ENCS

Cyber Security

Fundamentals of the Smart Grid 2019

Brad Prent, ENCS

28 August 2019

European Network for Cyber Security

ENCS

The European Network for Cyber Security (ENCS) is a non-profit organization that brings together critical infrastructure stakeholders and security experts to deploy secure European critical energy grids and infrastructure.

Schedule

ENCS

15:30 Cyber Security
- Understanding the threat landscape
- Get in control, get prepared
- Security frameworks

16:10 Breakout Group Exercise – Protocol Security

16:25 Q&A Session Introduction
- Approach to enhancing security

16:40 Q&A Session

17:00 End

Learning Goals

- Understanding cyber security threats for a smart grid
- Understanding how cyber security strategies are evolving, to mitigate increasingly more sophisticated threats to the smart grid

What You Need To Know

ENCS

- Understand the threat landscape
- How to get in control and get prepared
- Security frameworks
- Enhancing security for smart grids

What Has Changed?

ENCS

More Standards

CEN CENELEC ETSI

ISO IEC ISA

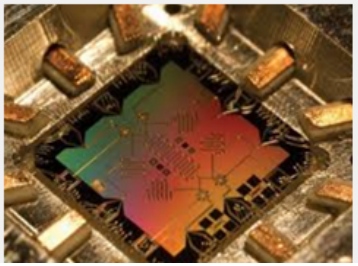
More Interconnectivity

More Targeted Attacks

More Active Threat Actors

More Automated Attacks/ Artificial Intelligence

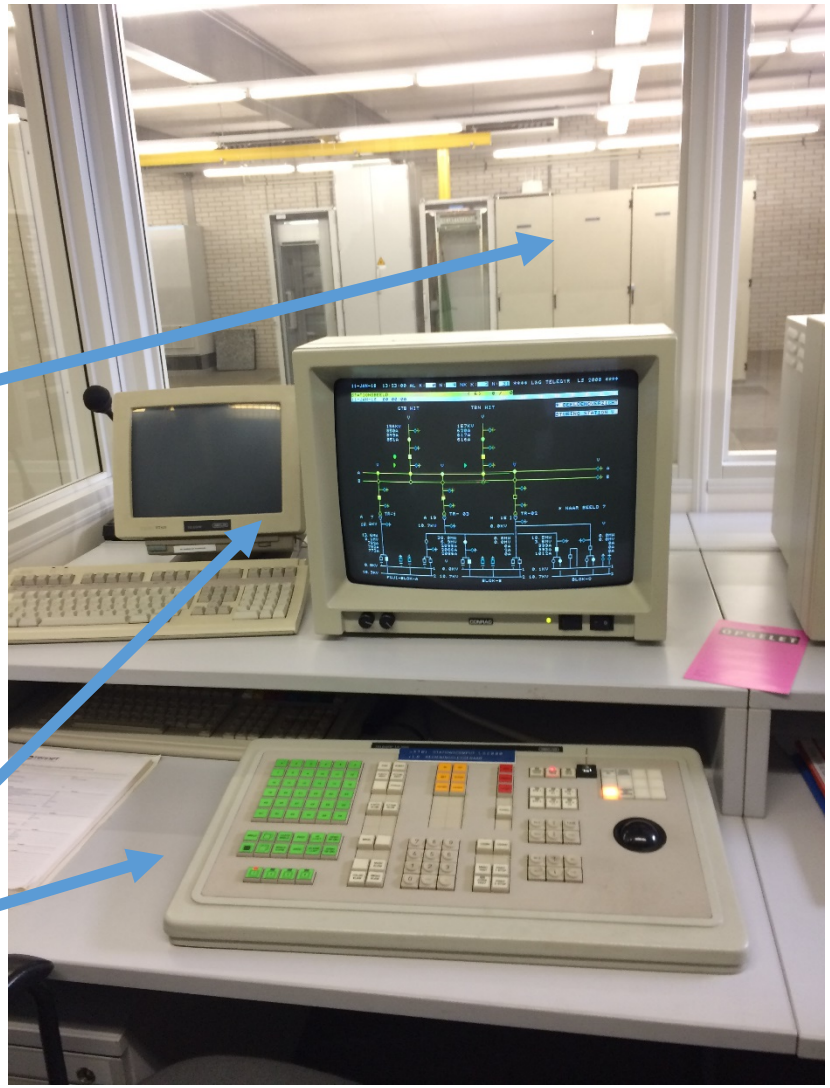
More Computing Power* and Better Tools



(Quantum Computing*)


ДАВЛЕНИЕ БС
НАСОСЫ ЦН-1

Substation (1998)



- Serial connection to RTU
- SCADA over proprietary protocol
- Custom hardware and software (including OS)

ENCS

Substation (2018)

ENCS

- IEDs connected over Ethernet using IEC 61850 (MMS, GOOSE)
- Configured with standard Windows laptop
- HMI and SCADA Gateway run Windows using IEC 104
- Use of USB

Bedroom Hackers Grew Up

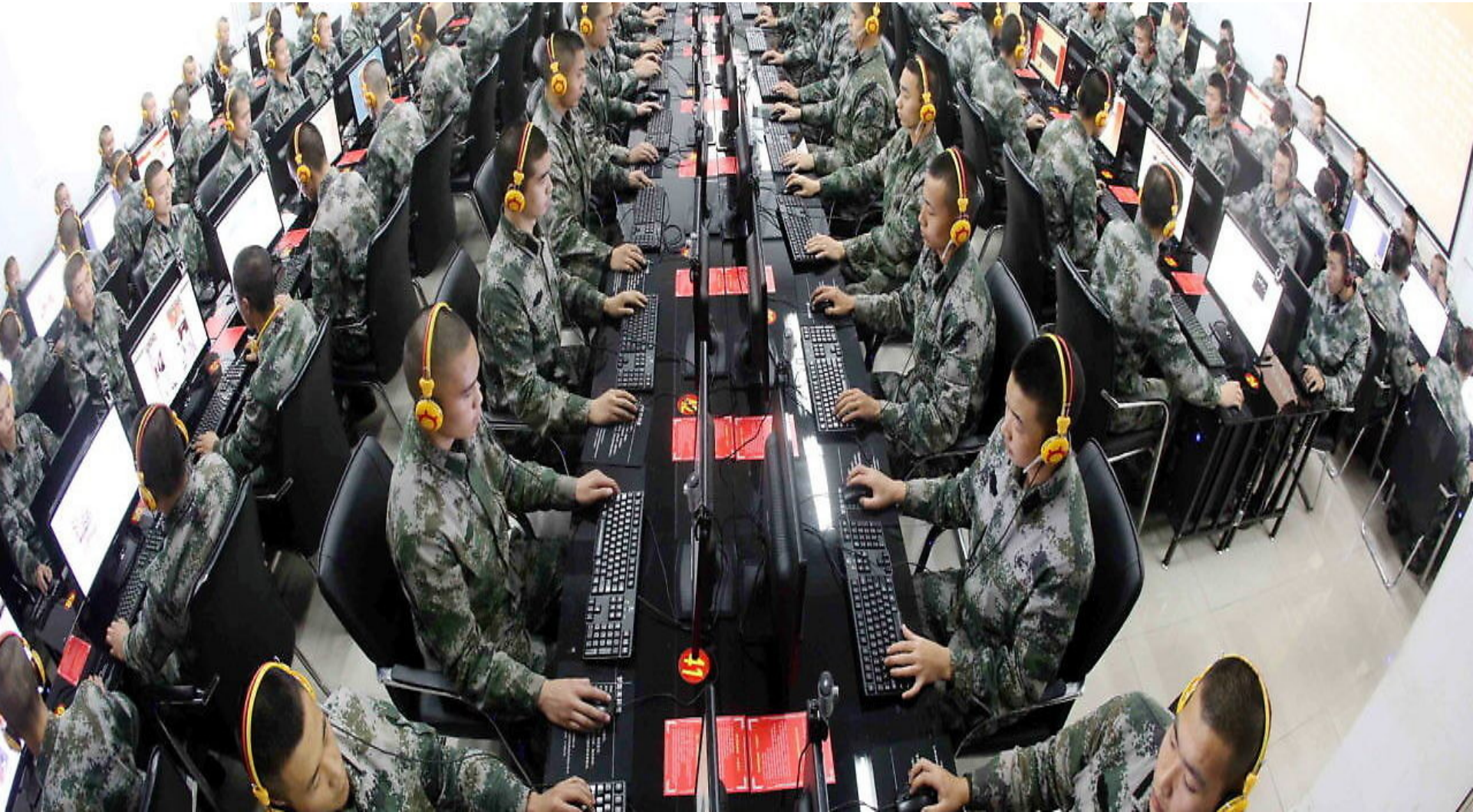
ENCS

Cyber Criminal = Ransomware = Money

ENCS

Militarisation Of Cyber Warfare

ENCS



Nation State Hackers?

ENCS

Are The Threats Real?

ENCS

The New York Times

U.S. Escalates Online Attacks on Russia's Power Grid

A heating power plant in Moscow. Officials described the move into Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections.
Maxim Shemetov/Reuters

By David E. Sanger and Nicole Perlroth

June 15, 2019

960

The US planted offensive malware in Russia's power grid

It's acting on vows to conduct more aggressive cyberwarfare.

Jon Fingas, @jonfingas
06.15.19 in Security

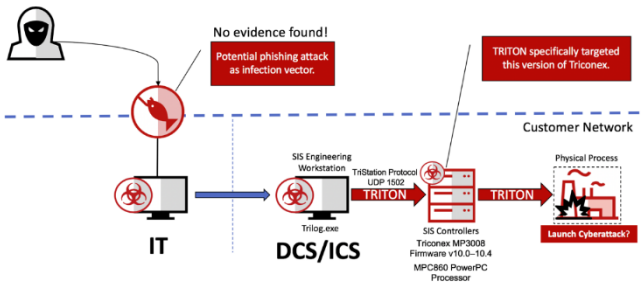
56
Comments

2079
Shares

engadget

Modern Threat History Highlights

ENCS



First Cyber Incident In Ukraine

ENCS

23 December 2015

- Power outage occurred in Ukraine
- Affected 50% of Ivano-Frankivsk region
- Malware was found at several of the affected regional Distribution System Operators (DSOs)
- Outage was caused by a cyber attack via IT

Technology

Hackers caused power cut in western Ukraine - US

12 January 2016 | Technology

Security

Malware 'clearly' behind Ukraine power outage, SANS utility expert says

Mounting evidence attacks are handiwork of elite Russian hacker team.

Ukraine Déjà vu

ENCS

17 December 2016

- Substation in Pivnichna
- Cut off from main power grid for 75 minutes
- Hackers sent malware via phishing email to employees
- Allowed them to steal login credentials and shut down substations

Energy firm points to hackers after Kiev power outage

Erm, it was hovering between -9˚C and -1˚C that day

21 Dec 2016 at 10:58, John Leyden

Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks

Russian hackers may be behind attacks leveled at the nation's power grid and artillery. The West should take note.

Industroyer

ENCS

July 2017

INDUSTROYER

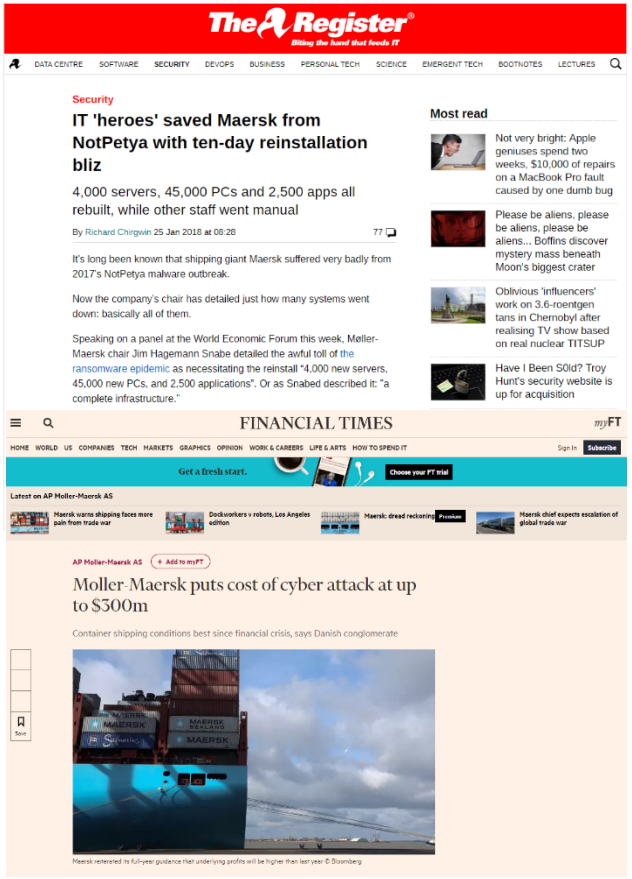
- Probably caused 2016 power outage in Ukraine
- Specifically aimed at electricity grids
- Supports sending IEC 104 commands
- Supports sending IEC 61850 commands
- Exploits against SIPROTEC protection relays

Collateral Damage From IT

ENCS

27 June 2017

- WannaCry / (Not)Petya ransomware randomly hit companies
- EternalBlue – NSA SMB v1 exploit
- Flat networks without segregation helped spread malware and make containment harder
- Could have affected any Windows computers in substations



The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES LECTURES

Security

IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz

4,000 servers, 45,000 PCs and 2,500 apps all rebuilt, while other staff went manual

By Richard Chirgwin 25 Jan 2018 at 08:28 77

It's long been known that shipping giant Maersk suffered very badly from 2017's NotPetya malware outbreak.

Now the company's chair has detailed just how many systems went down: basically all of them.

Speaking on a panel at the World Economic Forum this week, Møller-Maersk chair Jim Hagemann Snabe detailed the awful toll of the ransomware epidemic as necessitating the reinstall "4,000 new servers, 45,000 new PCs, and 2,500 applications". Or as Snabed described it: "a complete infrastructure."

Most read

Not very bright: Apple geniuses spend two weeks, $10,000 of repairs on a MacBook Pro fault caused by one dumb bug

Please be aliens, please be aliens, please be aliens... Boffins discover mystery mass beneath Moon's biggest crater

Oblivious 'influencers' work on 3.6-roentgen tans in Chernobyl after realising TV show based on real nuclear TITSUP

Have I Been S0ld? Troy Hunt's security website is up for acquisition

FINANCIAL TIMES myFT

HOME WORLD US COMPANIES TECH MARKETS GRAPHICS OPINION WORK & CAREERS LIFE & ARTS HOW TO SPEND IT Sign In Subscribe

Get a fresh start. Choose your FT trial

Latest on AP Moller-Maersk AS

Maersk warns shipping faces more pain from trade war

Dockworkers v robots, Los Angeles edition

Maersk: dread reckoning Premium

Maersk chief expects escalation of global trade war

AP Moller-Maersk AS + Add to myFT

Moller-Maersk puts cost of cyber attack at up to $300m

Container shipping conditions best since financial crisis, says Danish conglomerate

Maersk reiterated its full-year guidance that underlying profits will be higher than last year © Bloomberg

12:00 EDT – JUNE 27, 2017

Ukraine's police confirm MeDoc, an accounting software package taxes, as a NotPetya infection vector.

Robert M. Lee
@RobertMLee

Kyivenergo hacked, Ukrenergo affected kyivpost.com/ukraine-politi… > very little known right now but worth watching

♡ 38 2:48 PM - Jun 27, 2017

Kyivenergo hacked, Ukrenergo affected - Jun. 27, 2017

Kyiv's energy generating company Kyivenergo has reported a hacker attack, the company's press service has told the… - Jun. 27, 2017.

kyivpost.com

Maersk
@Maersk

We can confirm that Maersk IT systems are down across multiple sites and business units. We are currently assessing the situation.

♡ 202 2:21 PM - Jun 27, 2017

Kaspersky Lab's analysts are investigating the new wave of ransomware attacks targeting organizations across the world. Our preliminary findings suggest that it is not a variant of Petya ransomware as publically reported, but a new ransomware that has not been seen before. That is why we have named it NotPetya.

The company's telemetry data indicates around 2,000 attacked users so far. Organizations in Russia and the Ukraine are the most affected, and we have also registered hits in Poland, Italy, the UK, Germany, France, the US and several other countries.

This appears to be a complex attack which involves several attack vectors. We can confirm that a modified EternalBlue exploit is used for propagation at least within the corporate network.

Kaspersky Lab detects the threat as UDS:DangeroundObject.Multi.Generic.

Kaspersky Lab experts aim to release new signatures, including for the System Watcher component as soon as possible and to determine whether it is possible to decrypt data locked in the attack – with the intention of developing a decryption tool as soon as they can.

We advise all companies to update their Windows software, to check their security solution and ensure they have back up and ransomware detection in place.

Kaspersky Lab corporate customers are also advised to:

- Check that all protection is activated as recommended; and that they have enabled the KSN/System Watcher component.
- Use the AppLocker feature to disable the execution of any files that carry the name "perfc.dat"; as well as the
- PSExec utility from Sysinternals Suite.

Kaspersky
@kaspersky

The latest from @kaspersky researchers on #Petya: it's actually #NotPetya

♡ 637 7:12 PM - Jun 27, 2017

Why Target Smart Grids?

ENCS

Untargeted & Opportunistic Attackers

Script kiddies
- Stereotype teenage hacker
- Intends no real damage, but may cause it unintentionally

Hacktivists
- Deface websites
- Cause bad publicity

Researchers / Journalists
- Show what's possible
- Like a good story

Opportunistic Criminals
- Target IT, but may hit OT
- Just sending spams
- Ransomware

Targeted Determined Financed Attackers

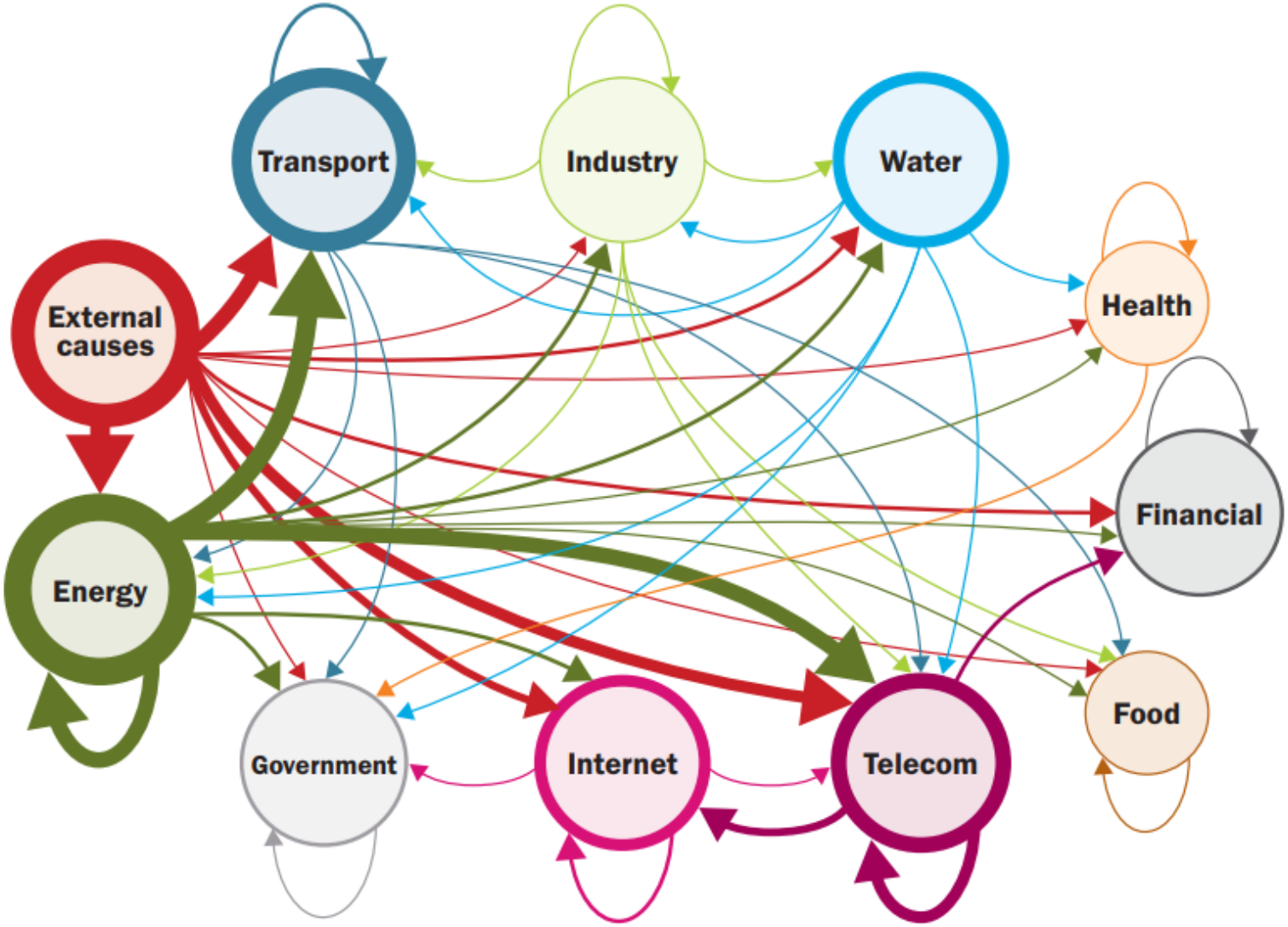
Disgruntled Employees
- Taking revenge
- Selling information on the black market

Terrorists
- May be interested in causing power outage

Criminals targeting OT
- Extortion
- Could work for terrorists of nation states

Nation State Actors
- Strategic assets
- Espionage
- Sabotage

Energy interconnects with all of **Society**



https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf

Key Risk To Smart Grids

ENCS

- Technology mix
  - New internet connected components are added everywhere in the grid architecture (smart meters, IoT etc.)
  - Patching hardly possible
- Cascading effects
  - Inside grids, spreading to other critical infrastructures
- IT security concepts invalid for the grid
  - monitoring/incident handling/recovery
- Security immaturity of OT suppliers

What You Need To Know

ENCS

- Understand the threat landscape
- How to get in control and get prepared
- Security frameworks
- Enhancing security for smart grids

European Regulatory Perspective

- NIS Directive (effective May 2018)
  - Appropriate technical and organizational measures
  - Mandatory (national) incident reporting
- Cybersecurity Act
  - New permanent mandate for ENISA
  - European cybersecurity certification framework for ICT products and services
  - *Certification framework yet to be decided*

EG2 Recommendations

ENCS

Network Code Cybersecurity

- Baseline protection for all grid operators
  (ISO 27001 and minimum security requirements)
- More advanced cybersecurity standards should apply to
  Operators of Essential Services (OES)

IEC 62443

ISO 27001

Commission Recommendations

ENCS

Specific measures addressing:

- Real-time requirements
- Cascading effects
- Legacy and state-of-the-art technology

Brussels, 3.4.2019
C(2019) 2400 final

COMMISSION RECOMMENDATION

of 3.4.2019

on cybersecurity in the energy sector

{SWD(2019) 1240 final}

Get In Control, Get Prepared

ENCS

- Technology mix
  - Defense in depth for legacy systems
  - Security requirements and testing for new grid components
- Incident management
  - Intrusion detection systems
  - Exercises
  - Recovery!
- Skills management
  - Awareness
  - Role based training
  - Expert knowledge

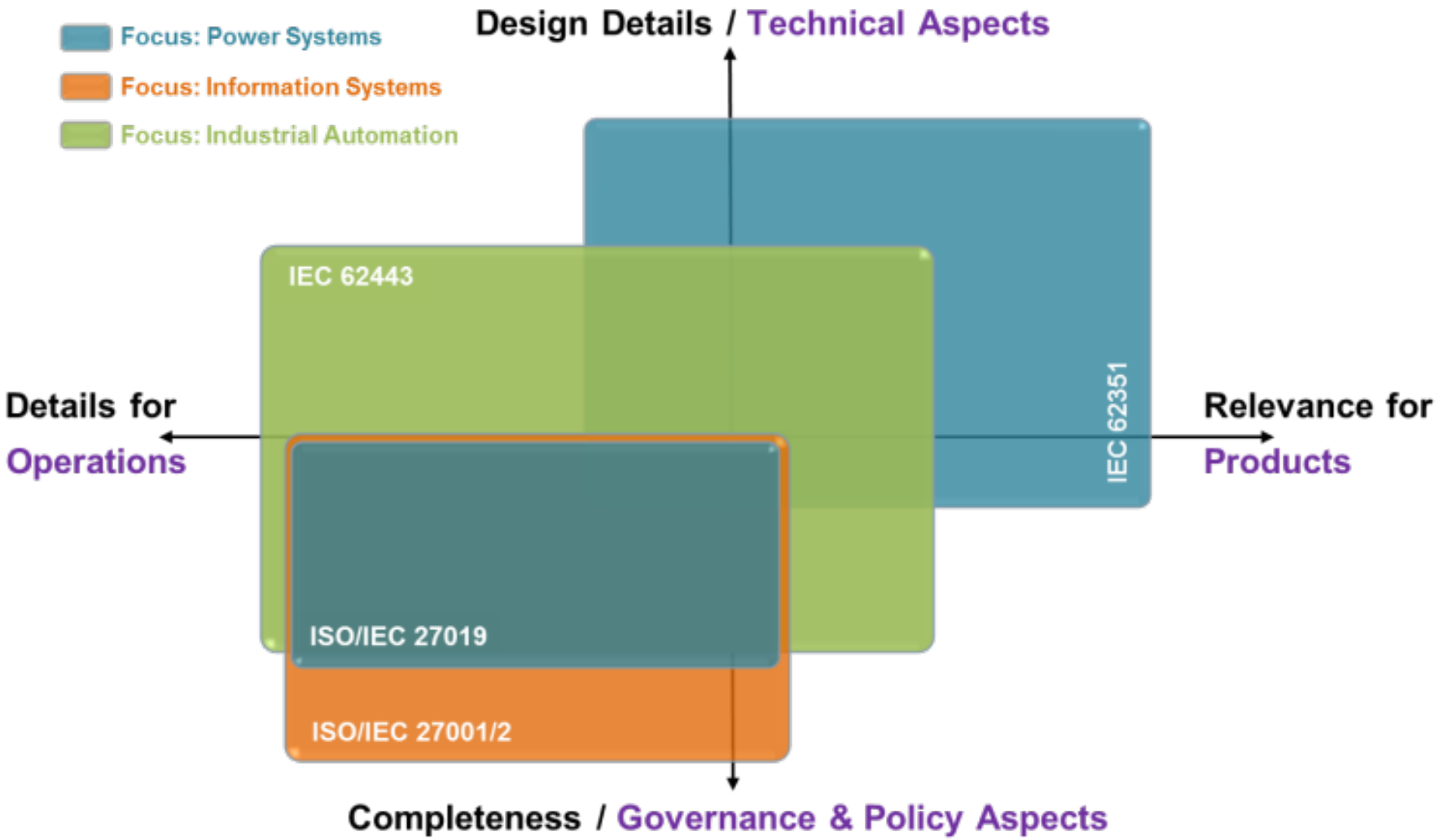
What You Need To Know

ENCS

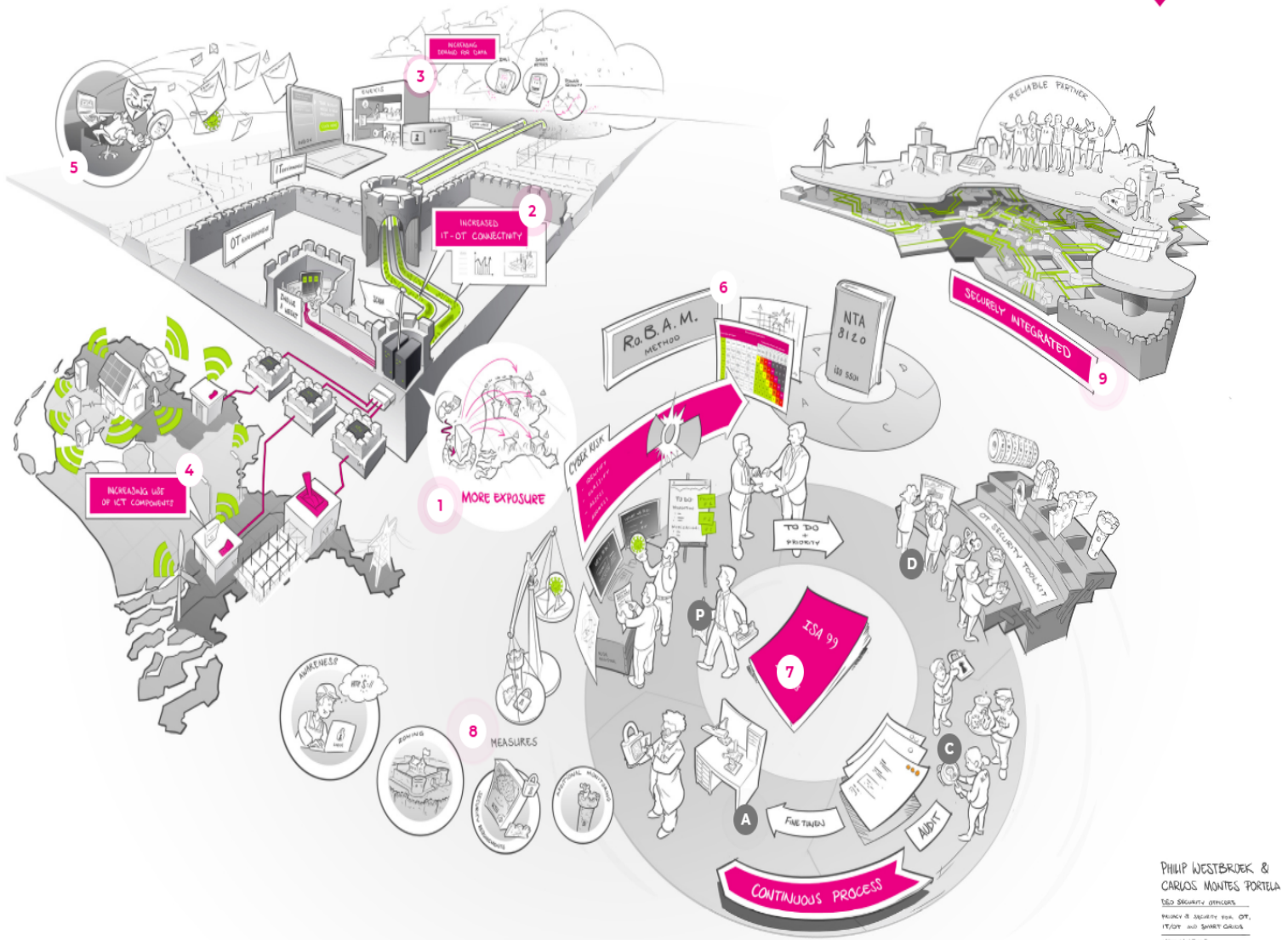
- Understand the threat landscape
- How to get in control and get prepared
- Security frameworks
- Enhancing security for smart grids

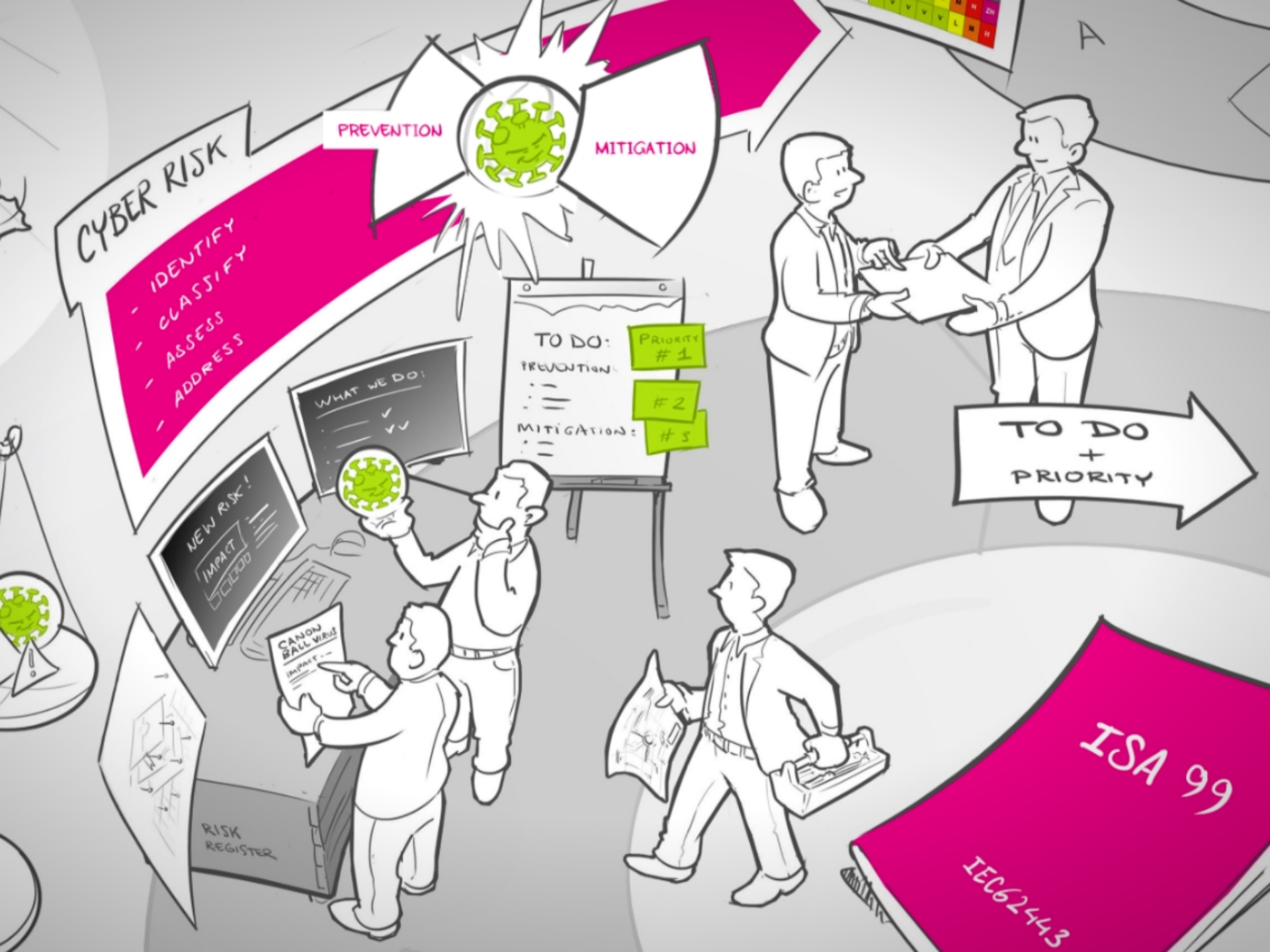
Frameworks in Energy Sector

ENCS



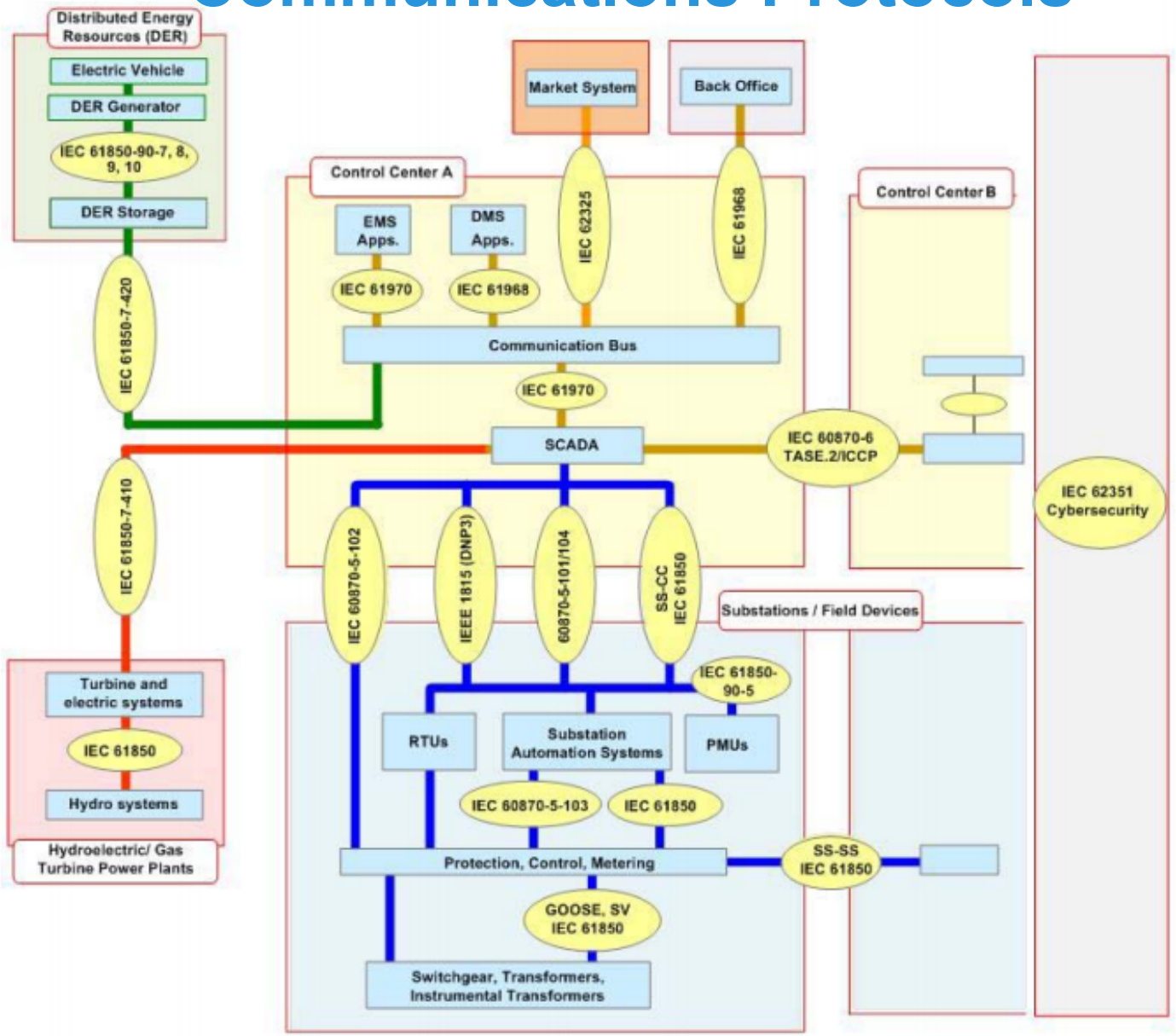
How They Can Meet In The Middle




CYBER RISK
- IDENTIFY
- CLASSIFY
- ASSESS
- ADDRESS
PREVENTION
MITIGATION
TO DO:
PREVENTION:
MITIGATION:
PRIORITY #1
#2
#3
WHAT WE DO:
NEW RISK!
IMPACT
CANON BALL VIRUS
RISK REGISTER
TO DO + PRIORITY
ISA 99
IEC62443

Breakout Group Exercise

Communications Protocols



Q&A Introduction

What You Need To Know

ENCS

- Understand the threat landscape
- How to get in control and get prepared
- Security frameworks
- Enhancing security for smart grids

Enhancing Security For Smart Grids

ENCS

Five key areas to enhance security

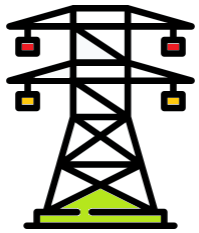
1. Implement an ISMS
2. Establish cyber risk management
3. Establish cyber technical controls
4. Prepare for the worst case
5. Manage the skill gap

Implement An ISMS

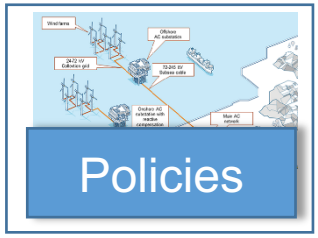
ENCS

Know your threats

Know your risks

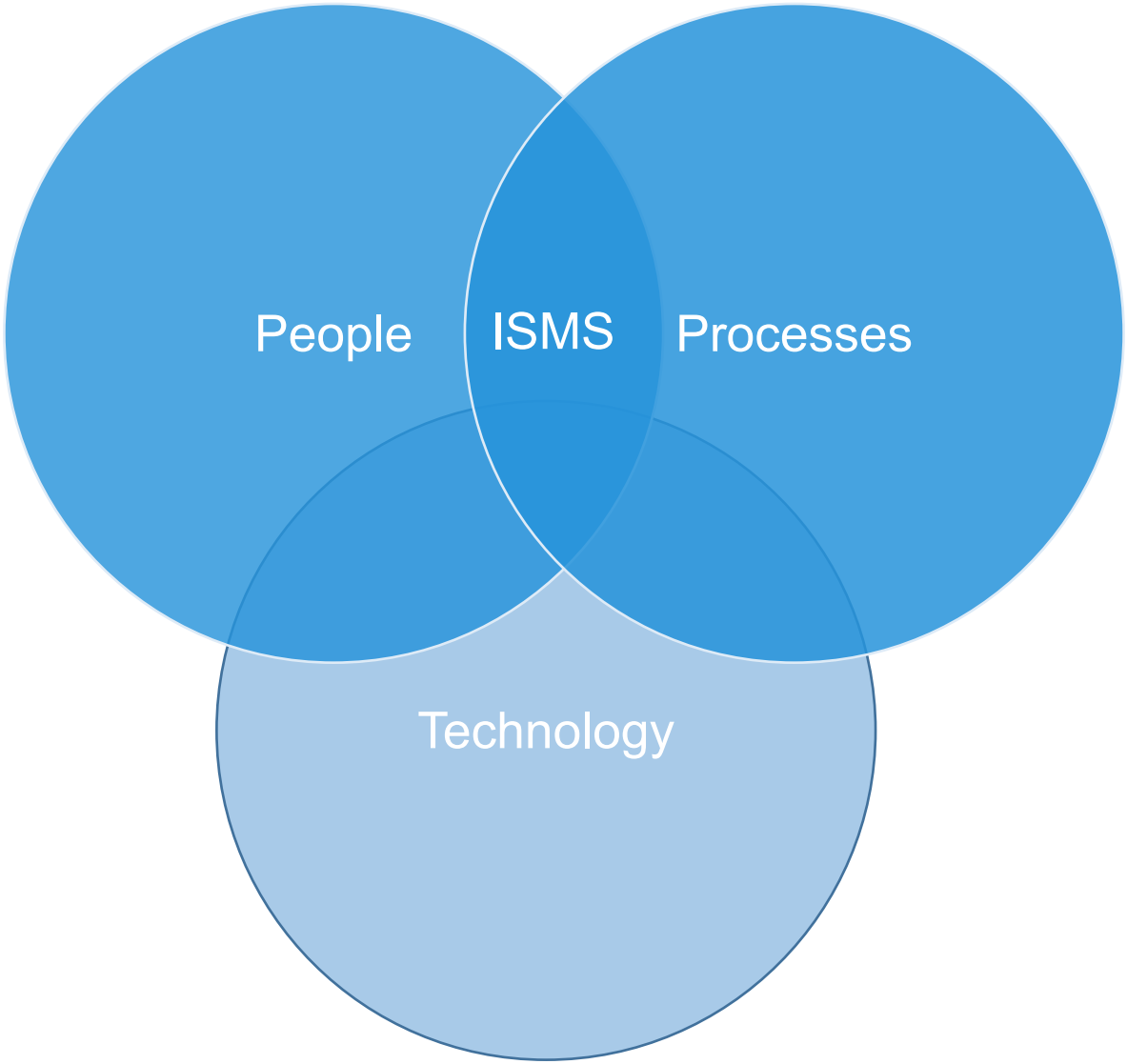


Set your policies



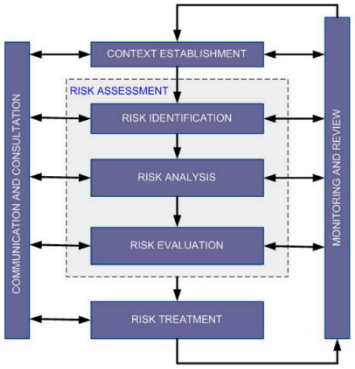
Prove your security controls

ISMS Is All About People and Processes

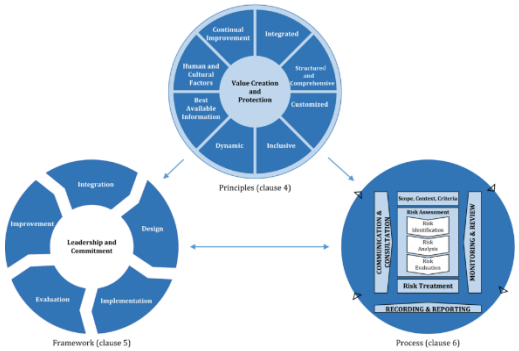


Risk Management Gives Security Focus

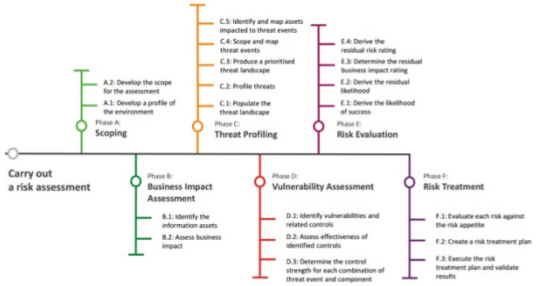
ENCS



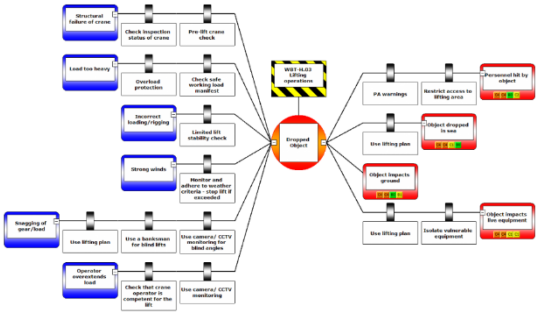
ISO 27005



ISO 31000



ISF IRAM2



BOWTIE

ISO Ref	Applicable	Reason For Inclusion	Implemented	Domain	ISO 27001:2013 Control Requirement	Current Control Measures	Evidence Location	Additional Control Measures Required	Accountable
5				Security Policies					
5.1				Management direction for information security	Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations				
5.1.1	Yes	Annual Risk Assessment	Yes	Policies for information security	A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.				
5.1.2	Yes	Annual Risk Assessment	Yes	Review of the policies for information security	The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness				

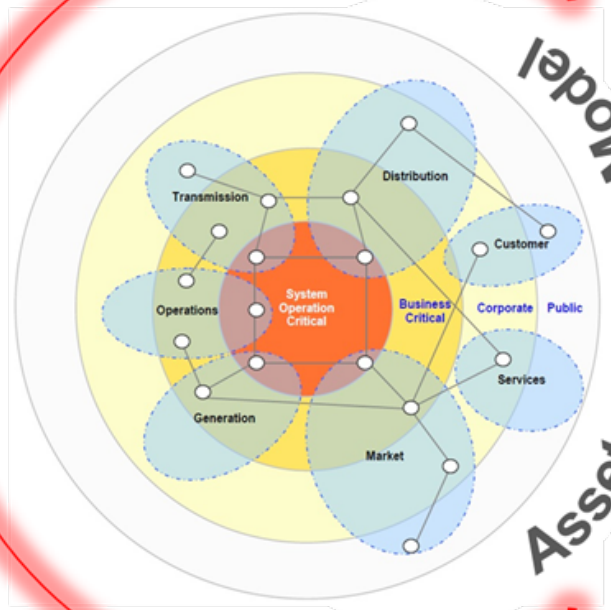
YOUR OWN VERSION?

Focus On Critical Assets At Risk

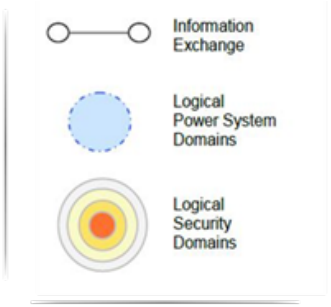
ENCS

- (D)DOS Attacks
- Sabotage & Espionage
- Misconfiguration or Inappropriate Design
- Targeted Attacks
- Unauthorized Access to Assets and Data
- Unintentional Information Leakage
- Unsolicited and Infected E-mail
- Misuse of Assets
- Malware Intrusion

Major Threats & Risks



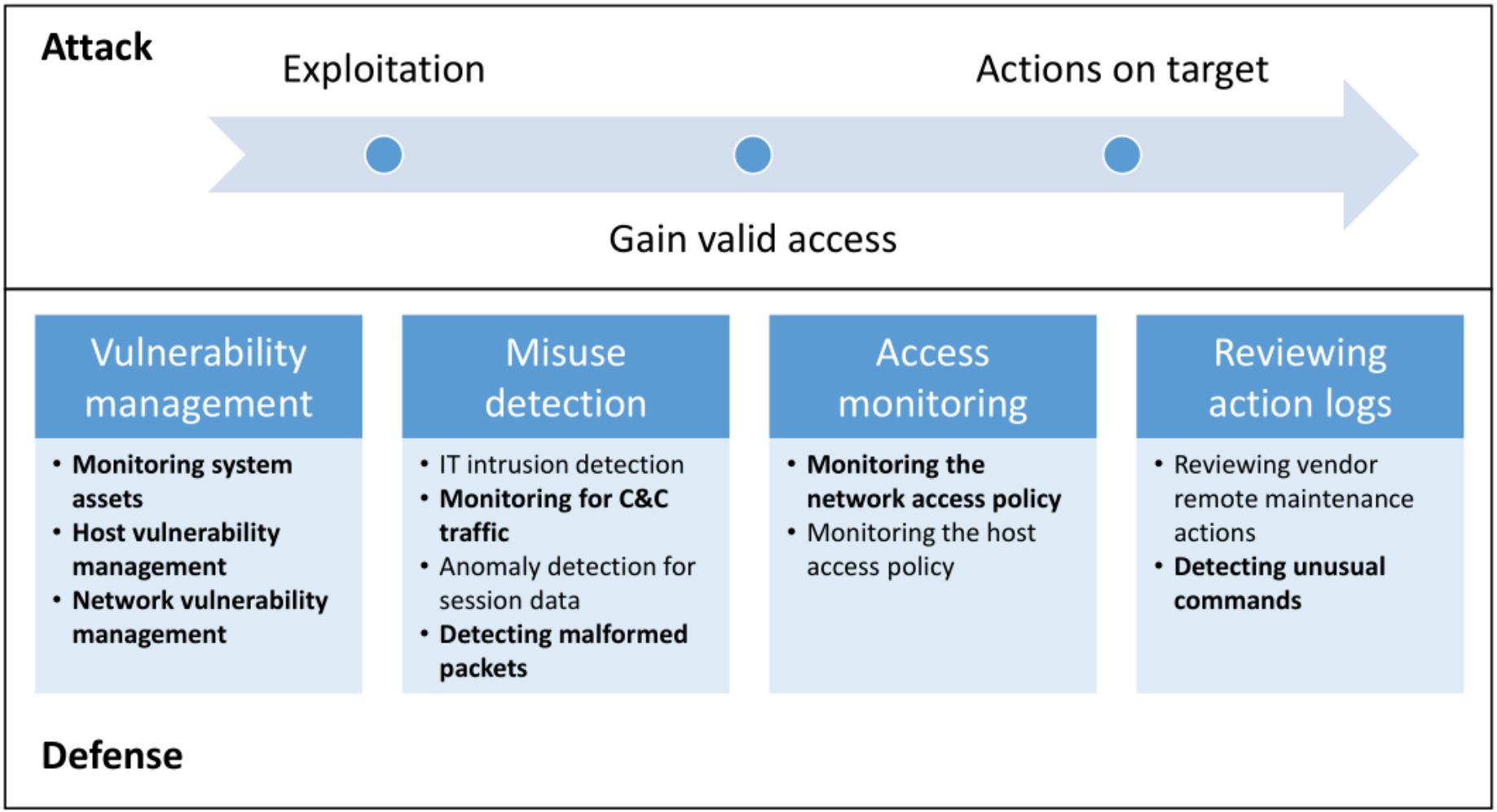
Asset Security Model



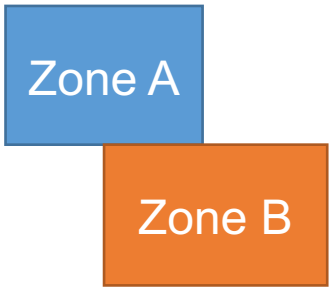
Cybersecurity Requirements

Define Strong Use Cases To Mitigate

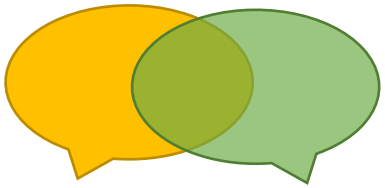
ENCS



Architectures



- **Zoning Model**
  - Implement a zoned network architecture that protects the interface between IT and OT systems
  - Divide OT infrastructure into different security zones based on their risk levels
  - Standards such as IEC 62443 can help here.



- **Secure Communication**
  - Authenticate and encrypt communication between zones
  - Gradually deploy secure communication to components

- **Access Control**
  - Define and implement centralized access control & 3rd party remote access strategies
  - Develop strategies for secure field maintenance access to infrastructure

System & Component Security

ENCS

- **Enhanced Lifecycle Management**
  For smart grid systems and components, including security requirements during procurement

- **Security Validation**
  Adoption of open/standardized tools and best practices for security validation

- **Futureproof Deployments**
  Adoption of reliable and efficient processes to perform software/firmware upgrades. Ensure sufficient hardware capacities are available

- **Functional Separation**
  Available support for secure separation of services on single physical units. (“Zoning for Components”)

Cyber Security Monitoring

ENCS

Security Monitoring

- Set up a SIEM system and start to collect information
- Set up teams to analyze and respond to security events
- Deploy SCADA network intrusion detection systems with deep-packet inspection and flow monitoring
- SOC, CSIRT, Trigger for BCM/DR

Threat Intelligence

- Foster industry exchange of **vulnerabilities** in industrial components
- At EU level: **Incident** Reporting through NIS Directive mandatory

Organise Your Smart Grid's CSIRT

ENCS

Cyber Security Incident Response Team

- Virtual OT CSIRT
- Integrated OT / IT CSIRT
- Industry CSIRT
- EU CSIRT (CERT-EU)
- Outsourcing / Collaboration model

Need operational security capabilities within the OT engineering departments to work with the response team

Have A Recovery Process

Not all components may work normally, may take months to bring all systems into operation again.

- Have a contingency plan
- Have up to date schematics available
- Have manually inputted configuration available
- Have backups (data, systems, configs, docs)
- Test if the plans and backups work
- Know how to test if system is working normally

Role Based Program

ENCS

Process	Leading role	Other roles
Selecting and implementing organizational security measures	**Security officers:** • Implement an ISMS • Understand risks to OT systems • Select measures feasible for OT	**All employees:** • Know how to apply security policies • Be aware of security risks
Selecting and implementing technical security measures;	**Security architects:** • Assess risks in detail • Select effective measures • Track the implementation • Evaluate the implementation	**Engineers:** • Translate architecture design into component configurations • Roll out configurations • Perform functional tests
Finding and mitigating vulnerabilities;	**Security analysts:** • Monitor for vulnerabilities • Assess the risk of vulnerabilities • Select fixes or mitigations • Track implementation • Validate implementation	• Apply patches or secure settings
Detecting and responding to security incidents	• Gather data for detection • Analyze alerts • Handle small incidents • Advice during major incidents	• Isolate systems • Recover systems to a secure state **Crisis organization:** • Coordinate major incidents • Prioritize response actions • Communicate about incidents

Collaboration and Resource Sharing

ENCS

Collaboration focus on

- Security requirements, testing and certification
- Education & Training
- Research

Security Community Building

- Policy
- Architecture
- Operations

Questions and Answers

https://www.encs.eu