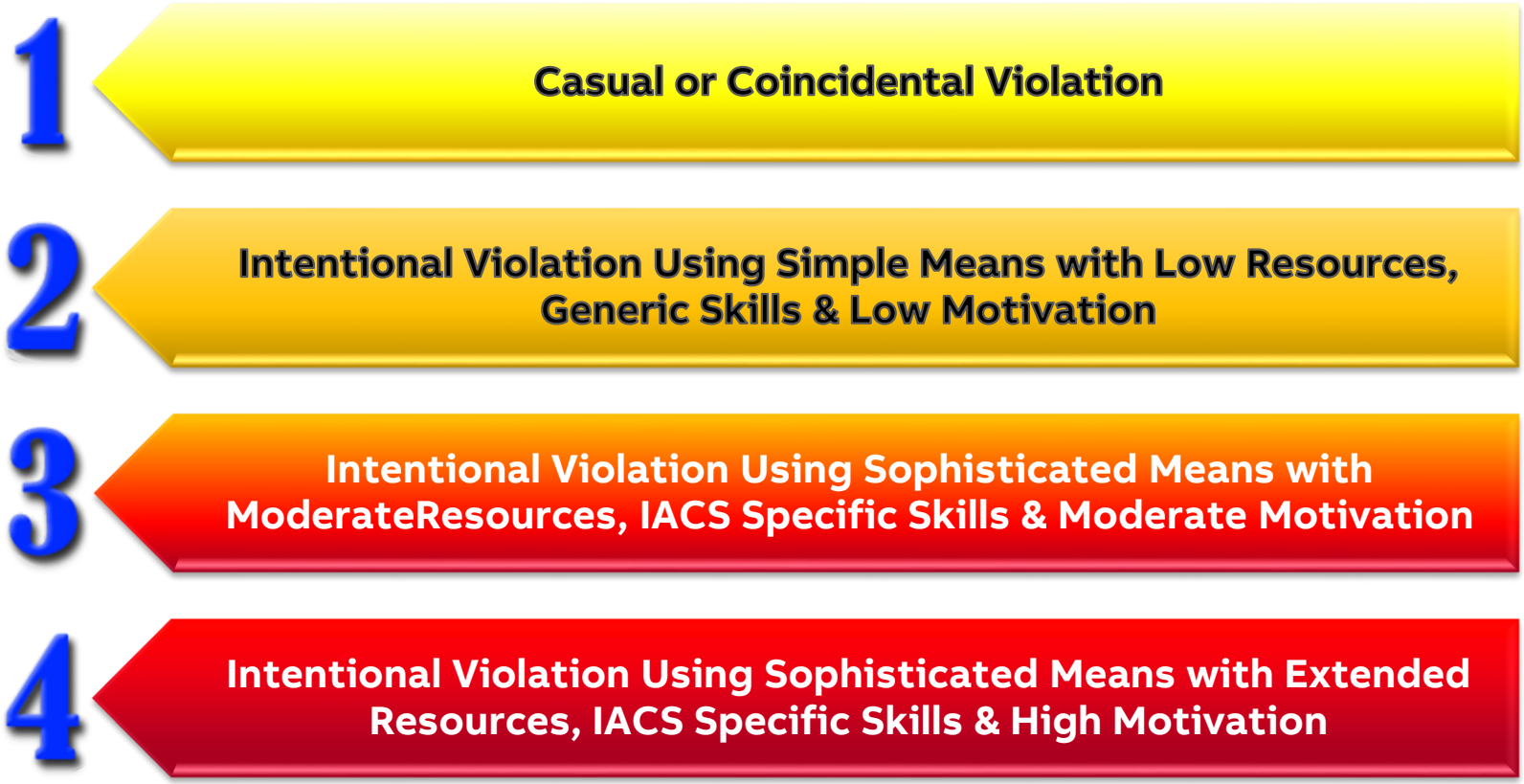


Image: ISA-62443-1-1, 2nd Edition (Under development)

Product supplier use of IEC 62443

Part 4-1 Product security development life-cycle requirements

- Secure development processess integrated with formal development process (e.g. ISO 9001 process)
- Security requirements for processes used during product development and support by a product supplier. One of the required development processes is to define security requirements for the product.

Supporting standards for the definition of product security requirements

- Part 3-3 System security requirements and security levels
  - Requirements for security capabilities of control systems taken as a whole
- Part 4-2 Technical security requirements for IACS components
  - Requirements for security capabilities of components used in control systems

Service providers use of IEC 62443

Part 2-4 Requirements for control system solution providers

- Requirements for integrating, installing, configuring and maintaining the security of the industrial control system

Areas covered:

- Staffing, network security, solution hardening, data protection, configuration management, event management, account management, patch management backup/restore, wireless, SIS integration with BPCS, malware protection, remote access
- Process inputs:
  - Product manuals required by Part 4-1
  - Product capabilites required by Parts 3-3 and 4-2
  - Security policies

Asset owners use of IEC 62443

- Part 2-1 Security program requirements for asset owners
  - Security requirements for control system installations
  - Integrates with Parts 3-3, 2-4 and 4-2
  - Places requirements on control systems that can support supply chain/procurement of devices/components, control systems and services
- Part 3-2 Security risk assessment, system partitioning and security levels
  - Process for cyber security risk assessment for defining a secure control system architecture
  - Partitioning into Zones and Conduits
- Part 1-5 Protection Levels (under development)
  - Addresses evaluation of a control system security program
  - Protection Levels as combination of Security Levels and Maturity Levels

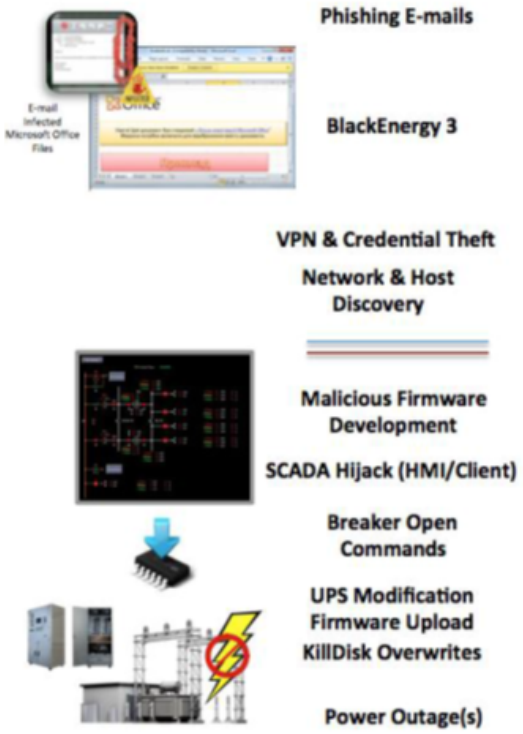
Real Life Example

Application of 62443-3-3 to the Ukrainian Case

Which Security Level would have been required to prevent the attack?

(Based on an analysis of which security controls were missing)

- Spear phishing to get malware on workstation(s) in the office network
- Theft of user credentials using malware on workstation in the IT domain (office network)
- Access SCADA workstation from IT domain (office network) over VPN
- Use of standard SCADA dialogues in SCADA workstation
- Open breakers at multiple substations to disconnect power
- Wipe disks using Killdisk
  Modify UPS to interfere with restoration efforts
  Denial of service on Call- Centers



References: SANS ICS, E-ISAC, March, 2016, and
«A forensic analysis based on ISA/IEC 62443 of the cyber attacks on the Ukrainian power grids»,
by Patrice Bock, Jean-Pierre Hauet, Romain Francoise, and Robert Foley, November, 2016

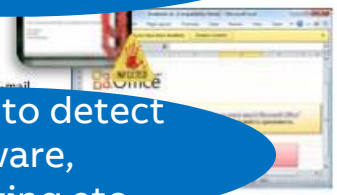
Cyber Attack on the Ukrainian Electricity Grid

Which 62443 security controls were missing?

Spear phishing to get malware on workstation(s) in the office network

Awareness training

Phishing E-mails



Theft of user credentials using malware on workstation in the IT domain (office network)

Anti-virus to detect malware, whitelisting etc.

BlackEnergy 3

VPN & Credential Theft

Access SCADA workstation from IT domain (office network) over VPN

Security monitoring of the networks

Network & Host Discovery

Use of standard SCADA dialogues in SCADA workstation

Operator control to terminate remote connections

Malicious Firmware Development

SCADA Hijack (HMI/Client)

Open breakers at multiple substations to disconnect power

Adequate Backup Policy

Breaker Open Commands

UPS Modification
Firmware Upload
KillDisk Overwrites

Wipe disks using Killdisk
Modify UPS to interfere with restoration efforts
Denial of service on Call- Centers

Power Outage(s)

Cyber Attack on the Ukrainian Power Grid

Which 62443 security controls were missing?

- FR 1 – Identification & authentication control
  - SR 1.13 - Lack of restrictions on access from untrusted networks, no explicit access aproval required
- FR 2 – Use control
  - SR 2.4 – Lack of protection made it possible to transfer malware to several systems on the OT network
  - SR2.6 – It was not possible for the Operator to terminate the attackers remote connection
- FR 3 – System integrity
  - SR3.3 – No malicious code protection (no anti-virus software on the systems)
- FR 4 – Data confidentiality - Ok
- FR 5 – Restricted data flow – OK, FWs restricted data flow
- FR 6 – Timely response to events
  - SR 6.2 – Lack of Network monitoring allowed the attackers to scan the networks for weeks…
- FR 7 – Resource availability
  - SR 7.4 – Disks were erased (Kill-disk), lack of adequate backup policy

Reference: A forensic analysis based on ISA/IEC 62443 of the cyber attacks on the Ukrainian power grids, by Patrice Bock, Jean-Pierre Hauet, Romain Francoise, and Robert Foley

Any Questions?