DNV

SMART GRID FORUMS

Understanding IEC 62443

Aligning IEC 62443 concepts, frameworks and controls with the cybersecurity risk of your power grid organisation

Webinar: 16:00-17:00 CET

Wednesday 27th October 2021

Crowdcast Webinar Platform

Christian Nerland, Mirnes Alic
DNV Cyber Security, Norway

27 October 2021

Understanding IEC 62443 - Introduction

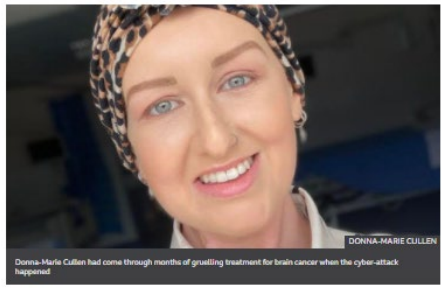
1. Increasing threat landscape
2. Cyber security for the Real world
3. Holistic Cyber Security
4. Starting early will pay-off
5. Recommended practices

Christian Nerland, *MSc, MBA*
Business Development Director
DNV Cyber Security

christian.nerland@dnv.com
+47 913 93 937

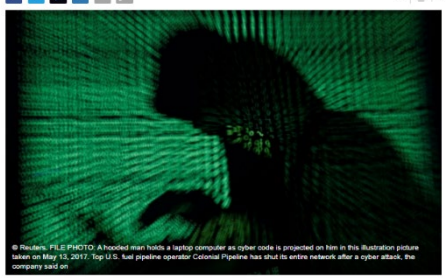
Increasing threat landscape – Impact is getting real..

HSE cyber-attack: Irish health service still recovering months after hack



Donna-Marie Cullen had come through months of gruelling treatment for brain cancer when the cyber-attack happened

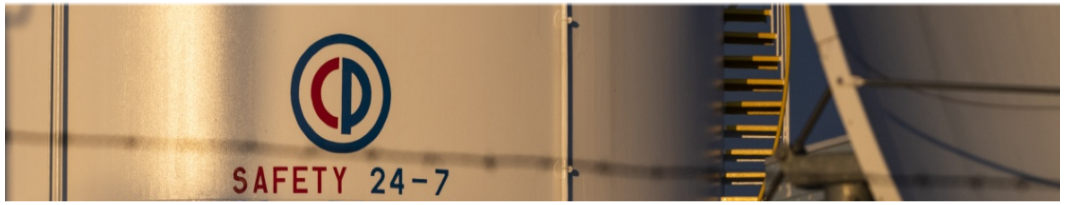
Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed



Technology

SolarWinds says dealing with hack fallout cost at least $18 million

By Raphael Satter



Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra

4. juni 2021, 21:58 CEST

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

LISTEN TO ARTICLE

▶ 4:58

SHARE THIS ARTICLE

Share

Tweet

Post

Email

From the Apple scoop machine

Be the first to know what's next in tech from Mark Gurman's Power On newsletter.

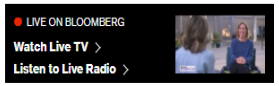
Enter your email

Sign Up

Bloomberg may send me offers and promotions.

By submitting my information, I agree to the Privacy Policy and Terms of Service.

The hack that took down the largest fuel pipeline in the U.S. and led to



CYBER SECURITY FOR THE REAL WORLD

27 October 2021

The OT/ CPS maturity journey

60% of orgs. are here

30% of orgs. are here

Decision point

10% of orgs. are here

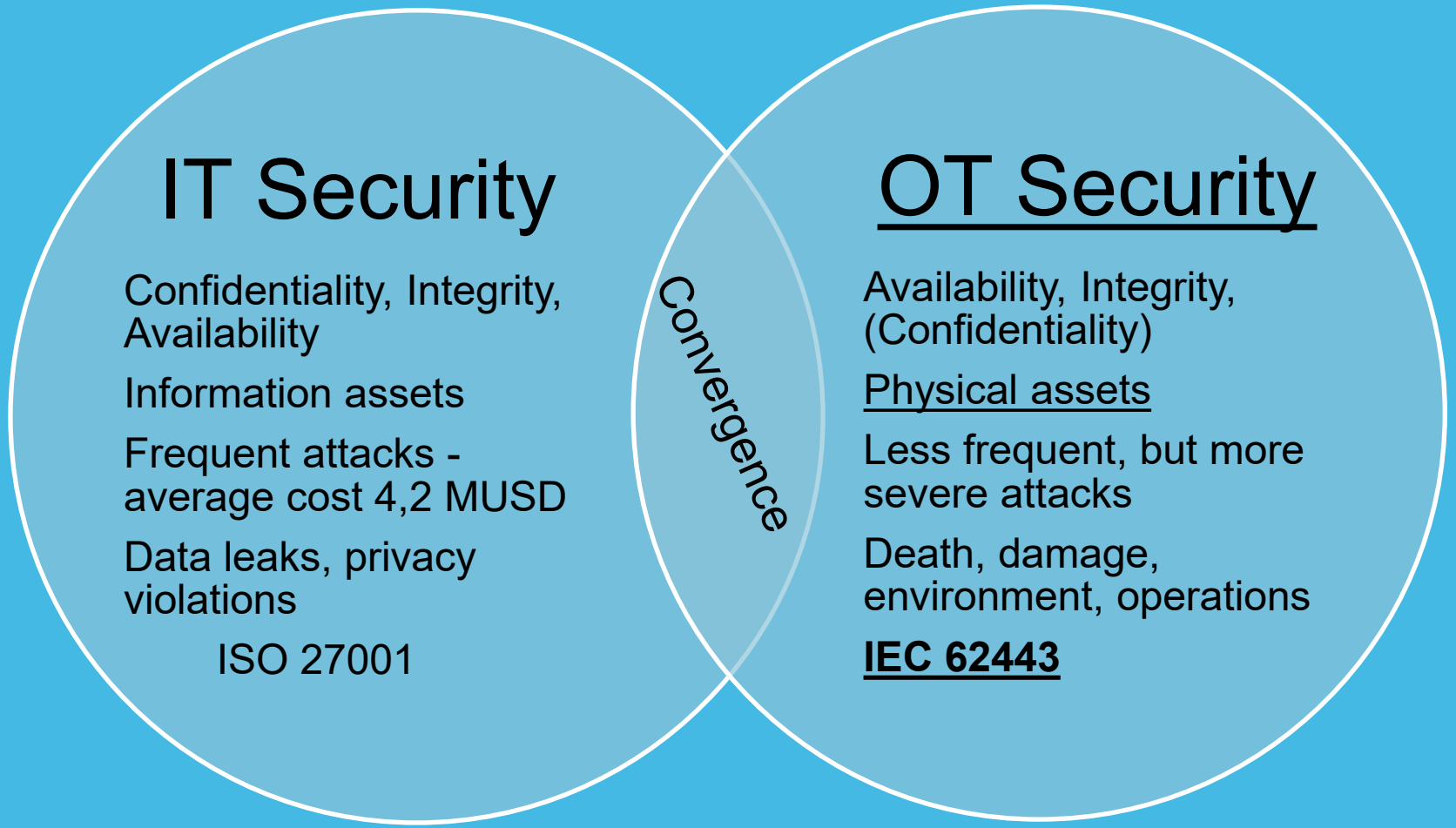
Phase 1	Phase 2	Phase 3	Phase 4	Phase 5	Phase 6
Awareness	**Outreach / asset discovery / network topology mapping**	**Understanding the severity**	**Firefighting**	**Integration**	**Optimization**
• Driven by: • Breach • Board of Directors / C-Suite • Government Bulletins • Government Intervention	• Internet outreach to understand current OT security governance • Proof of concept with OT security platform vendors	• Unmanaged devices connecting everywhere! • OT network isn't segmented! • Open ports everywhere! • OEM remoting in without a policy! • Windows XP everywhere! • Cybersecurity, physical security, supply chain security, HS&E and product security teams do not talk!	• Steering Committee/Org realignment • Focus on high value assets • Deployment of best POC solution • Network segmentation • Patching or compensating controls	• Creation of a Chief Security Officer to converge siloed security disciplines • OT security platform data feed to SIEM/SOAR/central SOC • Best of breed policy updates	• Shift to ORM (Operational Resilience Management) • Realization that a lot of the OT data gathered for security purposes also have operational, engineering, maintenance, compliance, procurement or C-suite reporting value

Source. Gartner 01.25.21

Increasing OT Robustness

DNV

Holistic cyber security



People | **Process** | **Technology**

Cyber Security – starting early will pay off!

- **Early involvement on Cyber Security is key**
  - To identify and clarify consequences for concept and early FEED decisions
  - To make sure relevant requirements are included towards all stakeholders

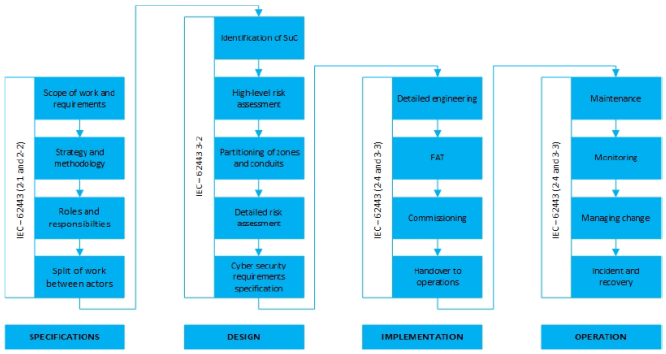
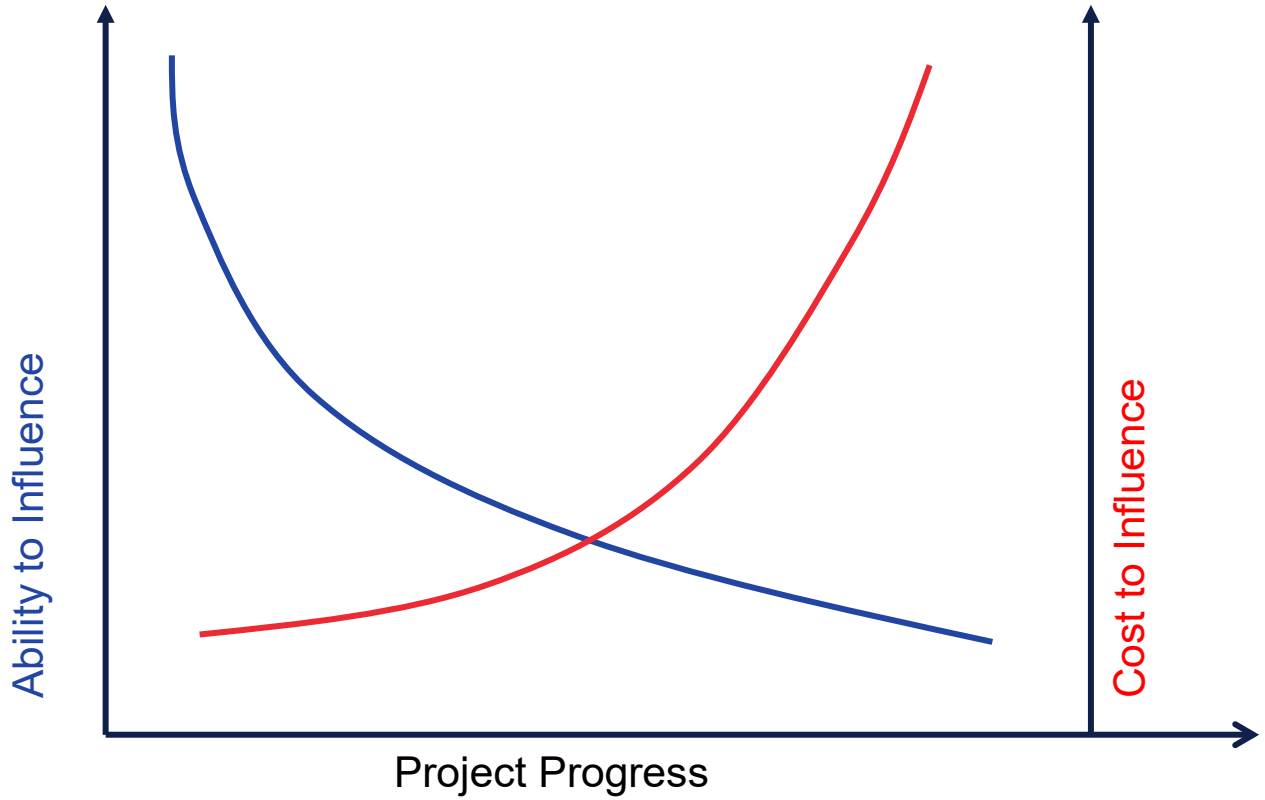
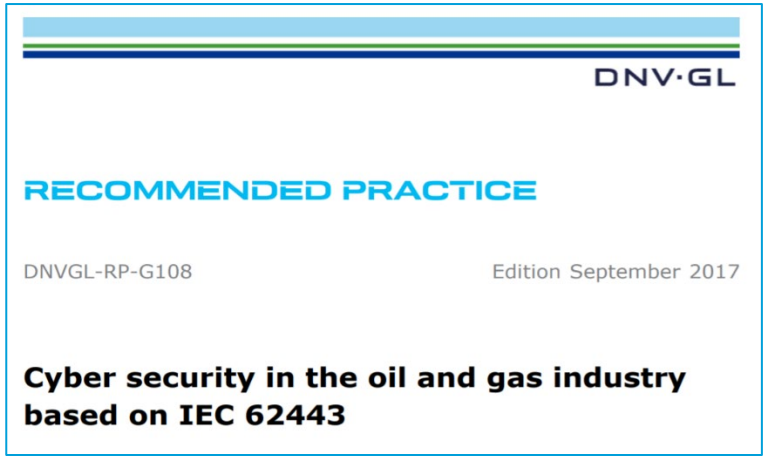


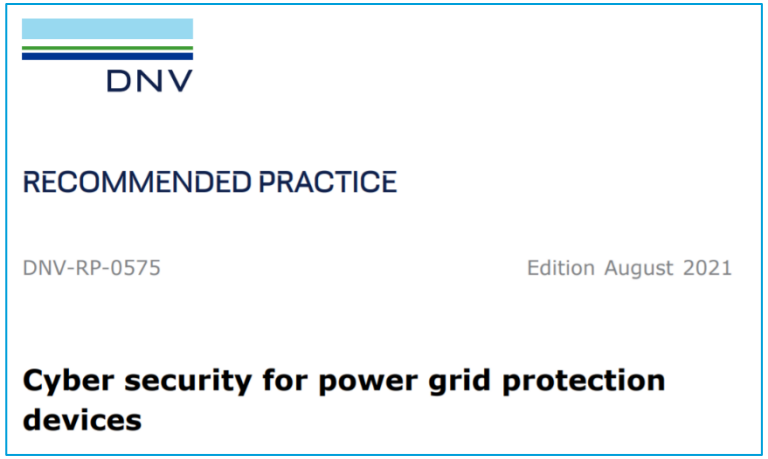
Figure 4-3 Cyber security during the substation lifecycle



Source: DNV-RP-0575 - Cyber security for power grid protection devices

Recommended practices



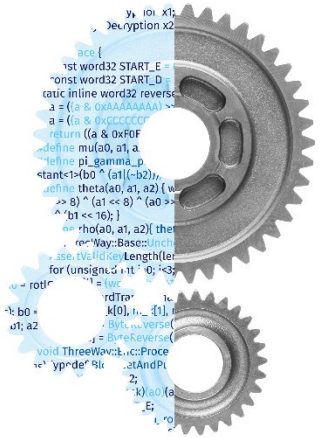


DNV RP G-108	Cyber security in the oil and gas industry based on IEC 62443 https://rules.dnv.com/docs/pdf/DNV/RP/2017-09/DNVGL-RP-G108.pdf
DNV RP 0576	Cyber security for power grid protection devices https://rules.dnv.com/docs/pdf/DNV/RP/2021-08/DNV-RP-0575.pdf
Energy Academy	Two-day training course to improve the cyber security of your OT network by using IEC 62351 devices and implementations. https://www.dnv.nl/training/training-course-on-cyber-security-189292

Applying IEC 62443

Know your cyber risks

Build a powerful force of defence



Win stakeholder support

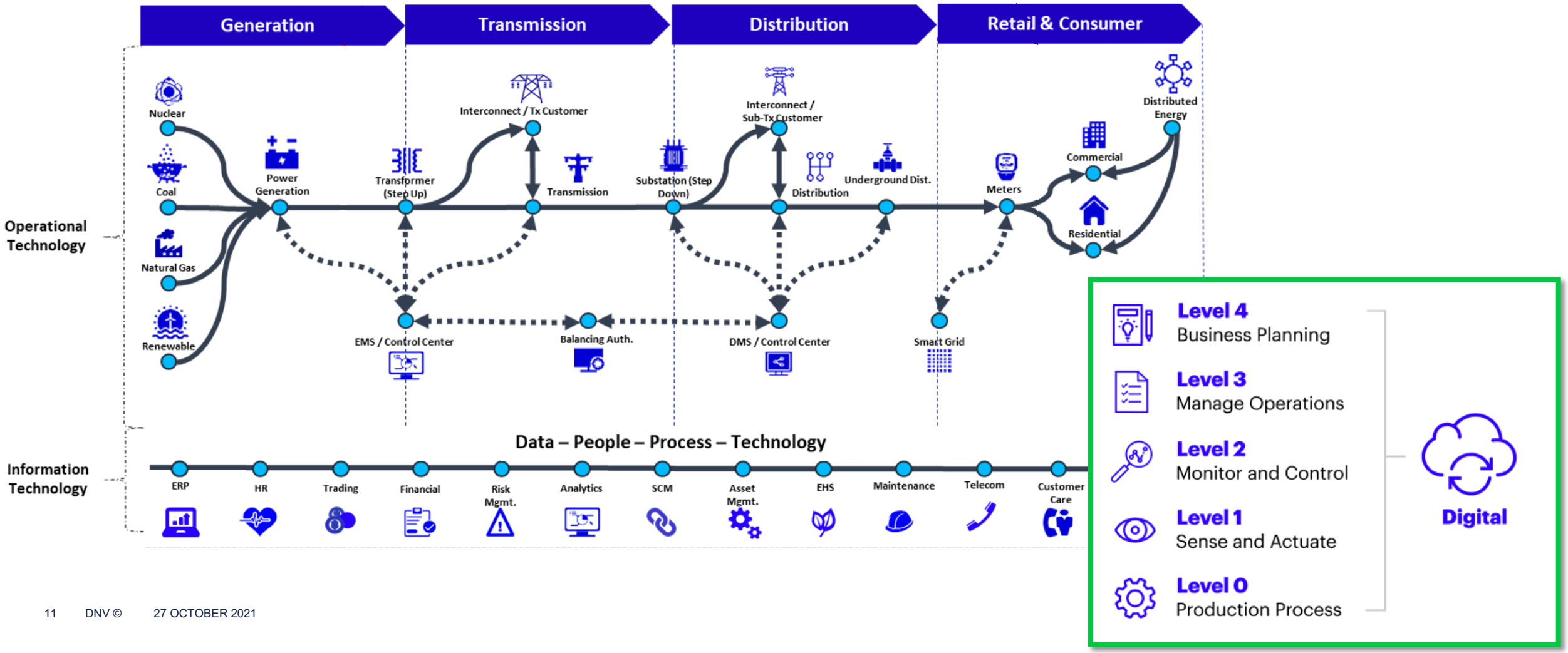
We will talk about …

- Exposure in Power Grid
- Applying IEC 62443
- Case study: Ukranian Power Grid

Mirnes Alic, *MSc*
GICSP, CISSP, GPEN
Cyber Security Consultant
DNV Cyber Security

Mirnes.Alic@dnv.com
+47 96 805 736

The Exposure



Where to apply cyber security in utilities/grid operations

C = Confidentiality
I = Integrity
A = Availability

S = Safety
A = Availability
I = Integrity
C = Confidentiality

Office

IT

IT for OT

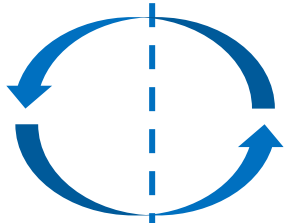
Grid/Plant Operations

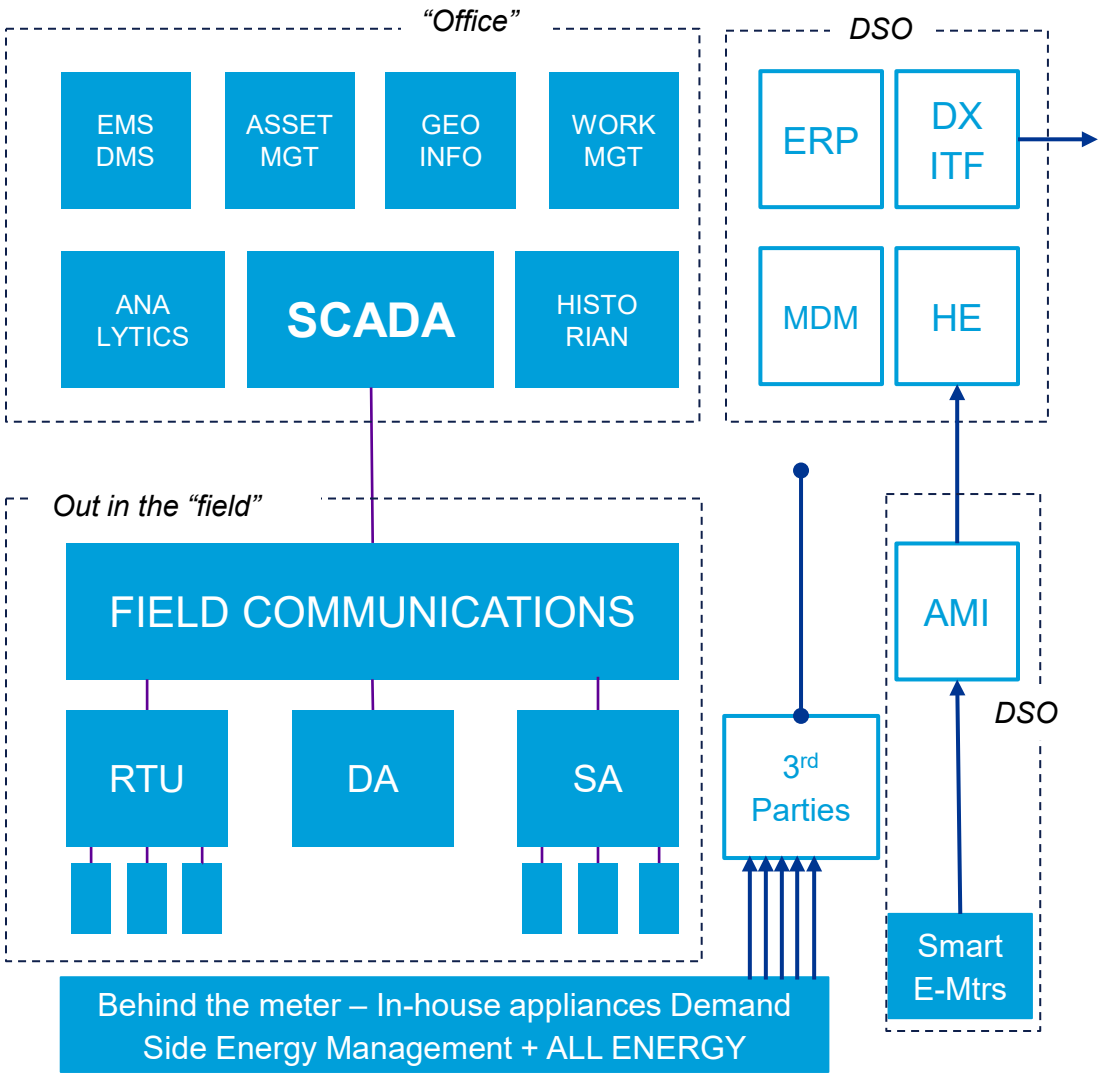
Wireless

Cloud

OT + "IoT"

Grid/Plant Processes





Applying utility cyber security standards

IT Systems
ISO 27001(x)

OT Systems
IEC 62443

Process Controls
IEC 62443-2-1

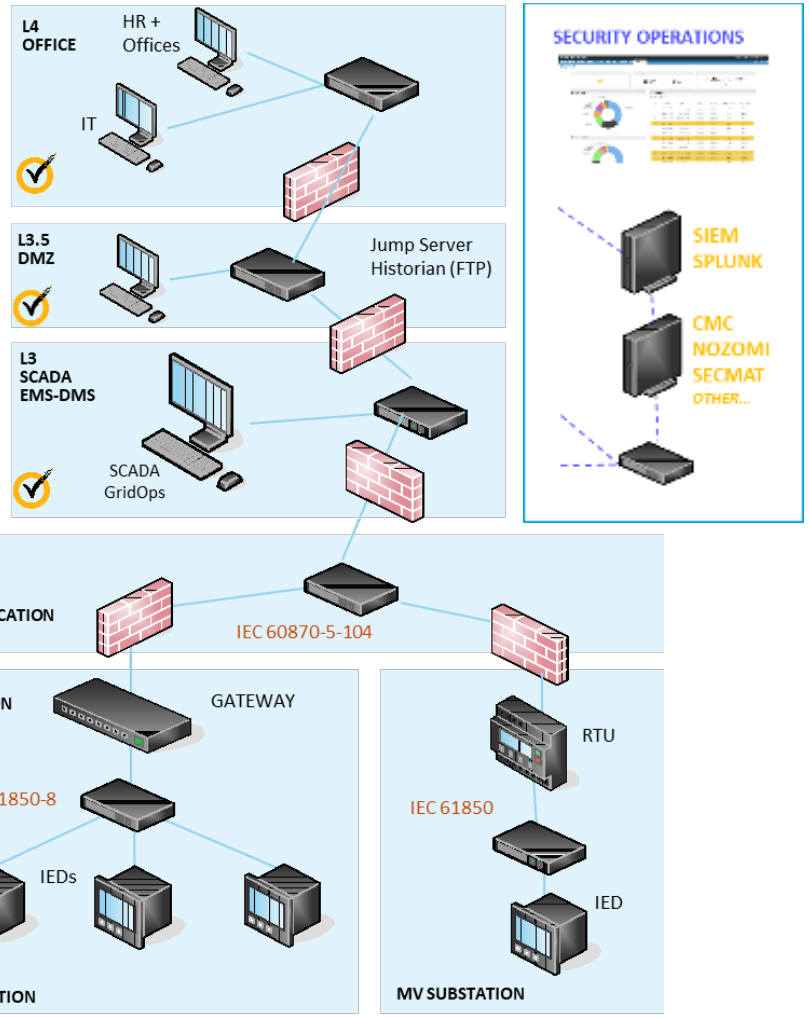
Tech. Security Levels
IEC 62443-3-3

Prot. + IED Security
IEC 62351

Grid Operations
Network/System Operators – Utilities
Portfolio Managers – Power Producers

SCADA + GridOps Systems
Secure System Architectures
Remote Control – Remote Access

SCADA Protocols
ICCP
IEC-101/104
IEC 61850
IED's



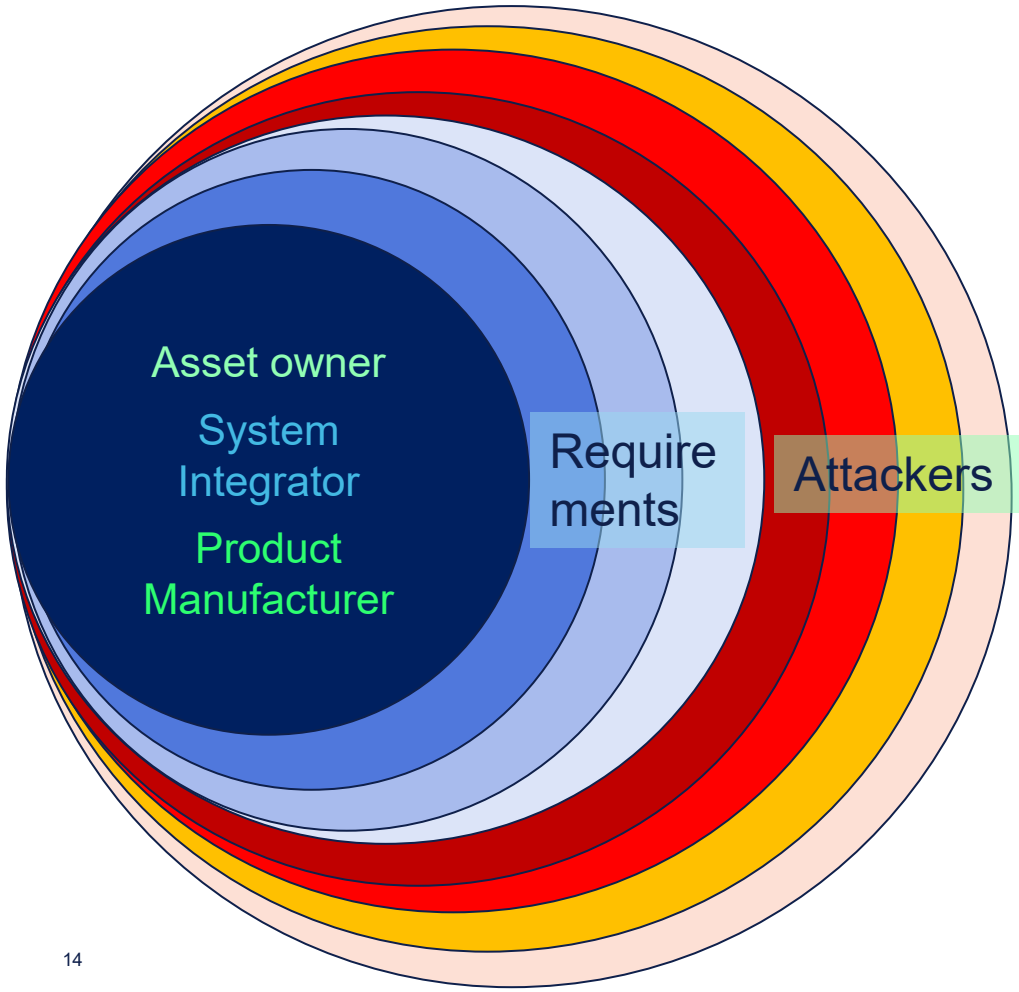
Add Power Generators:

- Large – DCS + SCADA connected to TSO
- Windmills (parks) – DER
- Solar (fields)

Add Smart Metering + Comms Infra

Add ICCP – TSO-TSO-RSC + DSO-TSO

IEC 62443



Asset owner

System Integrator

Product Manufacturer

Requirements/Controls

SL 1 2 3 4

Accident

Low skill

Moderate skill

Advanced threat

CSMS

RA

Defence-in-depth

Zones and Conduits

Security Levels

Critical Assets

Device Security

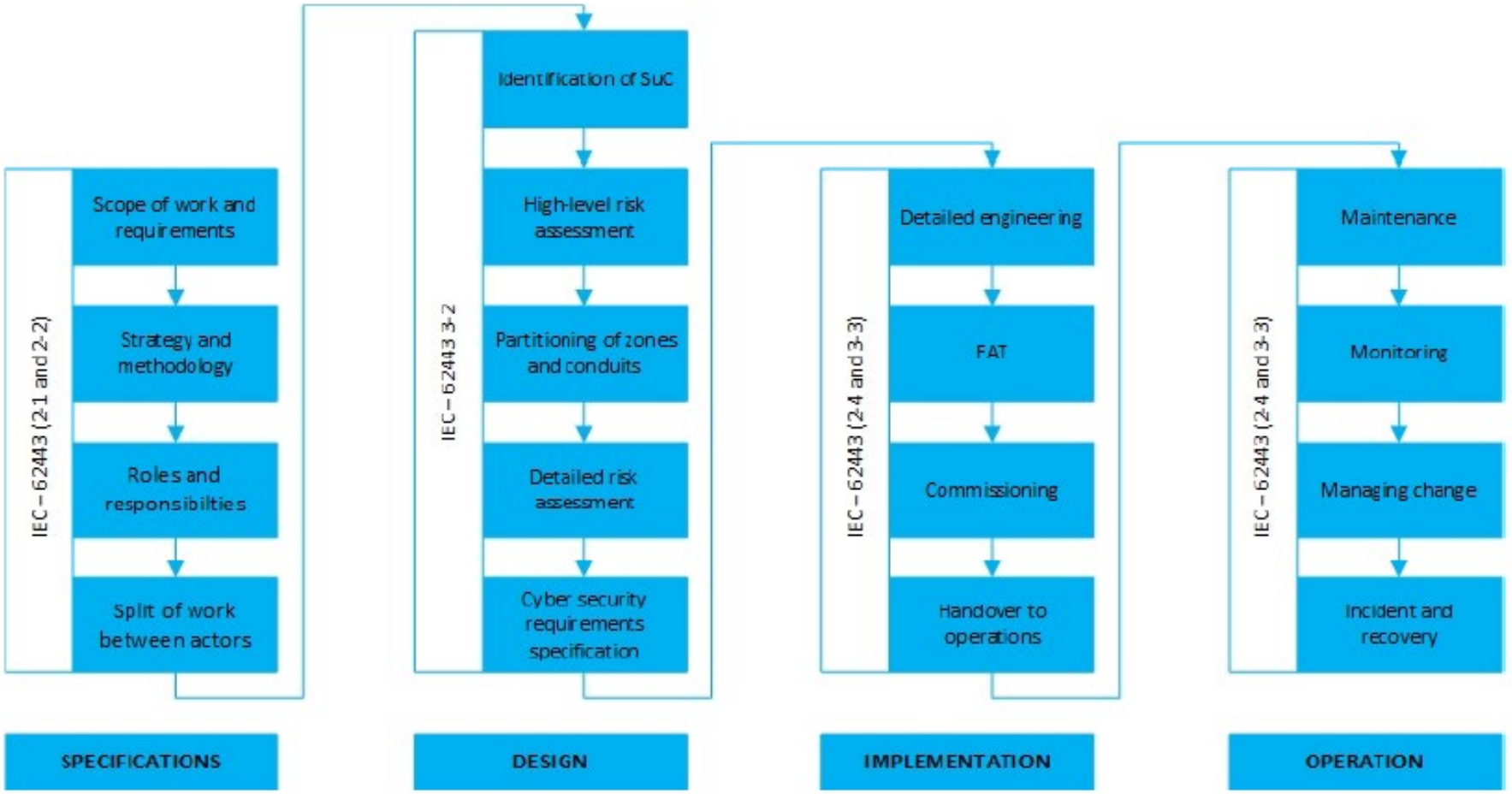
Visibility

Response

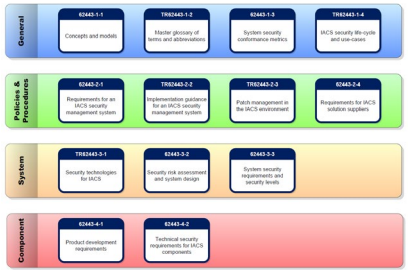
Human Factor

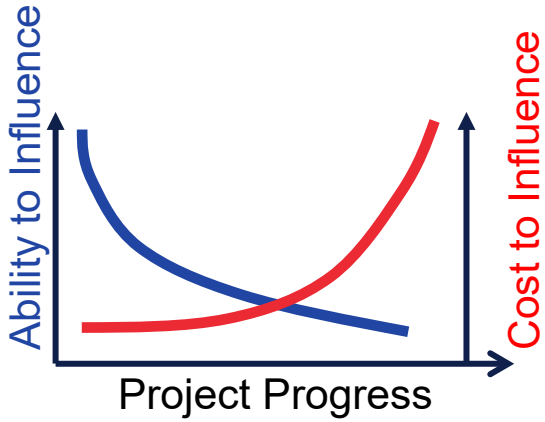
Supply Chain

IEC 62443 in project lifecycle



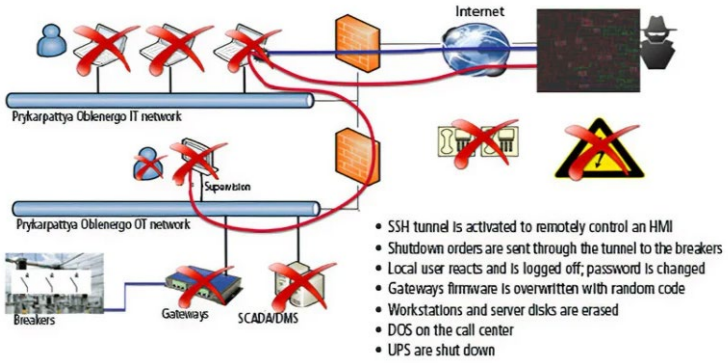
IEC 62443 chapters





Source: DNV-RP-0575 - Cyber security for power grid protection devices

Ukraine power grid attack through eyes of IEC 62443



3 steps:

1) Email phishing and C2

2) Recon IT / OT, enumeration, vulnerable devices, lateral movement, credential harvesting, becoming invisible, clean-up

3) Launch (attack duration 10 minutes)

Missing controls according to IEC 62443

FR	FR title	SR	SR title	SL1	SL2	SL3	SL4	Assessed SR
1-IAC	Identification and authentication control	1.1	Human user identification and authentication					FR1 = 0
1-IAC	Identification and authentication control	1.2	Authenticator feedback					
1-IAC	Identification and authentication control	1.3	Access via untrusted networks					
2-UC	Use control	2.1	Authorization enforcement					FR2 = 0
2-UC	Use control	2.4	Mobile code					
2-UC	Use control	2.6	Remote session termination					
2-UC	Use control	2.8	Auditable events					
2-UC	Use control	2.9	Audit storage capacity					
2-UC	Use control	2.11	Timestamps					
3-SI	System integrity	3.2	Malicious code protection					FR3 = 0
3-SI	System integrity	3.9	Protection of audit information					
4-DC	Data confidentiality	4.1	Information confidentiality					FR4 = 0
5-RDF	Restricted data flow	5.1	Network segmentation					FR5 = 2
5-RDF	Restricted data flow	5.2	Zone boundary protection					
5-RDF	Restricted data flow	5.3	Person-to-person communication restrictions					
5-RDF	Restricted data flow	5.4	Application partitioning					
6-TRE	Timely response to events	6.1	Audit log accessibility					FR6 = 1
6-TRE	Timely response to events	6.2	Continuous monitoring					
7-RA	Resource availability	7.3	Control system backup					FR7 = 0
7-RA	Resource availability	7.4	Control system recovery and reconstitution					
7-RA	Resource availability	7.5	Emergency power					
7-RA	Resource availability	7.7	Least functionality					

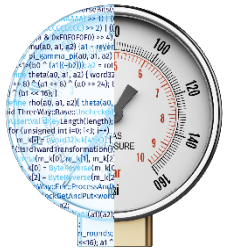
https://blog.isa.org/lessons-learned-forensic-analysis-ukrainian-power-grid-cyberattack-malware

DNV and IEC 62443

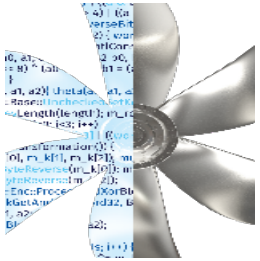
- Work with all stakeholders (asset owners, integrators, manufacturers)
- Draws from experience in different sectors
- Cyber Security Management System
- Risk assessment
- System and component testing and certification (IEC 62443 and IEC 62351)
- Training (IEC 62351 – DNV Energy Academy and IEC 62443)

  Two-day training course to improve the cyber security of your OT network by using IEC 62351 devices and implementations. https://www.dnv.nl/training/training-course-on-cyber-security-189292
- CyberGym Collaboration

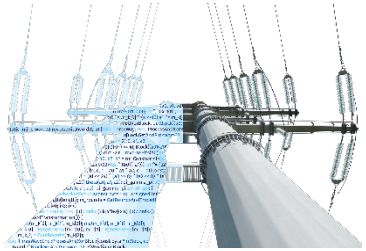
DNV cyber security market segments



Oil and gas

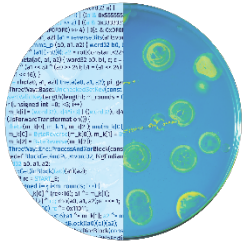


Maritime

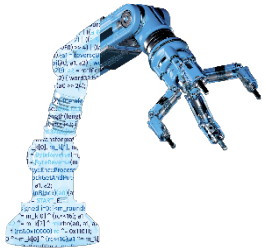


Electricity infrastructure & distribution

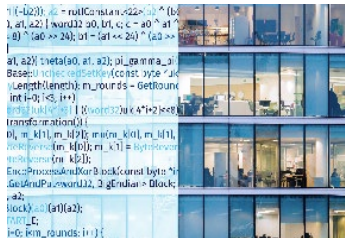
Renewables



Healthcare



Manufacturing



Public sector

Financial services