Regional Training Program on Cybersecurity for Transmission Utilities and System Operators

Background

The increasing digitization and adoption of IT systems exposes utilities to cybersecurity risks. The last decade has seen growing incidents of cyberattacks on the power sector worldwide. One of the primary reasons is the change in the way utilities used to operate and perceive airgap between information and operational technologies (IT and OT). Traditionally, utilities have had IT and OT working in silos. Power utilities have used IT to automate business functions such as billing, customer service, and accounting, while OT has been focused to control power grid operations like electricity transmission and distribution, critical energy infrastructure and power systems operations managed through Supervisory Control and Data Acquisition (SCADA) systems. Such a separation used to provide air gap for securing critical assets. However, today the technologies such as Internet of Things (IoT) are bridging this gap. A smart meter is an apt example – the meter itself is OT but the communication function with which the meter data analytics can be carried out is an IT function. This interaction between IT and OT continues to increase, especially with proliferation of distributed energy resources (DERs), IoT-compliant SCADA systems, and decision support systems for grid operators. Digitization of grid is inevitable and irreversible due to its advantages like increased efficiency, reliability, robustness, and better situational awareness. But at the same time, one needs to have an eye on the vulnerabilities introduced in the system by such digitization efforts. If enough care is not taken while implementing such modernization projects it may pose a big threat to critical infrastructure like power grids, for example. Therefore, the ability of utilities to proactively address these threats needs to be improved.

Internationally, a lot of activities are being undertaken to create awareness about cyberattacks on the power sector and ways to secure critical energy infrastructure. For example, power is one of the top three sectors in the U.S. targeted for cyberattacks. The sector has also been a prime target in Europe and Japan and was identified as the sector with the highest number of cyberattacks in Australia[1]. Electric power companies have been reporting continuous attempted intrusions, and though most fail, activity is accelerating. Utilities in South Asia region are not untouched by such incidents with the latest one reported in the public domain in April 2022[2]. Cybersecurity in the power sector is key to protecting critical national infrastructure. Any lack of security planning in designing smart grids can make the whole country vulnerable to cyberattacks and related foul-play. For instance, in India, the Ministry of Power (MoP) has created a framework to address cybersecurity threats at the central level. Further, the power sector planning body of the country, Central Electricity Authority (CEA), has also laid down guidelines on cyber security in 2021. Clearly, it is an upcoming area of great importance and skill-building goes together with strengthening cybersecurity in the power sector.

[1] Deloitte Report – Managing Cyber Risk in the Electric Power Sector

[2] Hindustan Times, April 08, 2022 - Chinese hackers targeted 7 Indian power hubs, govt says ops failed

Day 1 - The Hilton at Mumbai International Airport

April 16, 2024	Session Title (Topics)
Registration (0930 – 1000 Hrs)	Welcome and Registrations
Inauguration Session (1000 – 1130 Hrs)	▪ Welcome Address by Ms. Monali Zeya Hazra, Regional Energy & Clean Energy Specialist and Mission Environment Officer, Indo Pacific Office USAID/India ▪ Special Address by Mr. Balaji, Head WRLDC ▪ Special Address by Mr. S K Soonee, Senior Advisor, SAREP and founding CEO, POSOCO ▪ SAREP Introduction and Background – Rakesh Sir (PPT)
Tea Break (1100 – 1130 Hrs)	
S1 (1130 – 1300 Hrs)	Security perspectives in the power sector (Dr. Faruk Kazi) ▪ Introduction ▪ Motivation ▪ Issues & challenges in securing utility infrastructure (IT/OT) ▪ Energy Management System (EMS)/ Distribution Management System (DMS) SCADA Security ▪ Impacts of cyber attacks
1300 – 1400 Hrs	Lunch
S2 (1400 – 1530 Hrs)	Technological landscape (Mr. Navin Mehra, Leader, Regional Sales, Cyber Security, CISCO) ▪ Defence in Depth approach ▪ IDS/IPS ▪ SOC/SIEM/SOA/UEBA ▪ Data diode ▪ OT Firewall System hardening and best practices.
Tea Break (1530 – 1545 Hrs)	
S3 (1545 – 1715 Hrs)	Smart metering infrastructure, HES, MDM, and cloud computing (Dr. Shailendra Fuloria, CISO at Nagarro) ▪ Advanced Metering Infrastructure (AMI) / Automated Meter Reading (AMR) ▪ Digital architecture for smart metering ▪ Communication protocols & standards ○ Device Language Message Specification (DLMS)/ Companion Specification for Energy Metering (COSEM) ○ IS 16444/IS 15959 ▪ Introduction to HES & MDM ▪ Securing gateways & networking infrastructure Third-party API integration issues

*- *to be confirmed*

Day 2 - The Hilton at Mumbai International Airport

April 17, 2024	Session Title (Topics)
S4 (1000 – 1130 Hrs)	Corporate Security Culture & Business Continuity Plan (Mr. Sanjay Damle, Ex CISO Tata Power) ▪ Culture of Security and its benefits ▪ Chief Security Officer (CSO) vs Chief Information Security Officer (CISO) ▪ Disaster recovery and business Continuity Plan
Tea Break (1130 – 1145 Hrs)	
S5 (1145 – 1315 Hrs)	Cyber Security Standards (Mr. Shiv Kataria, Siemens) ▪ ISO 27000, 27001& IEC 62443 ▪ Set of security standards for the secure development of Industrial Automation and Control Systems (IACS) for the power sector ▪ National Institute of Standards and Technology (NIST) guidelines
1315 – 1400 Hrs	Lunch
S6 (1400 – 1530)	Indian Regulations and Compliances (Mr. Anand Shankar Chief GM, Technology Development PGCIL) ▪ CEA (Cyber Security in Power Sector) Guidelines ▪ NCIIPC Guidelines and Controls ▪ Data privacy issue
Tea Break (1530 – 1545 Hrs)	
S7 (1545 – 1715 Hrs)	Demonstration of Tools- SAREP Cybersecurity Posture Assessment Tool (CPAT) (Dr. Faruk Kazi) ▪ Maturity model approach ▪ Overview of C2M2 ▪ Understanding the NIST Cyber Security Framework C2M2 architecture Demonstration of CPAT tool.

Day 3 - Center of Excellence (CoE) in Veermata Jijabai Technological Institute (VJTI), Matunga

April 18, 2024	Session Title (Topics)
Arrival (0830 – 1000 Hrs)	Arriving at the Veermata Jijabai Technological Institute (VJTI)
S8 (1000 – 1130 Hrs)	Cyber Kill Chain & MITRE framework (Dr. Faruk Kazi) ▪ Cyber Kill Chain ▪ Case study of Black Energy-3 MITRE ATT&CK framework, D3FEND framework
Tea Break (1130 -1200 Hrs)	
S9 (1200 – 1330 Hrs)	Practical demonstration with below modules, Lab visit to VJTI, Mumbai ▪ Threat Modeling and Demonstrations ▪ Generation ▪ Transmission ▪ Smart metering infrastructure
1330 – 1430 Hrs	Lunch
Closing (1430 – 1530 Hrs)	Assessment, valedictory, and feedback
Networking Tea (1530 -1600 Hrs) Return to Hotel (1600 – 1700 Hrs)	