Cybersecurity Essentials and Management for Energy Sector

CSP001_S_E

PRESENTATION BY:
PINELOPI KYRANOUDI, CYBERSECURITY RESEARCHER AT TECHNICAL UNIVERSITY OF CRETE
ANTONIOS NTIB, RESEARCHER AT TECHNICAL UNIVERSITY OF BRAUNSCHWEIG

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

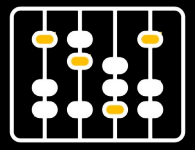
Project Agreement no. 101083594

Goals: Who-What-Why you need to take this training

WHO

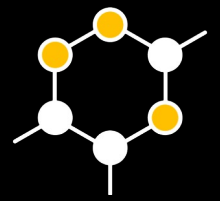
Professionals involved in the operation, security, and management of energy systems, including engineers, operators, cybersecurity specialists, and decision-makers

WHAT



Seminar on cybersecurity risk, incident response, and operational resilience in energy systems, covering IT, OT, and IIoT environments

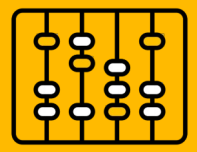
WHY



Equipping participants with the ability to assess risk, respond to incidents, and ensure safe and stable operation of critical energy systems

CSP Training Logistic: When-Where-How

WHEN



Time schedule (to be posted in DCM platform)

WHERE

Physically, virtually, or both (to be posted in DCM platform)

HOW

Instructor-led sessions

Value Propositions

Benefits to Participants

- Level of Training Module: Advance
- Cybersecurity Professional Training
- Rooted with European Cybersecurity Skills Framework
- Cutting-edge insights from industry-academic experts
- Certificate of the completion
- Helps with skills development and career advancement

WHAT

Training Topics

- Introduction to Energy Cybersecurity
- Understanding Energy Cyber Risks
- Risk Assessment and Management
- Business Continuity and Best Practices

WHY

Learning Outcomes

Knowledge:

- Understanding of cybersecurity threats and risks in energy systems
- Familiarity with standards, frameworks, and regulatory requirements
- Awareness of real-world incidents and case studies in the energy sector
- Understanding of risk assessment and risk management approaches
- Knowledge of IT, OT, and IIoT security practices and challenges
- Understanding of business continuity, backup, and recovery principles

Training Outline

Topic-1: Introduction to Energy Cybersecurity

Overview of cybersecurity threats in the energy sector.

Importance of energy cybersecurity.

Introduction to relevant cybersecurity standards (e.g., Organización Internacional de Normalización (ISO)/ International Electrotechnical Commissio (IEC) 2700x, ISO 27019, National Institute of Standards and Technology (NIST) SP-800-82).

Topic-2: Understanding Energy Cyber Risks

Identification of cyber risks in energy operations.

Case studies and real-world examples of cybersecurity incidents in the energy industry.

IT, OT & IIoT infrastructure and devices.

Training Outline

Topic-3: Risk Assessment and Management

Risk assessment VS risk management.

Risk assessment and management methods.

Risk assessment and management in cyber-physical systems (IT, OT, IIoT).

Topic-4: Business Continuity and Best Practices

Incident response.

Data backup and recovery planning.

Staff education on cybersecurity best practices (e.g. Redundant Array of Inexpensive Disk (RAID), cold storages, access methods to server rooms).

Background Knowledge and Prerequisites

Background knowledge:

Basic understanding of computers and networking

Familiarity with common internet security threats and vulnerabilities

Awareness of cybersecurity

Prerequisites:

None

Resources:
Reference Material

1. ISO/IEC 27001:2022, Information Security Management Systems — Requirements
2. ISO/IEC 27005:2018, Information Security Risk Management
3. ISO/IEC 22301:2019, Security and Resilience – Business Continuity Management Systems
4. IEC 62443 Series, Industrial Communication Networks – IT Security for Industrial Automation and Control Systems
5. NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments, 2012
6. NIST SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations, 2018
7. NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide, 2012
8. NIST SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security, 2015
9. NIST, Cybersecurity Framework (CSF) 2.0
10. ENISA, ENISA Threat Landscape 2023
11. ENISA, Cyber Security Information Sharing in the Energy Sector
12. U.S. Department of Energy (DOE), Cybersecurity Capability Maturity Model (C2M2), Version 2.1, 2022
13. CISA, Cybersecurity Incident & Vulnerability Response Playbooks, 2021
14. Dragos Inc., CrashOverride Analysis of the Ukraine Electric Power Event
15. CISA, Analysis of the Colonial Pipeline Ransomware Incident

Course progress

01. Introduction to Energy Cybersecurity

02. Understanding Energy Cyber Risks

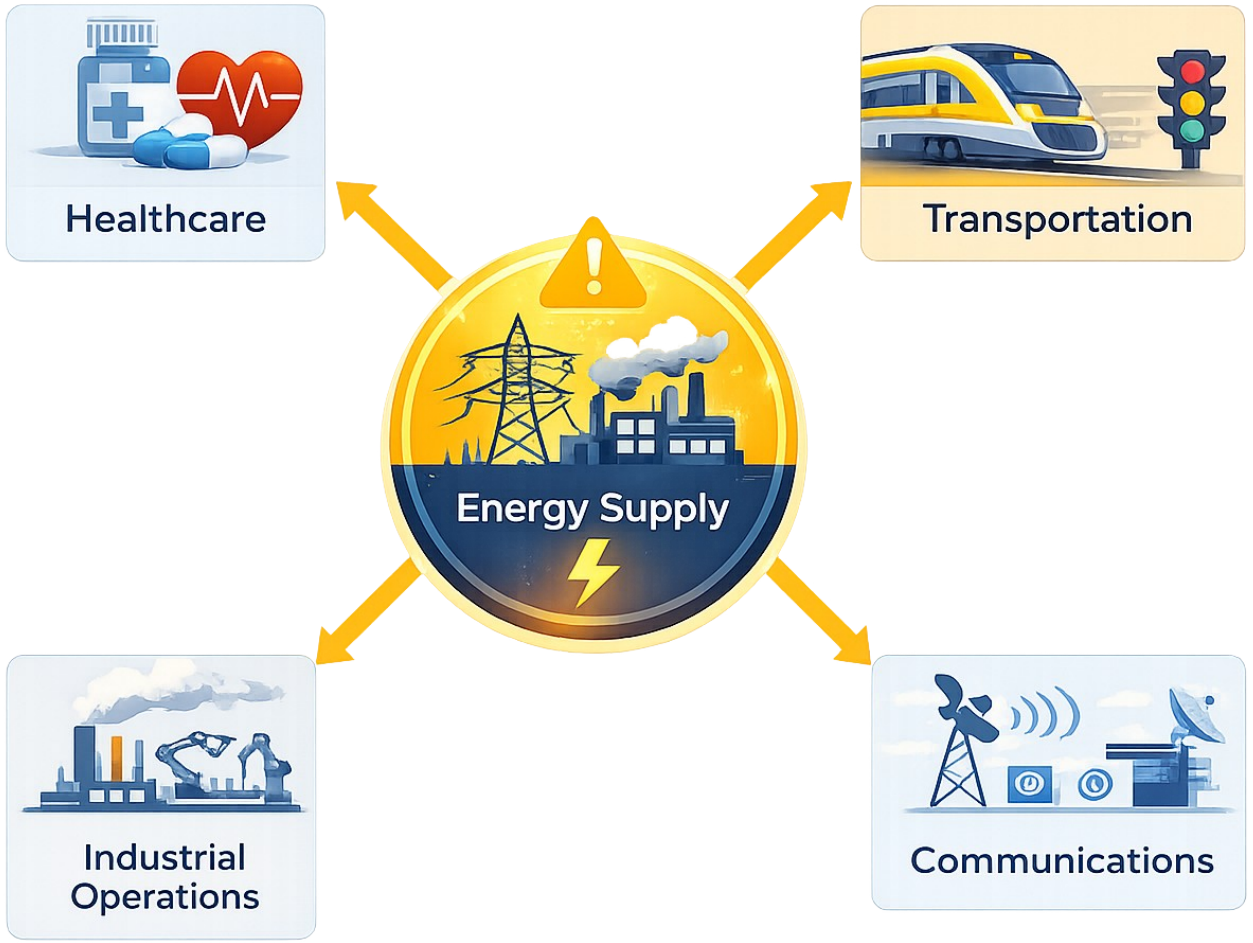
03. Risk Assessment and Management

04. Business Continuity and Best Practices

Energy Cybersecurity as a Cyber-Physical Discipline

- **Energy cybersecurity** is not limited to protecting data – it safeguards systems that directly control **physical processes** such as electricity generation and distribution.
- Unlike traditional IT environments, failures in energy systems can lead to **real-world consequences**, including equipment damage and service outages.
- This makes cybersecurity in the energy sector inherently **cyber-physica**l, combining digital protection with operational safety.
- Understanding this **dual nature** is essential for designing effective protection strategies.

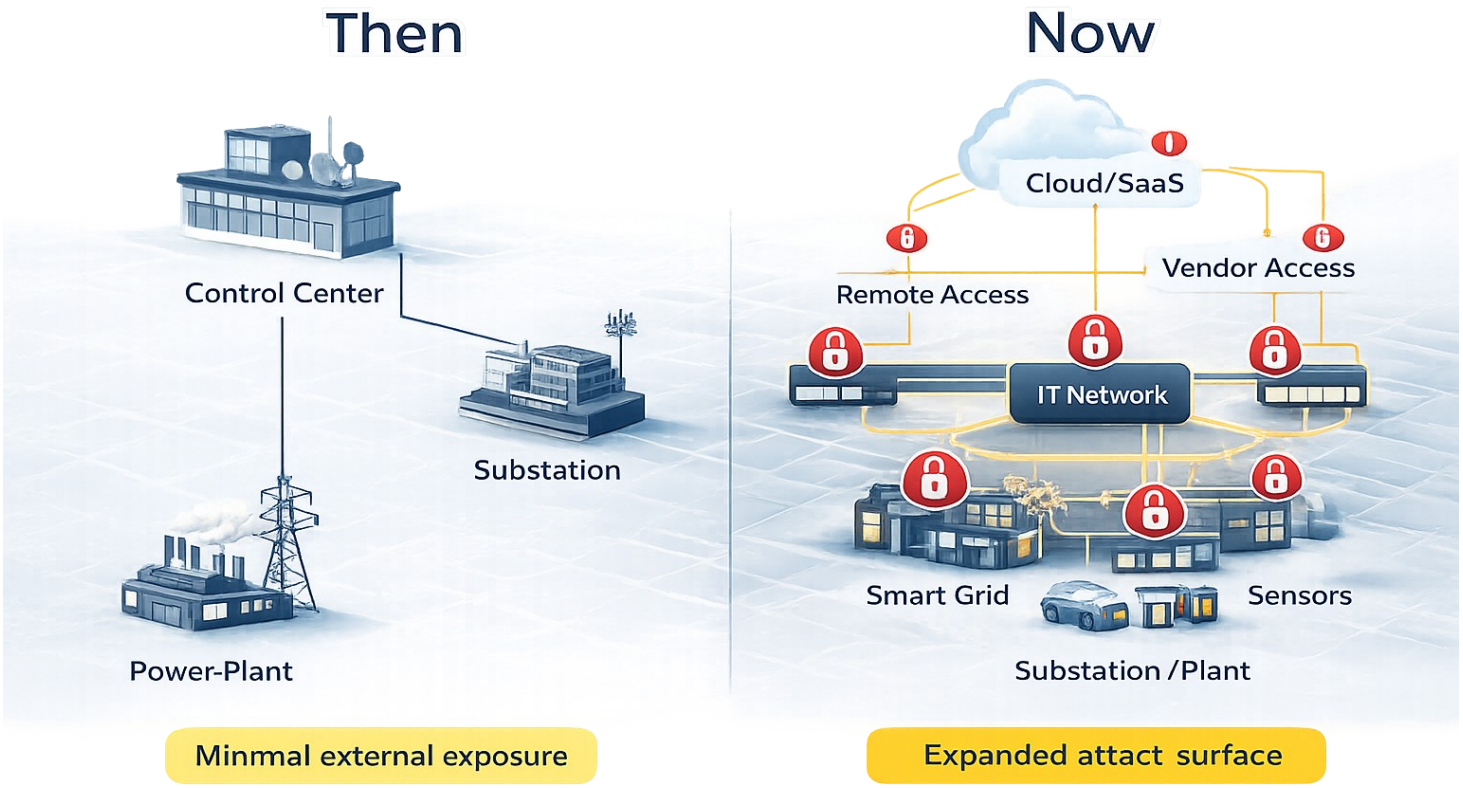
Why Energy Systems Are Critical Infrastructure



- Energy systems form the **backbone of modern society**, enabling healthcare, transportation, communications, and industrial operations.
- A disruption in electricity supply can trigger **cascading failures** across multiple sectors within minutes.
- Cybersecurity failures in this domain therefore extend beyond **financial loss** and directly affect **public safety** and **national stability**.
- This elevates energy cybersecurity from a **technical concern** to a **strategic necessity**.

Digitalization Expands the Energy Attack Surface

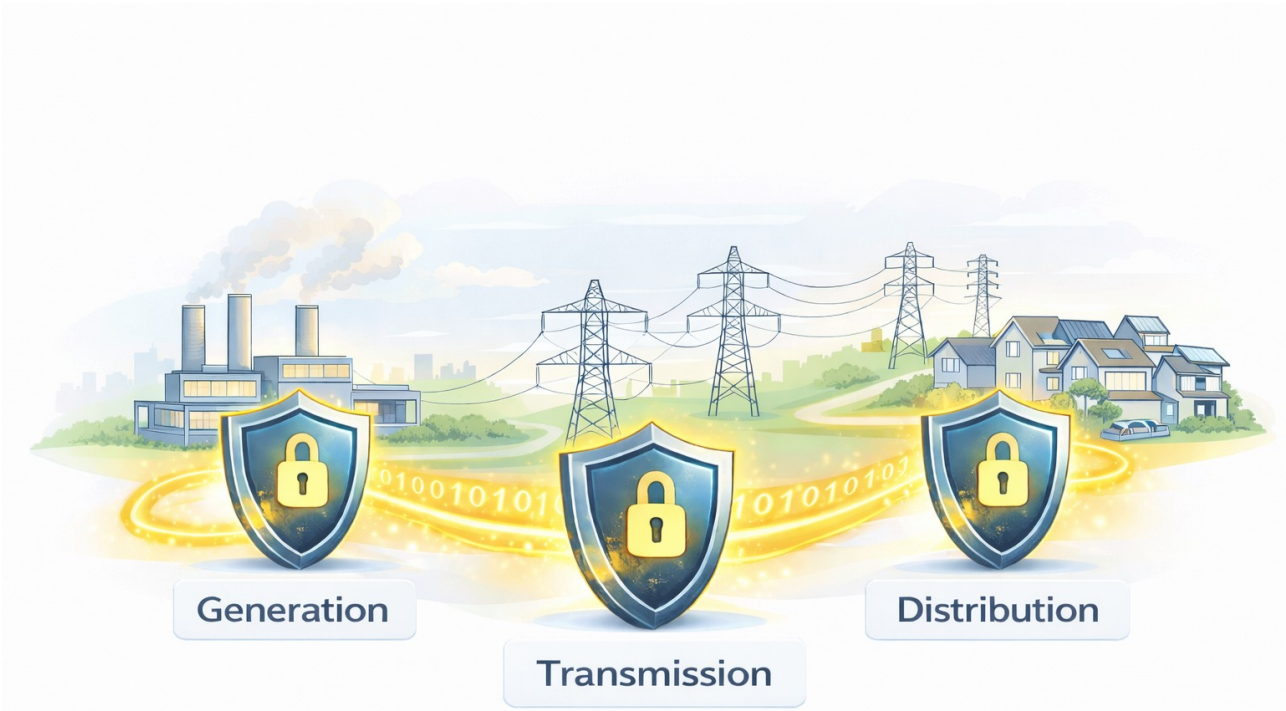
- Modern energy systems increasingly rely on **smart grids, Industrial Internet of Things (IIoT) devices,** and **remote control technologies**.
- While these improve **efficiency** and **observability**, they introduce new **connectivity points** that can be exploited.
- Every integration, whether **cloud-based, vendor-driven, or remote**, creates additional exposure to cyber threats.
- As a result, the **attack surface** of energy infrastructures has grown significantly over the past decade.



IT and OT Convergence Introduces Systemic Risk

- Information Technology (**IT**) systems manage **business data**, while Operational Technology (**OT**) systems control **physical processes**.
- In energy environments, these two domains are increasingly **interconnected**, enabling more efficient operations.
- However, this convergence allows threats originating in **IT environments** to propagate into **critical OT systems**.
- This creates **systemic risks** that require coordinated security controls across both domains.

Energy Value Chain Requires End-to-End Protection



- The energy sector operates across a continuous value chain: **generation**, **transmission**, and **distribution**.
- Each stage depends on the **integrity** and **availability** of the previous one, making the system highly **interdependent**.
- A cyber incident in one segment can **propagate downstream** and disrupt the entire supply chain.
- Therefore, cybersecurity must be applied **consistently across all layers**, not in isolation.

Threat Actors Target Energy Systems Differently

- Energy infrastructures attract a diverse range of **threat actors**, including **cybercriminals, insiders,** and **nation-state groups**.

Actor Type	Primary Motivation	Typical Access Vector	Energy-Specific Impact
Cybercriminals	Financial gain	IT network compromise, ransomware entry	Disruption of billing systems, temporary operational outages
Insiders	Error, misuse, or malicious intent	Legitimate access to OT/IT systems	Misconfiguration of control systems, unsafe operational states
Nation-state	Strategic / geopolitical objectives	Targeted intrusion into IT – lateral movement to OT	Coordinated disruption of grid operations, potential large-scale outages

Common Cyber Threats in Energy Environments

- Energy systems face a limited number of **recurring threat types**, but their impact is amplified due to **operational dependencies** and **real-time requirements**.
- According to **ENISA Threat Landscape 2023**:
  - **Ransomware** remains the dominant disruptive threat, responsible for a significant portion of incidents targeting critical sectors
  - **Denial-of-Service (DoS/DDoS**) attacks have increased, affecting availability of energy-related services and interfaces
  - **Supply chain attacks** continue to rise, exploiting trusted vendor relationships to gain indirect access
  - **Social engineering (e.g. phishing)** remains a primary initial access vector across sectors

Cyber Threats Have Physical Consequences

- Energy systems execute commands that directly affect **physical operations**.
- Unlike traditional IT environments, cyber incidents in energy infrastructures can lead to real-world outcomes such as **equipment malfunction** or **service disruption**.
- This is because energy systems depend on **continuous, real-time data exchange** between components.
- Even short disruptions or manipulated signals **can propagate rapidly** and affect system stability.
- Operational Implications:
  - **Loss of availability** → disruption of energy supply and service continuity
  - **Compromised communications** → incorrect or delayed control decisions
  - **Manipulated signals** → unsafe system states or equipment damage

The Necessity of Structured Cybersecurity

- Cybersecurity standards provide **structured frameworks** for implementing consistent and effective protection measures.
- They define **policies, controls,** and **best practices** tailored to organizational and sector-specific needs.
- In the energy sector, they help bridge the gap between **IT and OT security** requirements and support **compliance, auditing,** and **continuous improvement**.
- Different organizations provide guidance that helps **structure cybersecurity practices**. Together, they form a **complementary toolkit**, not competing approaches.

Role of Cybersecurity Standards, Frameworks and Sector-Specific Guidance

Layer	Role	Example
Governance & management	Defines how cybersecurity is organized, managed, and audited	ISO/IEC 27001
Sector-specific controls	Extends controls for energy utilities and process control environments	ISO/IEC 27019
Technical OT / ICS security	Defines lifecycle security requirements for industrial control systems	ISA/IEC 62443 series
ICS implementation guidance	Provides practical guidance for securing control systems environments	NIST SP 800-82
Risk-based cybersecurity framework	Provides a structured model for managing cybersecurity risk across critical infrastructure	NIST CSF
Sector guidance & best practices	Provides guidance on information sharing practices across energy subsectors (ISACs, CSIRTs)	Cyber Security Information Sharing in the Energy Sector
Threat intelligence & analysis	Provides analysis of cyber threats, trends, and threat actors affecting critical sectors (including energy)	ENISA Threat Landscape

Course progress

01. Introduction to Energy Cybersecurity

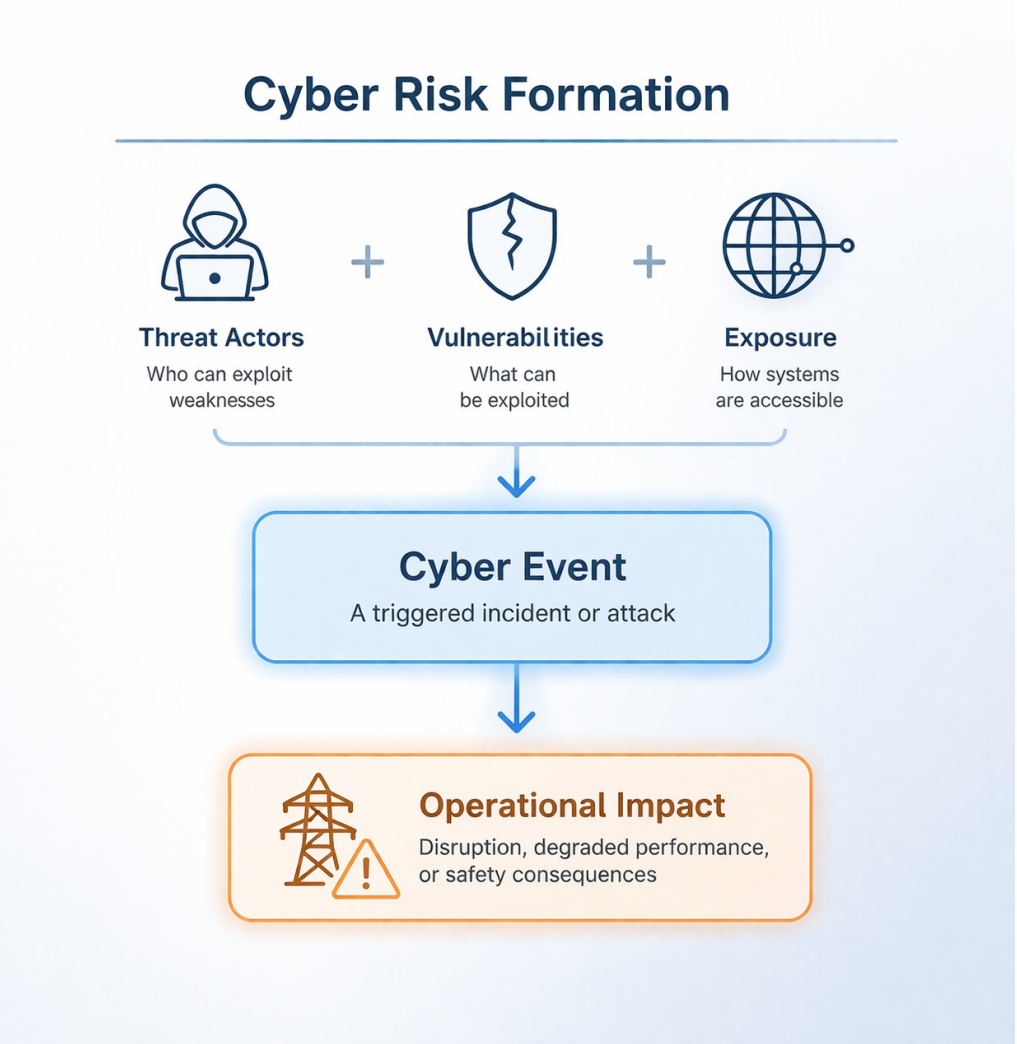
02. Understanding Energy Cyber Risks

03. Risk Assessment and Management

04. Business Continuity and Best Practices

What “Cyber Risk” Means in Energy Systems

- In energy environments, **cyber risk** refers to the potential of a cyber event to disrupt **system operation** or degrade **operational performance**.
- A cyber event becomes a risk when it affects **availability**, **control integrity**, or the **safe execution of processes**.
- These risks do not arise from isolated technical weaknesses but from the interaction between **vulnerabilities**, **threat actors**, and **system exposure**.
- Understanding cyber risk in this context requires assessing how technical issues can **propagate across interconnected systems** and ultimately influence **overall system behaviour**.



Where Cyber Risks Originate

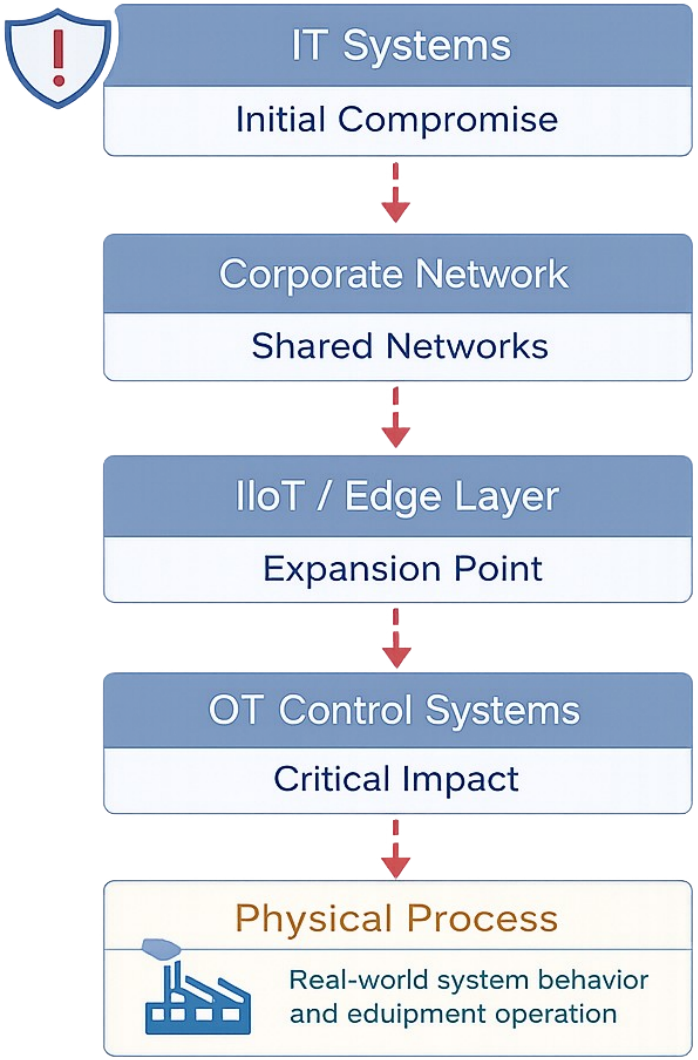
- Cyber risks in energy systems originate from multiple domains that interact within the same operational environment:
  - **IT environments**, which support business operation, such as enterprise systems, user endpoints, corporate networks
  - **OT environments**, which control physical processes, such as SCADA, PLCs, substations, control systems
  - **IIoT and edge devices**, which connect physical systems to digital platforms, such as smart meters, sensors, and remote monitoring technologies
  - **External dependencies**, such as vendors, cloud services, and remote access channels
- Each domain introduces distinct forms of **exposure**, but the most significant risks emerge from the interaction between domains rather than from isolated components.
- The most critical risks emerge at the **interfaces between domains**, where interconnected systems create pathways for **threat propagation**.

IT vs OT vs IIoT Risk Characteristics

- Cyber risks in energy systems differ significantly across **IT, OT and IIoT environments**, as each serves fundamentally different purposes within the same infrastructure.
- Treating these environments in the same way can be problematic, as applying IT-centric controls to OT or IIoT systems may introduce **additional operational risk** instead of reducing it

IT Environment	OT Environment	IIoT / Edge Layer
Data-centric systems	Process-centric systems	Connectivity-centric systems
Confidentiality & Integrity driven	Availability & Safety driven	Integrity & Availability driven
Ransomware, data breach, access abuse	Loss of control, unsafe states	Device compromise, unauthorized access
Can tolerate downtime to some extent	Downtime is critical	Limited resilience to disruption

IT/OT/IIoT Interconnection as a Risk Multiplier



- The integration of **IT and OT environments** improves visibility and operational efficiency, but it also introduces **new pathways for risk propagation**.
- In modern energy systems, these environments are no longer directly connected only through internal networks, but increasingly through **IIoT and edge devices** that act as intermediaries between digital platforms and physical processes.
- A compromise in IT systems **can propagate** through shared networks, remote access channels, and IIoT-enabled communication layers, eventually reaching critical OT systems.
- This interconnected structure creates **systemic risk**, where a localized issue can escalate across domains and lead to **operational disruption**.

Key Risk Categories in Energy Operations

- Cyber risks in energy systems can be grouped into core categories that directly impact **system operation and control**.
- These categories reflect how cyber events affect the ability to **operate**, **monitor**, and **trust system behavior**.
- These risks do not occur in isolation and can reinforce each other, ultimately affecting **grid stability**, **operational safety**, and **service continuity**.

Risk Category	Operational Impact
Loss of availability	Inability to operate systems, leading to downtime and service interruption
Loss of integrity	Incorrect or manipulated data and control commands, potentially causing unsafe or unstable operation
Loss of visibility	Reduced or lost monitoring capability, limiting situational awareness and decision-making
Unauthorized access	Direct or indirect control over critical systems, enabling malicious or unintended actions

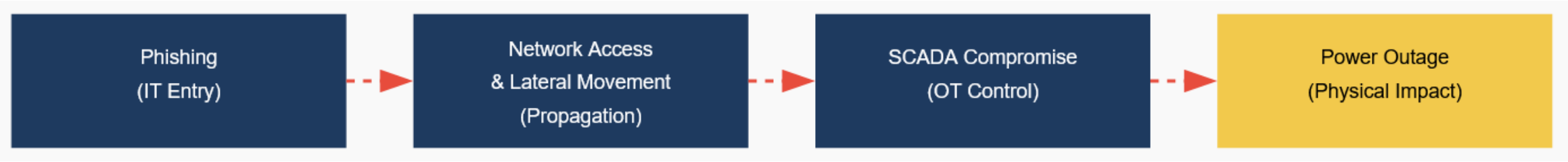
Vulnerabilities in Energy Infrastructure

- Energy systems often contain inherent vulnerabilities due to a combination of **technical limitations** and **operational constraints**.
- Many of these vulnerabilities are not the result of poor design, but of systems that were not originally built for **connectivity**, **interoperability**, or **exposure to cyber threats**.
- These factors increase both the **likelihood of compromise** and the **potential impact** of cyber incidents, particularly in highly interconnected energy environments.

Vulnerabilities in Energy Infrastructure (cont'd)

Category	Representative Patterns	Typical Implication
Structural and Technical	Legacy systems not designed for secure connectivity; limited patching capability, long equipment lifecycles, default or weak configurations	Increased attack surface and prolonged exposure to known vulnerabilities
Systemic and Architectural	IIoT and edge device integration, reliance on real-time communication, complex interdependencies across systems	Higher likelihood of risk propagation and operational disruption
Operational and Process-related	Maintenance constraints, limited downtime windows, fragmented responsibilities	Delayed response, inconsistent security controls
External and Supply Chain	Vendor dependencies, third-party access, cloud integration	Indirect compromise paths and expanded trust boundaries

Case Study: Ukraine Power Grid Attack (2015–2016)



- The Ukraine power grid attacks represent one of the first confirmed cases where a cyber operation led to **direct disruption of energy supply at scale**.
- Attackers initially gained access through **phishing campaigns targeting corporate IT systems**, allowing them to establish a foothold and move laterally within the network.
- From there, they pivoted into **SCADA-based control environments**, where they executed coordinated actions to **remotely disconnect substations**.
- This resulted in power outages affecting **hundreds of thousands of customers**, demonstrating how cyber attacks can propagate across systems and lead to **real-world operational impact**.

Source: https://www.boozallen.com/content/dam/boozallen/documents/2016/09/ukraine-report-when-the-lights-went-out.pdf

Case Study: Colonial Pipeline (2021)

- The Colonial Pipeline incident was caused by a **ransomware attack targeting corporate IT systems**, without direct compromise of operational control environments.
- The attackers gained access through **credential-based intrusion**, leading to the encryption of business systems and disruption of core administrative functions.
- Although the pipeline's OT systems were not directly affected, the organization halted operations due to **limited visibility into the extent of the compromise** and concerns over safe system operation.
- This resulted in a temporary shutdown of pipeline operations, causing **fuel supply disruptions across multiple U.S. regions** and highlighting the operational dependence on IT systems.
- The incident illustrates how disruptions in **supporting digital infrastructure** can propagate into critical operations, even in the absence of direct OT compromise.

Source: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

IT, OT & IIoT Infrastructure Components in Energy Systems

- In energy systems, cyber risk is shaped by how different infrastructure components **process data**, **execute control**, and **interface with the physical environment**.

- Rather than viewing IT, OT, and IIoT as layers, it is more useful to understand them as **distinct categories of assets** with **different exposure characteristics**.

Component Type	Examples	Security-Relevant Characteristics
User & Access Systems	Workstations, HMIs, remote access portals	High exposure to credential-based attacks and phishing entry points
Data & Processing Systems	Servers, cloud platforms, monitoring dashboards	Concentrate data flows and visibility, making them critical for integrity and decision-making
Control Execution Systems	SCADA, PLCs, RTUs	Translate digital commands into actions, where compromise leads to loss of control
Field & Interface Devices (IIoT)	Sensors, smart meters, edge gateways	Operate at the boundary, often with limited security and high physical proximity

Course progress

01. Introduction to Energy Cybersecurity

02. Understanding Energy Cyber Risks

03. Risk Assessment and Management

04. Business Continuity and Best Practices

Risk Assessment vs Risk Management

- **Risk Assessment** identifies and evaluates risk, while **Risk Management** defines and applies actions to control it.
- **Risk Assessment provides the foundation for Risk Management** by enabling informed decision-making.

Aspect	Risk Assessment	Risk Management
Objective	Identify and evaluate risks	Reduce. control or accept risks
Focus	Threats, vulnerabilities, impact	Controls, mitigation, decisions
Key Question	What can go wrong and how severe is it?	What should be done about it?
Scope in Energy Systems	Entry points (IT), exposure (IIoT), impact (OT)	Coordinated actions across IT, IIoT, and OT environments

Risk Management Structure

- **Risk management is** not a one-time activity, but **a continuous cycle** that adapts to changes in system architecture, threats, and operational conditions.

Phase	Purpose
Risk Assessment	Identification, analysis, and evaluation of risks affecting systems and operations
Risk Treatment	Selection and implementation of measures to reduce, avoid, transfer, or accept risk
Monitoring & Review	Continuous tracking of risk levels and control effectiveness as systems evolve

Risk Assessment & Management Process

Phase	Step	Actions
Risk Assessment	1. Scope Definition	System boundaries, scope definition, objectives across IT, OT, IIoT
	2. Asset & System Understanding	Asset inventory, system roles, dependency mapping
	3. Risk Identification	Threat identification, vulnerability discovery, exposure points
	4. Risk Analysis	Likelihood estimation, impact assessment
	5. Risk Evaluation	Risk prioritization, comparison against criteria
Risk Treatment	6. Control Selection	Control selection, feasibility and resource estimation
	7. Treatment Strategy Definition	Treatment strategy selection (mitigation, acceptance, transfer, avoidance)
	8. Control Implementation	Control deployment, safeguard integration across IT, IIoT, OT
Monitoring & Review	9. Monitoring & Review	Continuous monitoring, effectiveness evaluation, adjustment

Risk Assessment Methods

Method	Approach	Strength	Limitation	Typical Use in Energy Systems
Qualitative	Descriptive levels (e.g., Low, Medium, High)	Fast, simple, easy to communicate	Subjective, limited precision	Early-stage assessments, high-level risk overview
Semi-Quantitative	Scoring models and ranking (e.g., risk matrices)	Structured prioritization	Dependent on scoring assumptions	Asset prioritization across IT, IIoT, OT environments
Quantitative	Numerical estimation (probability, impact values)	High accuracy and comparability	Data-intensive, complex	High-criticality systems, safety analysis, investment decisions

Risk Assessment in IT, OT & IIoT Environments

- **Risk assessment in energy systems** follows a **common process**, but requires **domain-specific evaluation across IT, OT, and IIoT environments** due to fundamental differences in exposure, operation, and impact.

- Applying a uniform assessment model without domain adaptation can lead to **incorrect risk prioritization and ineffective controls**.

Domain	Primary Risk Focus	Assessment Consideration
IT	Data confidentiality and integrity	High exposure, frequent attack vectors, dynamic threat landscape
OT	Availability and safe operation	Safety-critical impact, low tolerance for disruption, limited intervention capability
IIoT / Edge	Connectivity and distributed exposure	Large-scale deployment, limited visibility, increased attack surface

Risk Treatment

- **Risk Treatment:** the selection and application of measures for risk reduction, taking into account operational impact, system limitations, and available resources across IT, OT, and IIoT environments.

Risk Treatment Option	Description	Practical Meaning in Energy Systems
Mitigation	Reduction of likelihood or impact	Security controls, segmentation, monitoring, system hardening
Avoidance	Elimination of the risk source	Removal of functionality, disabling connectivity, design changes
Transfer	Allocation of risk to third parties	Insurance, outsourcing, contractual agreements
Acceptance	Retention of risk within tolerance limits	No additional controls beyond monitoring and awareness

Monitoring & Review

- **Monitoring and review ensure that risk remains under control over time**, as systems, threats, and operational conditions evolve across IT, OT, and IIoT environments.

Activity	Purpose	Energy Context
Continuous Monitoring	Detect changes in system state, threats, and exposure	Real-time monitoring of system state, control signals, alarms, and device status across grid operations and field assets
Control Effectiveness Evaluation	Verify that implemented measures reduce risk as expected	Ensuring controls do not disrupt operations or safety
Change Management Integration	Reassess risk when systems, configurations, or operations change	System upgrades, maintenance activities, integration of new assets (e.g., IIoT)
Periodic Review	Re-evaluate risks and update decisions based on new conditions	Regulatory updates, evolving threats, and infrastructure changes

Risk Management in Cyber-Physical Energy Systems

- Risk management in energy systems **often fails** not due to lack of controls, but **due to incorrect assumptions and misaligned decisions**:
  - **Application of IT controls in OT environments** without considering operational impact
  - **Evaluation** of systems in isolation, **ignoring interdependencies**
  - **Underestimation of risk** from IIoT devices and field exposure
  - **Treatment of risk assessment as a one-time activity**, not a continuous process
- Operational Impact:
  - Unplanned service **disruptions or downtime**
  - **Unsafe system states**
  - **Loss of system visibility**
  - **Escalation of local issues** into wider system impact

Course progress

01. Introduction to Energy Cybersecurity

02. Understanding Energy Cyber Risks

03. Risk Assessment and Management

04. Business Continuity and Best Practices

From Risk Management to Business Continuity

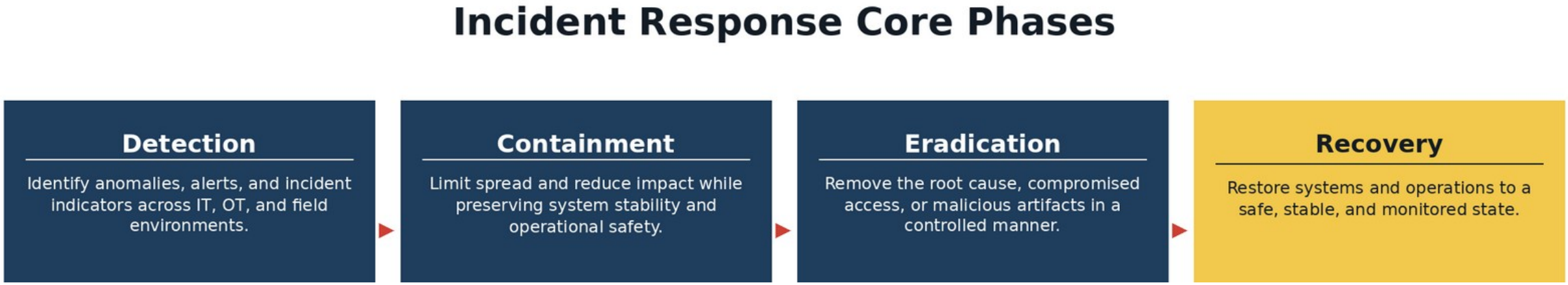
- **Risk management** reduces risk, but **does not eliminate** it.
- **Disruptions can still occur due to:**
  - unforeseen events
  - system complexity
  - operational constraints
- **Business continuity focuses on:**
  - responding to incidents
  - restoring systems and data
  - maintaining operation under disruption
- This is where **incident response**, **recovery planning**, and **operational readiness** become critical.

Business Continuity in Energy Systems

- In Energy systems, **maintaining continuity requires** keeping systems operational or returning them to a safe state without disrupting physical processes.
- **Business Continuity in Energy systems depends on:**
  - system availability (OT)
  - data and monitoring capability (IT)
  - field operations and controlled access (IIoT)
- **Disruptions must be handled to ensure:**
  - minimal service interruption
  - stable system behavior
  - safe and controlled restoration of operations

Incident Response in Energy Systems

- **Incident Response defines how organizations handle incidents** without disrupting system operation or creating unsafe conditions.



- **Operational Constraints**
  - Response actions must not disrupt ongoing operations (OT)
  - Limited ability to isolate or shut down systems
  - Coordination required across IT, OT, and field teams (IIoT)
- **Response actions must be adapted to the system**, not applied uniformly as in IT environments.

Data Backup and Recovery Planning

- **Backup and Recovery** define **how systems and data are restored safely** and in the correct order after disruption or compromise.
- **Scope in Energy Sector**
  - IT systems and operational **data**
  - OT system **configurations**
  - IIoT devices **settings**
- **Recovery Requirements**
  - **Backups must be available** even during cyber incidents (e.g. offline / isolated storage)
  - **Recovery must follow a controlled sequence**, not parallel restoration
  - **Systems must be validated** before being returned to operation

Backup Strategies

Approach	Description	Typical Use
Full Backup	Complete copy of data and systems	Periodic baseline for recovery
Incremental Backup	Only changes since last backup	Storage efficiency and frequent updates
Offline / Cold Storage	Backups stored offline or isolated	Protection against ransomware and compromise
Redundant Storage (RAID)	Data replication across disks	High availability and fault tolerance

Selection Criteria

- **Recovery Time Objective (RTO):** target time required to restore system functionality
- **System Criticality and Operational Impact:** impact of system unavailability on operations
- **Data Loss and Integrity Risk:** likelihood and impact of data loss or corruption

Effective Recovery in Energy Systems

- Recovery in energy systems **must ensure that systems return to operation** without introducing instability or unsafe conditions.
- **Poor recovery can cause more damage** than the initial incident.

Poor Recovery	Effective Recovery
Restoring systems in parallel without coordination	Controlled restoration sequence based on system dependencies
Reconnecting systems without validation	Validation of system state before reconnection
Ignoring dependencies between IT, OT, and field devices	Gradual return to operation with monitoring

Staff Awareness and Training

- In energy systems, **human actions can directly affect system operation and safety**.
- **Staff must be able to execute procedures as defined** during normal operation, incident response, and system recovery.
- **Operational Competencies:**
  - **Understanding system impact** when interacting with IT, OT, and IIoT systems
  - **Execution of operational and recovery procedures as defined**
  - **Controlled use of access and privileges** during normal and critical conditions
  - **Coordination between teams** during incident handling and system restoration
  - **Consistent application of procedures** under pressure
  - **Avoidance of unauthorized or unintended actions**
  - **Support of stable and predictable system behaviour**

Best Practices in Energy Cybersecurity

- **Cybersecurity practices in energy systems** must be adapted to operational requirements, system constraints, and physical impact.
- **Security measures must support system operation and safety** without causing disruption or instability.
- **Core Principles**
  - **Apply controls** based on system criticality
  - **Adapt IT security practices** to OT and IIoT environments
  - **Maintain network and system separation** between IT, OT, and IIoT environments
  - **Continuously monitor and update controls** based on system changes

Operational Takeaways

- **Cyber risk extends beyond IT** and can affect physical system operation
- **System behaviour is defined by interactions** between IT, OT, and IIoT components
- **Risk** must be **assessed and managed based on system impact**, not only vulnerabilities
- **Incidents** must be **handled without disrupting** system stability or safety
- **Recovery** must **follow controlled and validated procedures**
- **Human actions** directly **influence system operation and outcomes**
- **Security measures must be adapted** to system constraints and operational requirements
- The **objective** is to **maintain safe and stable system operation under all conditions**.

Thank you

Please send all questions to:
pkyranoudi@tuc.gr
antonios.ntib@tu-braunschweig.de