NATIONAL CONFERENCE

CYBER SECURITY IN POWER SECTOR: COLLABORATION IS THE KEY TO SUCCESS

NEW DELHI 6-8 JAN, 2025

CYBER SECURITY RISKS AND PREVENTIVE MEASURES IN SMART GRIDS

JAYANT SINHA

SR. PRINCIPAL CONSULTANT

(ENERGY TRANSITION & UTILITIES)

Email: jayant.sinha@entruistpower.com

URL: https://entruistpower.com/

LEARNING FROM HISTORY: CYBERATTACKS ON INDUSTRIAL CONTROL SYSTEMS

Colonial Pipeline, USA May 2021: Ransomware attack in which hackers gained entry into company's computer network. The company had to pay a ransom of $4.4 million in exchange for decryption tool to restore network.	• **Impact**: Caused acute fuel shortage, leading to sharp rise in oil prices.
CPC Corp, Taiwan May 2020: Taiwan's state-owned petroleum and natural gas company was exposed to ransomware attack, using USB flash drive to infect company's computer network.	• **Impact**: The payment system of CPC Corp was adversely affected in the attack.
Ukraine Power Grid Dec 2015: In a Trojan attack on Ukraine's power distribution system, the hackers targeted a power substation, disabling circuit breakers one after another.	• **Impact:** The affected power lines suffered loss of power for six hours, but it took several months to make the substation control systems fully operational.
Bowman Avenue Dam 2013: Hackers attacked the Supervisory Control and Data Acquisition (SCADA) system of the New York dam by exploiting a susceptible network connection.	• **Impact:** The damage was averted as the dam sluice gate was manually disconnected for maintenance.
Iran Nuclear facility 2010: Iran's nuclear facility suffered Stuxnet worm attack, allegedly engineering by US National Security Agency and Israeli Intelligence to target programmable logic controllers (PLCs).	• **Impact:** Unusual failure rate of centrifuges for uranium enrichment, which was detected by inspectors of International Atomic Energy Agency during inspection.

WHEN CYBER ATTACK CAUSED NATIONAL POWER GRIDS TO CRASH

Ukraine Power Grid (Dec. 2015)

- Cyber attack caused blackout in Ukraine, affecting 230,000 people
- Sophisticated malware used to gain access to control systems of three regional power distribution companies
- Phishing emails sent to gain initial access and malware deployed to disrupt grid control systems
- Blackout lasted several hours, disrupting daily life and causing economic losses
- Affected power companies worked with international cybersecurity experts to restore the grid

Israel Water and Power Authority (2020)

- In April 2020, the Israel Water & Power Authority were targeted by a cyber attack that disrupted electricity & water
- Ransomware used by attackers to encrypt critical power systems who demanded ransom to restore access.
- Attack caused temporary disruptions in SCADA systems of Israel's utility networks
- The authorities worked with cybersecurity firms to remove the ransomware and restore the systems

India's Grid failure (Oct. 2020)

- Cyber attackers targeted Indian power grid, causing disruptions in Maharashtra and other states
- Malware injected to gain access to control systems and disrupt operations in regional and state load dispatch centres (RLDC/ SLDC)
- Caused power outages in multiple states, affecting millions of residents causing economic losses
- Actions taken by Grid Controller & Computer Emergency Response Team (CERT-in) to restore power



NEED FOR SMART GRID CYBERSECURITY

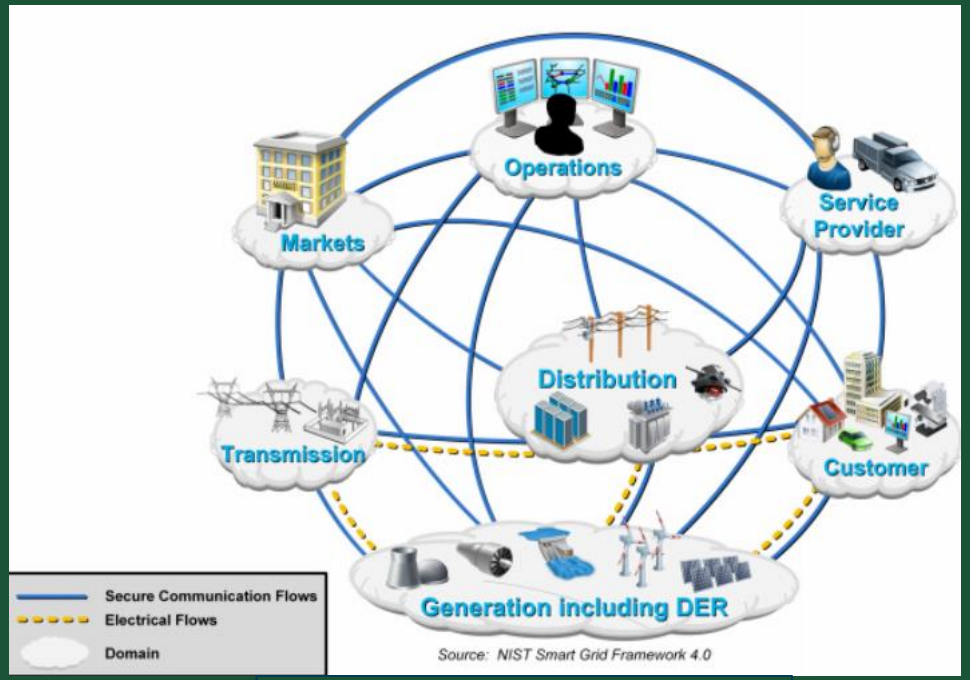
Substantial dependence on **bidirectional communication** with smart grid assets and networks

Increased digitalization runs the risk of data breaches and network vulnerabilities exposing smart grids to the possibility of cyber-attacks

Control system **malware** like Stuxnet, targets SCADA systems which compromises grid security

Virtual private networks (VPNs), public key infrastructure (PKIs), intrusion prevention/ detection systems (IPS/ IDS), firewalls and anti-virus are common **cybersecurity measures**

Electric Power Research Institute (EPRI), National Institute of Standards and Technology (NIST), Smart Grid Interoperability Panel (SGIP) and IEEE have laid down **standards for cybersecurity implementation**



Source: NIST Smart Grid Framework

SMART GRID CYBERSECURITY IMPLEMENTATION

Aims

End-to-End Security: Security measures implemented at every point in the smart grid system - smart metering, database and applications

Multi-layered Defense: Multiple layers of security to protect against different threat vectors

Software updates and patches: Regularly updates and patches to address vulnerabilities

Incident Response Plan: Plan to respond quickly to cyber security threats

Outcomes

Confidentiality

- Prevent unauthorized access of highly secured information e.g. energy metering, electricity usage, customer data and control commands.

Integrity

- Prevent modification of critical information of field sensors, smart meters, utility data and control systems which might disrupt grid operations, communications and reliability.

Availability

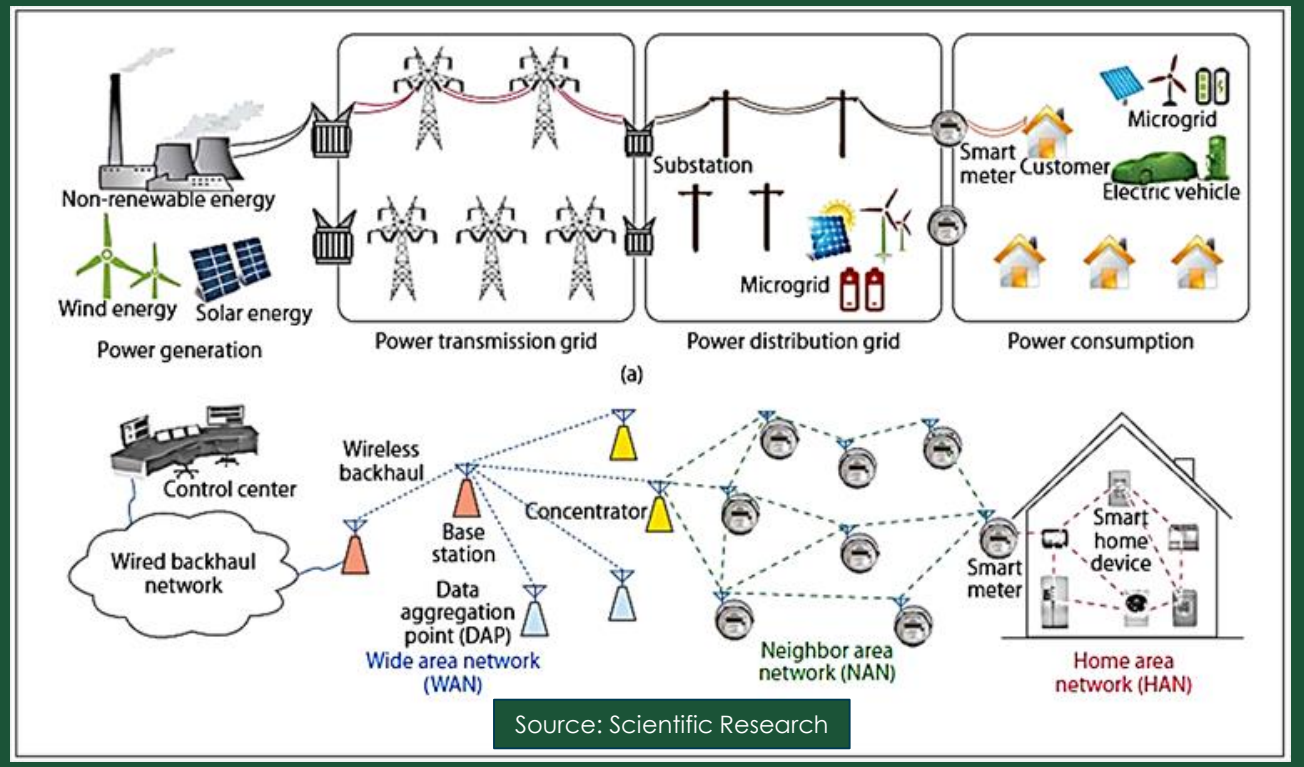
- Prevent unauthorized persons to access and control smart grid systems; build safeguards against Denial-of-service (DoS) attacks which can delay, deny or disrupt data flow and control operations.

SECURITY OF DATA AND NETWORK COMMUNICATIONS

Smart grids are characterized by bi-directional power flow, with increasing use of DERs, BESS and EVs/ V2G

To monitor bi-directional grid, sophisticated control strategies are used with multiple sensors and communication channels

Heavy data flow over heterogeneous communication networks increases the risks to cyber security of the smart grid



Source: Scientific Research

DER: Distributed Energy Resources
BESS: Battery Energy Storage System
EVs/ V2G: Electric Vehicles/ Vehicle to Grid

TYPES OF CYBER ATTACK VECTORS IN POWER SYSTEMS

False Command/ Data injection attack	•Manipulate power system state estimation
Denial of Service	•Data deluge, data disruption
Malware* attacks	•Stuxnet, Trojans
Data Manipulation	•Change control parameters, relay settings, encryption
Time synchronization/ Time delay attacks	•Generate GPS/ RTC error, trigger control delays
Man-in-the-Middle attacks	•Active/ Passive Eavesdropping, social engineering

*Malware includes viruses, ransomware, keyloggers, trojans, worms, spyware, malvertising, scareware and backdoors

EXAMPLES OF CYBER EXPLOITATION IN SMART GRID SYSTEMS

Solar Powered Microgrids

- If the inverter software that control power conversion and communication with the grid is not secure, an attacker can intercept its data and embed a malicious code or malware to destabilize the grid.

DER (Distribution Energy Resources) integration

- DER integration with electricity grids using modern control systems can be targeted by cyber attackers by injecting false information or manipulating data. Intrusion-detection software can alert grid operators to prevent such activities.

SCADA, DCS & PLC:

- SCADA, Distributed Control Systems and Programmable Logic Controllers in smart grid systems can be potential targets for cyber attacks, which can be countered using network segmentation, access control, patch management and AI/ ML techniques.

Smart Grid Communications:

- In modern smart grids, Industry 4.0, Industrial Internet of Things (IIoT) and Cloud services might also expose vulnerabilities to cyber attacks. Customized security strategies can help bridge the gaps in cyber security.

MEASURES TO PROTECT INDUSTRIAL NETWORKS AGAINST MALWARE ATTACKS

Network Segmentation	• Design the network in segments so that malware infects only a part of the network and not the whole system
Role-Based Access Control	• Provide access to authorized users based on specific roles, and granting access according to the responsibility assigned
Regular Updates & Vulnerability Management	• Regularly check the system for potential security gaps, and apply software patches/ updates to plug vulnerabilities
Antivirus and Anti-Malware	• Install strong antivirus and anti-malware programs to prevent and eliminate threats, both at servers and end points
Intrusion Detection/ Intrusion Prevention Systems	• Install IDS/ IPS to monitor network traffic and check for any malicious or suspicious activity
Virtual Private Networks	• Use VPN to achieve secure remote connection to industrial networks

MEASURES TO PREVENT CYBER ATTACKS IN SMART GRIDS-1

Cryptography:

- Encrypt with hash function to make smart grid data unrecognizable or hidden from cyber attackers.
- Hash function should be algorithmically strong and cannot be cracked easily.

Authentication and Key management:

- Use authentication (multi-factor) and role-based authorization to access smart grid data and applications.
- Use public key infrastructure (PKI) and key management for authorized users.

Code attestation and code analysis:

- Check integrity of the software with audit trails to detect suspicious activities.
- Check quality of codes, ensuring no security issues or vulnerabilities.

Device and software security:

- When new components are added to the application, perform penetration tests to eliminate vulnerabilities.

Encryption: Protects data in transit and at rest.

Authentication: Verifies the identity of devices and users.

Access control: Restricts access to sensitive data and systems.

MEASURES TO PREVENT CYBER ATTACKS IN SMART GRIDS-2

Firewalls, IDS, IPS:

- Use firewalls to control network traffic based on predefined security rules to allow authorized access.
- Use Intrusion detection and prevention systems to detect and block malicious activity.

Incident response plan:

- Plan for quick and effective response to cyber security incidents.

Security audits and assessments:

- Conduct regular security audits and assessments to help identify vulnerabilities in the smart grid infrastructure.

Security awareness training:

- Train employees on cyber security practices to reduce the risk of insider threats

Intrusion detection and prevention:
Detects and blocks malicious activity

Security audits and assessments:
Regularly identify vulnerabilities and weaknesses

Security awareness training:
Educates employees about security best practices.

CYBER SECURITY SOLUTIONS FOR SMART GRIDS

Malware Protection system	• Anti-malware system protect smart grids against malicious/ phishing software - Trojan horse, BlackEnergy, Stuxnet and Ransomware, by updating firewall configurations/ security patches.
Blockchain Based Cybersecurity	• Blockchain technology in smart grid systems is used to manage energy transactions/ power trading securely, prevent data tampering and check cyber frauds.
Artificial Intelligence/ Machine Learning Based Cybersecurity	• AI techniques are used to improve the reliability of smart grid systems, by developing intelligent models for identifying threats early and taking proactive counter measures against cyber attacks.

THANK YOU

JAYANT SINHA
Sr. Principal Consultant
(Energy Transition & Utilities)
jayant.sinha@entruistpower.com

EnTruist POWER

WHO WE ARE

EnTruist Power is a consortium of Energy and Utilities industry experts dedicated to providing Energy Transition, Environment Management and Digital Transformation solutions for a net-zero and sustainable future. We provide services to our industry partners/ clients in energy transition, smart grids, renewable energy, waste management, circular economy, utility automation, and compliance reporting (ESG, LCA) focusing on strategic business outcomes, environment leadership and sustainability.

OUR SERVICES

- **ADVISORY**: Clean and sustainable energy, risk management, KM and capacity building programs on Smart Grids, ADMS, DERMS, SCADA/ EMS, Green H2, Cyber Security, etc.
- **TECHNICAL**: Feasibility studies for energy system integration, asset/ performance management, energy efficiency, emission control and cost reduction.
- **MARKET ANALYSIS & RESEARCH**: Due diligence of latest trends, technologies, industry practices, competitor analysis, industry benchmarks and standards.
- **TRAINING & CAPACITY BUILDING**: Training and KM workshops, course planning, content development, classroom and remote online sessions for industry and utility clients.

Our core specializations

Our team of industry experts provide advisory, technical consultancy, market research and training services in the following specialized areas:

- Renewable Energy Management
- Smart Grids and Microgrids
- Distributed Energy Resources Management System
- Advanced Distribution Management System
- SCADA/ Energy Management System (EMS)
- Virtual Power Plants (VPP)
- Enterprise Risk Management (ERM)
- Regulatory, LCA & ESG reporting
- Sustainability Management, ESG & LCA reporting
- Waste Management & Circular Economy
- Electricity System Operations & Markets
- Blockchain and Cyber Security in EMS applications

CONTACT US

EnTruist POWER

Business Enquiries:
info@entruistpower.com
Technical & Training Enquiries:
technical@entruistpower.com
URL: https://entruistpower.com