Cybersecurity Essentials and Management (Energy Sector)

CSP001

Topic 2/10: Foundational Knowledge and Taxonomy of Energy Cybersecurity and Body of Knowledge

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Cyberattacks on Energy

Energy Industry

Energy Industry as a Prime Cyberattack Target

- Disruption can lead to widespread chaos, economic losses, and endanger lives.
- Critical infrastructure: Power grids, oil refineries, and nuclear facilities are attractive targets.
- Economic motives: Cybercriminals seek financial gain through ransomware, extortion, or market manipulation.
- State-sponsored attacks: Geopolitical tensions may drive nations to target rival energy infrastructures for strategic advantage.

Cyberattacks on Energy

Why Cybersecurity is Crucial?

Energy Industry as a Prime Cyberattack Target

- Infrastructure vulnerability: Aging systems, interconnected networks, and legacy protocols are susceptible to exploitation.
- Data integrity: Manipulating energy consumption data can disrupt supply-demand balance and cause economic instability.
- Operational disruption: Malware or denial-of-service attacks can halt energy production and distribution, causing widespread outages.
- Environmental risks: Tampering with control systems may lead to environmental disasters, endangering ecosystems and public health.

Cyberattacks on Energy

Increasing Complexity in Cyber Landscape

Energy Industry as a Prime Cyberattack Target

- Attacks on energy infrastructure can serve as forms of cyber warfare or terrorism, making energy vulnerabilities matters of national security.
- Energy organizations navigate a multifaceted cyber landscape amid geopolitical uncertainties.
- Responsibilities extend beyond cybersecurity to include decarbonization and facilitating energy transition.
- Accommodating complex grid connections and infrastructure demands amidst dynamic regulatory environments.

Backbone of the Economy

Energy Industry as a Prime Cyberattack Target

- Energy is indispensable for critical economic sectors:
  - (i) Manufacturing
  - (ii) Agriculture
  - (iii) Transportation
- Interruptions in energy supply can lead to significant disruptions, halting production and logistics.

Case Study: Colonial Pipeline

Case Study: Colonial Pipeline Cyberattack

Energy Industry as a Prime Cyberattack Target

- In 2021, Colonial Pipeline, the largest U.S. pipeline operator, was hit by a ransomware cyberattack.
- Shutdown of Colonial Pipeline disrupted fuel supply to half of the East Coast, resulting in price spikes and fuel shortages.
- Colonial Pipeline incident highlighted the sector's susceptibility to cyber threats.
- Identified vulnerabilities, such as unfilled cybersecurity management positions and inactive VPNs, underscored systemic weaknesses.

Case Study: Colonial Pipeline

Case Study: Government Alerts and Precautions

Case Study: Colonial Pipeline

- In April 2022, the U.S. government issued an alert warning energy companies of high cyberattack risks.
- Recommendations included:
  - Enabling multi-factor authentication
  - Regularly changing system and device passwords
- Energy companies must prioritize cybersecurity measures to protect both their operations and consumers from potential cyber threats.
- Proactive measures are essential to mitigate risks and ensure resilience in the face of evolving cyber threats.

Case Study: Colonial Pipeline

Ransomware Attacks

Case Study: Colonial Pipeline

Major threat: Cybercriminals use malware to block access to an organization's data or threaten to leak sensitive information.

Mitigation strategies:

- Develop robust incident management response plans.
- Secure computer systems proactively.

Case Study: Volue Technology

- Norwegian green energy supplier Volue Technology experienced disruptions in 44 countries due to ransomware attacks.

Mobile Phishing

Growing vulnerability: Energy sector witnesses a 161% increase in phishing attacks targeting mobile devices.

Risks: Cybercriminals exploit employee mobile devices containing sensitive information.

Response: Employee training on identifying and thwarting phishing attempts.

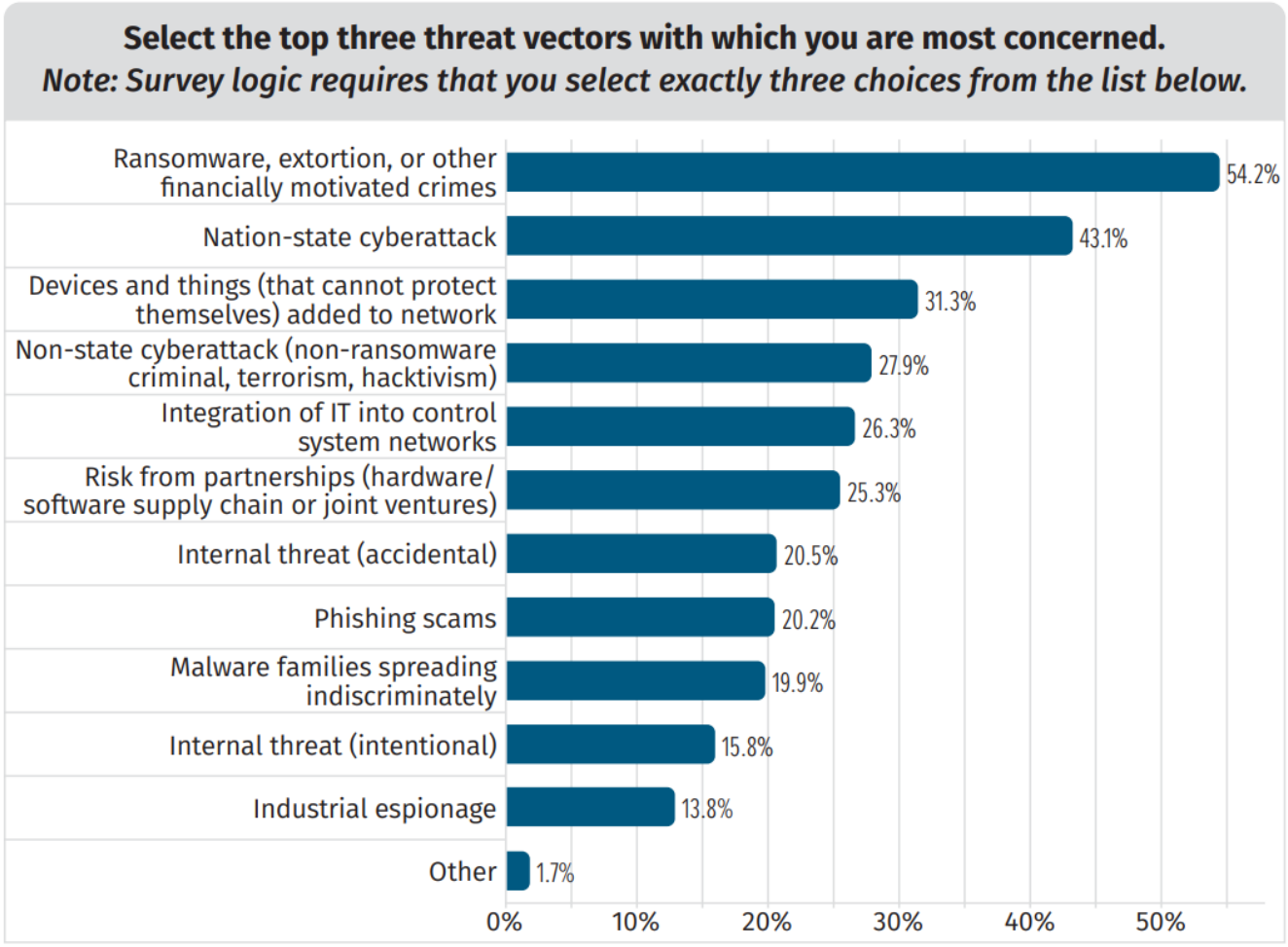
Supply Chain Attacks

Threat overview: Cybercriminals gain unauthorized access to company networks through third-party vendors with weaker cybersecurity protocols.

Countermeasures: Mandate cybersecurity best practices for third-party vendors. Ensure effective incident response plans are in place.

Top Attacks

Top Threat Vectors on Energy



Bristow, M. (2021). A sans 2021 survey: Ot/ics cybersecurity. *eng. In*.

Risk Over Time

Risk Over Time

Table 3. Threat Actor Risk Over Time

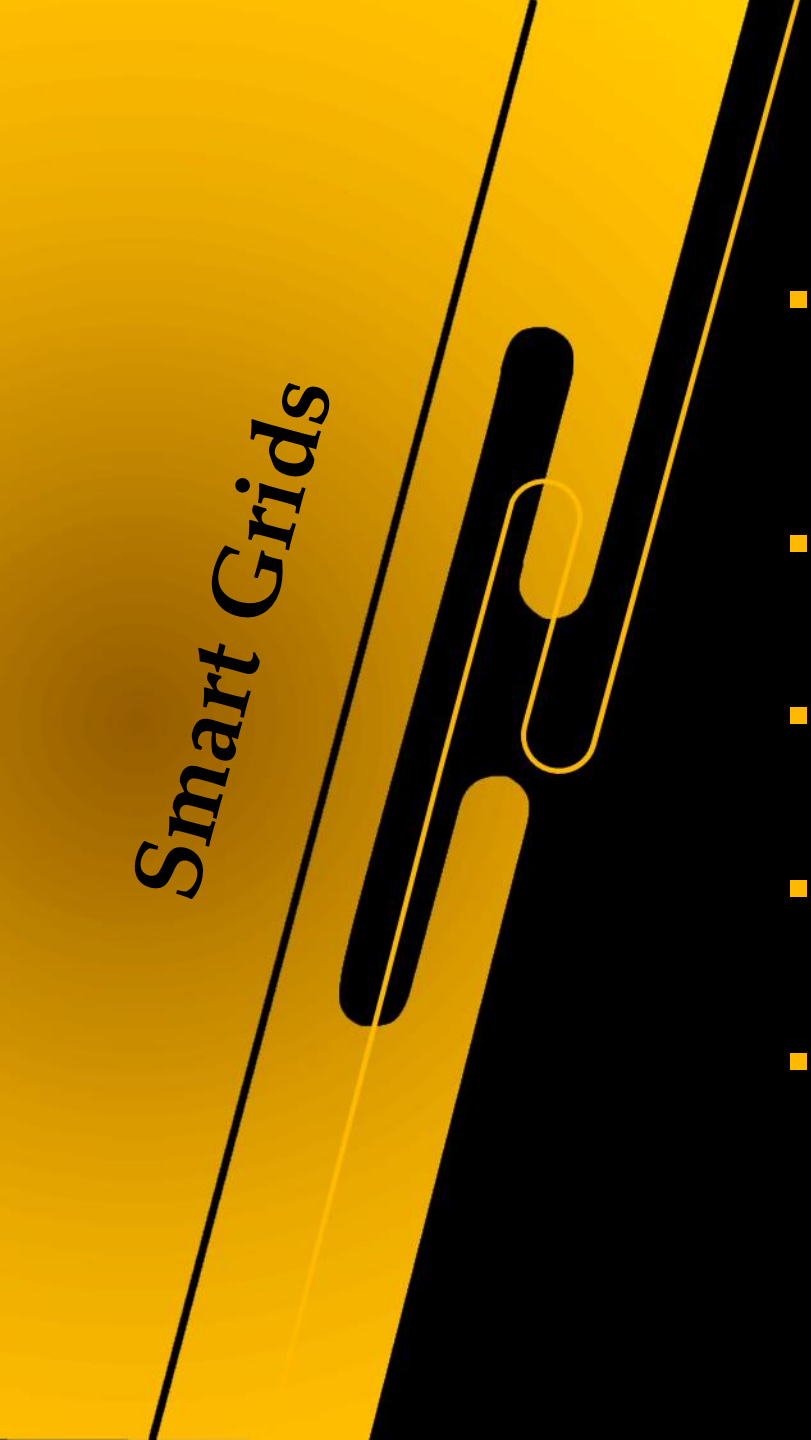
Answer Choices	2021 Rank	2019 Rank	Change
Hackers	1	1	—
Organized crime	2	5	+3 ▲
Current service providers, consultants, contractors	3	3	—
Current employees	4	2	-2 ▼
Activists, activist organizations, hacktivists	5	6	+1 ▲
Unknown (sources were unidentified)	6	7	+1 ▲
Foreign nation-states or state-sponsored parties	7	4	-3 ▼
Domestic intelligence services	8	11	+3 ▲
Former equipment providers	9	12	+3 ▲
Former employees	10	10	—
Current equipment providers	11	8	-3 ▼
Competitors	12	9	-3 ▼
Suppliers or partners	13	13	—
Former service providers, consultants, contractors	14	14	—
Other	15	15	—

Bristow, M. (2021). A sans 2021 survey: Ot/ics cybersecurity. *eng. In*.

Leading Attack Vectors

Observation that leading attack vectors, while not remote access technologies, leverage interconnectivity as an enabling function

- Exploit of public-facing applications—What level of connectivity or control is possible from applications exposed to the internet, and what architecture is in place to mitigate risks to the ICS?
- Internet-accessible devices—Is device connectivity bypassing the DMZ?
- Spear-phishing attachment—Properly configured OT environment should not have direct access to email services directly, yet phishing continues to be a relatively high-ranked vector.

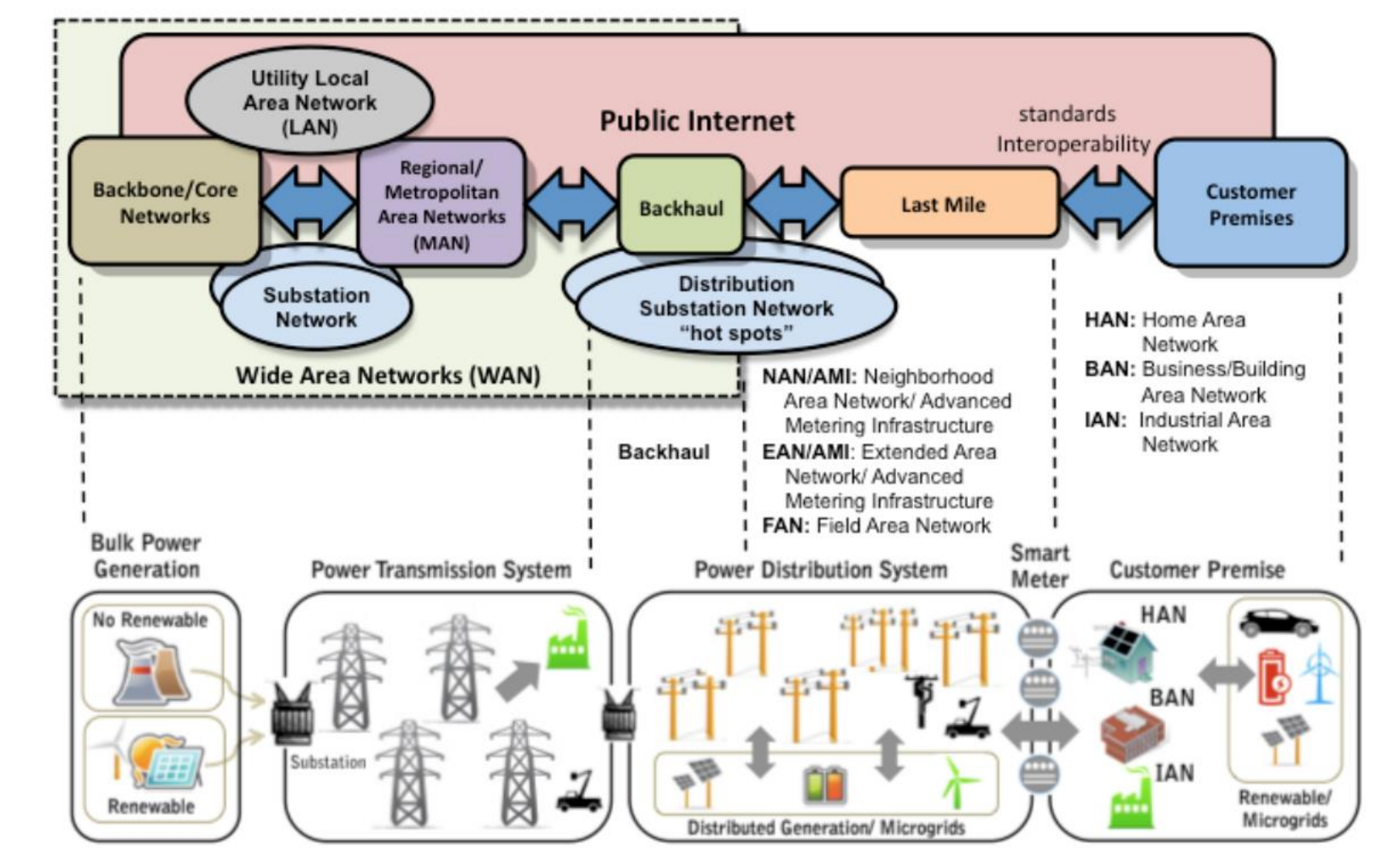


Smart Grids

- Smart grids integrate actions from all connected end-users. Provide bidirectional communications between end-users and grid operators
- Consumers (households, enterprises) connected to DSOs via smart meters and WAN network
- Smart meters demarcate DSO ICT infrastructure and Customer Premises Network
- Increase automation and control capabilities in transmission and distribution grids
- Existing technologies (EMS, DMS, SCADA) being updated for smart grids

Smart Grids

Smart Grids



https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids

Smart Grids

Smart Grids

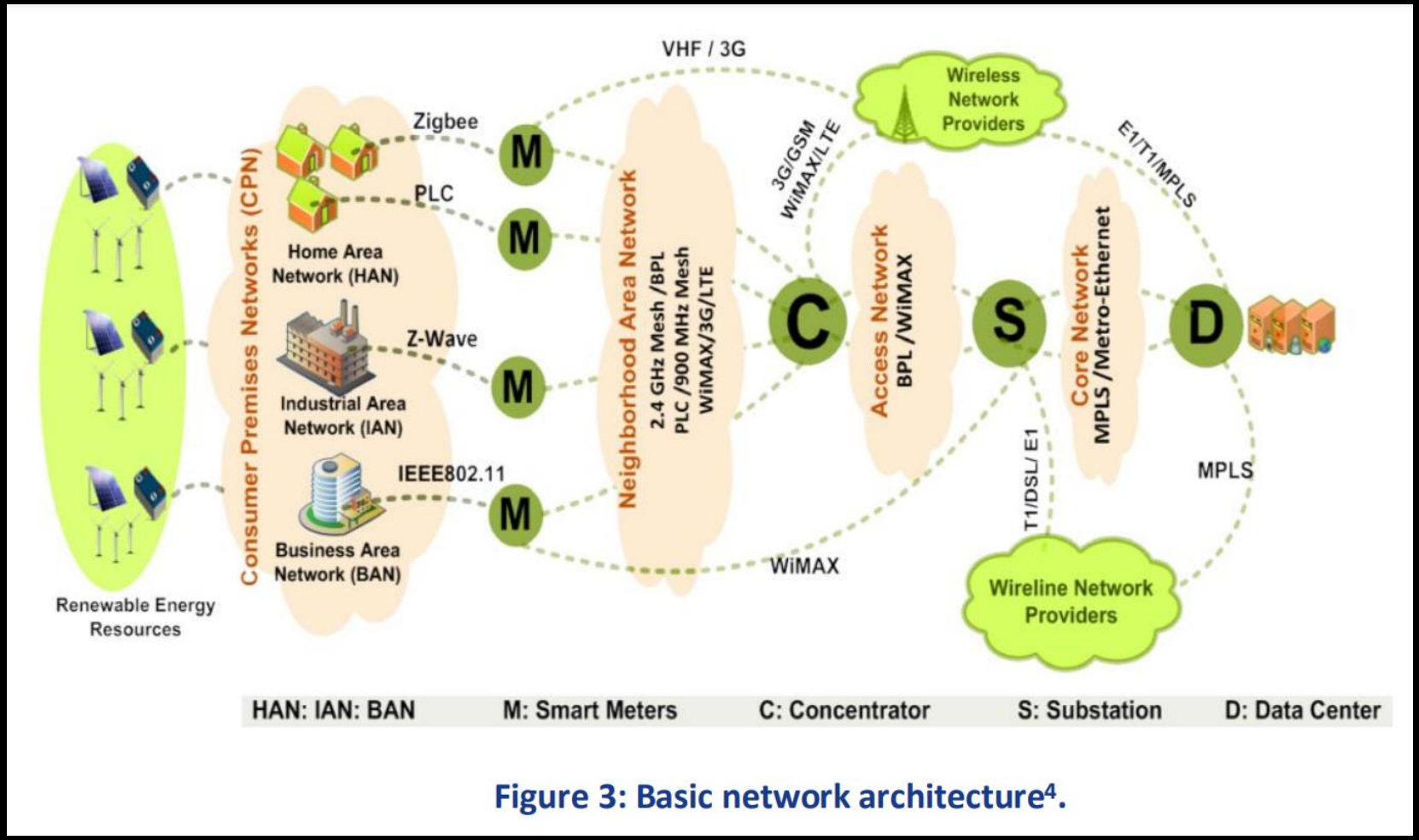


Figure 3: Basic network architecture[4].

https://www.enisa.europa.eu/publications/communication-network-interdependencies-in-smart-grids

Smart Grids

Communication in Smart Grids

- Transport Layer Security (TLS): Cryptographic protocol for network communication security, using asymmetric cryptography and symmetric encryption for data protection. SSL v3 is an outdated predecessor.
- IEC 62351: Standard for securing protocols like IEC 60870, IETC 61850, IEC 61970, and IEC 61968. Features include TLS encryption, node authentication, and message authentication.
- IEV IEC 61850-90-12: Provides guidelines for WAN engineering, especially focusing on protection, control, and monitoring between substations and control centers.

Communication in Smart Grids

- Internet Protocol Security (IPSec): Protocol suite for protecting IP communications with authentication and encryption, operating on the Internet Layer.
- Secure Shell (SSH): Protocol for secure remote connections, applying encryption for data protection. Requires an operational SSH server on the remote machine.
- DNP3 Secure: Enhanced version of DNP3 protocol with added security measures like authentication and data encryption, compliant with IEC 62351-5 standard.
- Virtual Private Network (VPN): Conceptual private network over public networks like the Internet, using tunnelling protocols and encryption for secure communication and data confidentiality.

Challenges

Challenges in Wind Plant Cybersecurity

- Wind plants exhibit diverse automation and control systems, posing challenges for addressing cybersecurity risks, mitigations, and regulations at a sector-wide level.
- Variability in wind plant designs includes differences in size, generation capacity, network design, communications protocols, control center structures, maintenance practices, and geographic locations.
- Establishing a universal set of security requirements is hindered by these variations, although sharing general security guidance remains feasible.
- Attack surface refers to the cumulative exposed systems, networks, or cyber assets vulnerable to adversarial targeting, which can result in malicious impacts.

Substation Components

Collector Substation Communications

- Utility Transmission Control Center: This component serves as the central hub for managing and controlling the transmission of electricity within the regional power grid. It oversees the operation of substations, monitors grid performance, and coordinates power distribution across the network.
- Supervisory Wind Plant Operations Control Center: This control center is responsible for supervising and managing the operations of the wind plant. It monitors the performance of wind turbines, controls power generation, and ensures optimal efficiency and safety of the wind plant operations.
- Forecasting Server: This server utilizes weather data and predictive algorithms to forecast future wind conditions. It helps optimize power generation by providing insights into expected wind patterns, enabling better planning and scheduling of wind energy production.

Substation Components

Collector Substation Communications

- Substation Network: This network connects various substations within the wind plant's infrastructure. It facilitates the transmission and distribution of electricity between different components of the wind plant and the wider power grid.
- Wind Plant - Local Network: This network encompasses the internal communication infrastructure of the wind plant. It connects various components such as turbines, monitoring systems, and control centers, facilitating data exchange and coordination for efficient operation and management of the wind plant.

Internal Threat Groups

Asset Owner/Operator (AOO) or Aggregator: Responsible for administrative operations and maintenance, Potential for inadvertent exposure of critical information.

Original Equipment Manufacturer (OEM): Designs and implements power production equipment, Vulnerable to targeted attacks and supply chain compromises.

Utility: Recipient of generated power, with potential indirect threats if compromised.

Maintainers and Technicians: Essential for routine upkeep, lacking consistent security standards.

Integrator/Installers: Have privileged access to wind plant systems, prime targets for compromise.

Third-Party Services and Data Collectors: Integral to data aggregation, software solutions, requiring meticulous vetting.

External Threat Groups

External Threat Groups

Landowners: May inadvertently damage assets during routine activities.

Activist Groups: Motivated by environmental concerns, pose risks of physical attacks or protests.

Cyber & Physical Criminal Elements: Target wind plants for financial gain or malicious intent, increasingly through ransomware attacks.

Nation-State Actors: Engage in espionage and reconnaissance activities, posing significant threats to wind infrastructure and national security interests.

External Threat Groups

Potential Attack Vectors

Attack Vectors Overview: Means by which adversaries gain initial access to networks or systems.

Classified into three groups:

- Close, Physical Access
- Remote, Cyber-Enabled Means
- Blended Cyber-Physical Attacks

Types of Attack Vectors: Physical access at wind turbines or collector substations. Cyber access via remote connections. Targeting of transient cyber assets, e.g., field technician maintenance equipment.

Industroyer in Ukraine

Use Case: Industroyer in Ukraine 2016

December 2016: Ukrainian transmission operator Ukrenergo cyberattack at a single transmission substation near Kyiv.

Modular malware indicated potential for a larger, synchronized attack.

Industroyer: Modular malware framework enabling direct interaction with ICS equipment via industrial protocols.

Industroyer2: A revised version in April 2022 targeted a Ukrainian energy provider, limited to IEC 60870-5-104.

Industroyer2: Configurable with wipers deployed to destroy data and evidence post-execution.

Industroyer in Ukraine

Industroyer in Ukraine

1. Initial Access: Attackers gained access to the Ukrainian transmission substation's network, possibly through stolen credentials or vulnerabilities in the network perimeter.
2. Malware Deployment: Industroyer, a modular malware framework, was deployed, enabling direct interaction with ICS equipment via industrial protocols (IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OPC).
3. Enumeration and Reconnaissance: Malware modules enumerated the substation environment to identify targets and assess system vulnerabilities.
4. Manipulation of Control: Attackers manipulated physical process control within the industrial environment, changing setpoint values or parameters, such as opening substation breakers.

Industroyer in Ukraine

Industroyer in Ukraine

5. Denial of Service (DoS): A DoS module rendered specific series of Siemens Siprotec relays unresponsive, disrupting normal device functionality.
6. Loss of Safety: The malware disrupted protective relay functionality, leading to a loss of safety event within the substation.
7. Theft of Operational Information: Attackers compromised the data historian, stealing critical operational information about the substation environment.

Freeman, S. G., Kress-Weitenhagen, M. A., Gentle, J. P., Culler, M. J., Egan, M. M., & Stolworthy, R. V. (2024). *Attack Surface of Wind Energy Technologies in the United States* (No. INL/RPT-24-76133-Rev000). Idaho National Laboratory (INL), Idaho Falls, ID (United States).

Lessons Learned: Industroyer in Ukraine

Protocols Vulnerability: Adversaries exploited vulnerabilities in widely-used industrial protocols, highlighting the importance of securing communication protocols and monitoring for anomalous behaviors.

Modular Malware Adaptability: Industroyer's modular nature allowed adversaries to adapt the malware for various targets, emphasizing the need for flexible and adaptive defense mechanisms.

Early Detection and Response: Timely detection of anomalous activities and rapid response are critical to mitigating the impact of cyberattacks on critical infrastructure.

Enhanced Monitoring and Access Control: Implementing enhanced monitoring and access control mechanisms can help identify and prevent unauthorized access to critical systems and data.

Cross-Sector Collaboration: Collaboration between sectors and sharing threat intelligence can improve resilience against cyber threats, particularly those targeting critical infrastructure.

Challenges

Cybersecurity Challenges in the Energy Sector

Real-time Requirements: Some energy systems require rapid response, limiting the implementation of standard security measures due to latency issues.

Cascading Effects: Interconnected electricity grids and gas pipelines can lead to widespread outages or supply shortages across borders.

Legacy Systems and New Technologies: Integration of legacy infrastructure with modern automation and control technologies, such as IoT devices, poses cybersecurity risks.

Governance and ecosystem

1. Is there an up to date list of the most critical IT systems and OT systems, and what are the relevant cyber threats that could affect them?
2. Do we have an overall cyber-risk management program (also known as information security management system), and does it cover both IT and OT systems?
3. Do we have a good understanding of our overall ecosystem, our dependencies on other organisations in and outside the sector, our suppliers and vendors?

Protection

1. Do we have a vulnerability management program in place that ensures that all IT and OT systems are timely patched and updated? How does this program cover our legacy systems?
2. Do we have protection in place for remote access of IT and OT systems, such as two-factor authentication, particularly for privileged (administrator) accounts?
3. Do we have segmentation in the organisation's network, and do we implement zero-trust network architecture principles.
4. Is our staff aware of phishing threats and other forms of cyber-attacks? Is there a staff program for training and awareness raising on cyber security?

Defense

1. Do we have clear roles and contact points for incident response, both for IT and OT incidents?
2. Do we have up-to-date incident response plans and procedures? Did we test them recently?

Resilience

1. Do we have appropriate backup and recovery procedures in place?
2. Do we have up-to-date business continuity and contingency plans? Did we test them recently?
3. Do we have crisis management procedures in place, do we know who to contact in case there are attacks or incidents?

ENISA - PREPARING FOR CYBER ATTACKS IN THE ENERGY SECTOR

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com