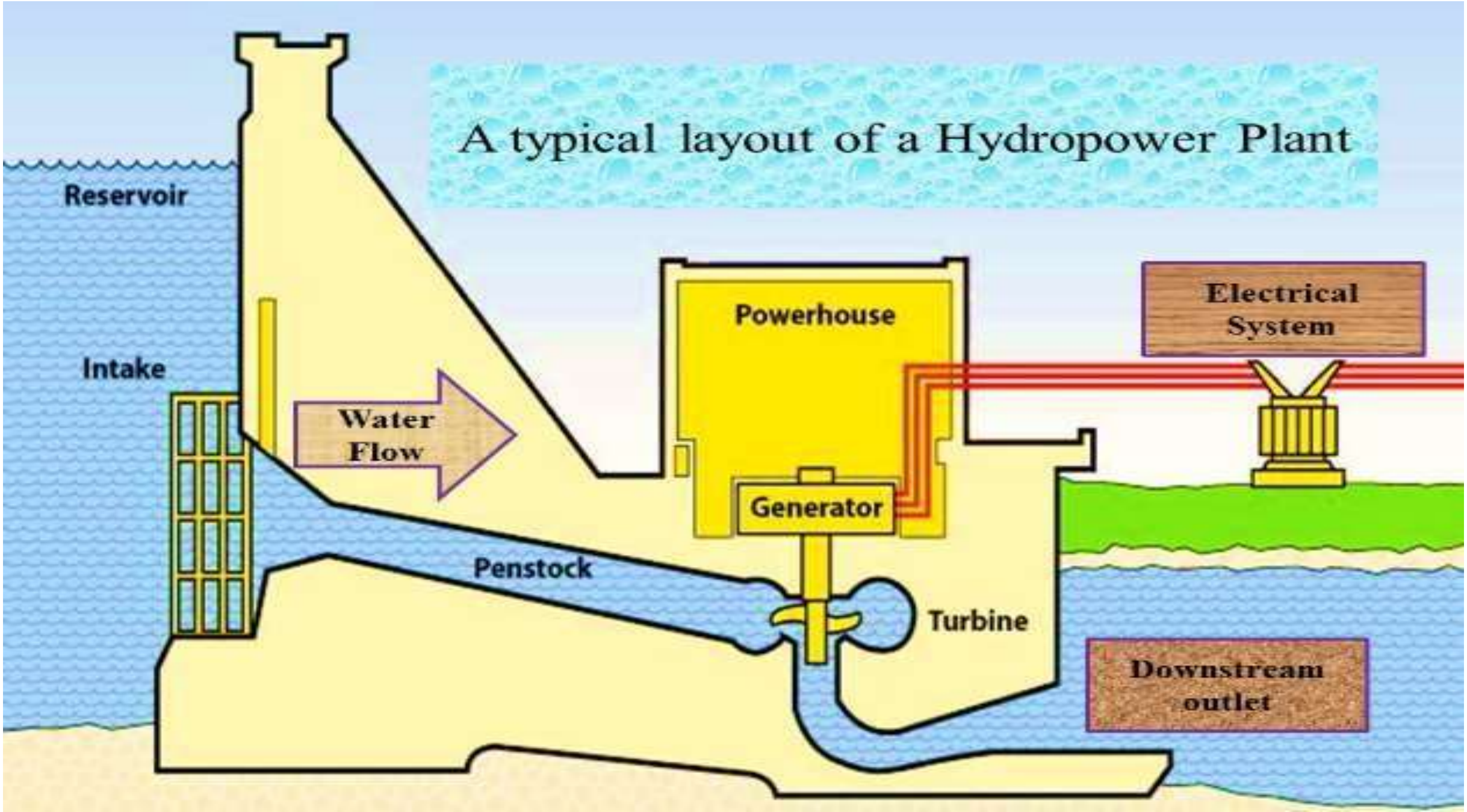
Enhancing Cybersecurity
in
Hydro Power Plants
Through
Artificial Intelligence(AI) Applications

By: L K S Rathore Director(Cyber Security), CEA

Hydro Power at a Glance

- One of the most important challenges we face as a in the power sector is the increased variability demand for energy.
- In response to this worldwide demand, hydropower is presented as a relatively clean, reliable, and renewable energy source and an interesting option to decarbonize our global economy by reducing greenhouse gas emissions.
- Flexible Energy Generation Assets that can supply both Base Load & Peaking Power efficiently and economically are the need of the future and necessary to address the dynamically evolving energy needs of the Country.
- Balancing of grid due Variable Renewable Energy Sources (VRE) can be maintained up-to certain extend by hydro electric energy.
- Hydro Installed Capacity in India is around 51897 MW(including Small Hydro - 4987 MW) as on 31st December 2023. where as Hydro total IC in Global level is around 1397 GW(Including 175 GW PSP)(Source –World Hydropower Outlook)
- Hydropower currently provides over 15% of the world's electricity.
- With an average growth of 4% per year, hydropower has become a key source for electricity generation – globally supplying 71% of all renewable electricity.


A typical layout of a Hydropower Plant
Reservoir
Intake
Water Flow
Powerhouse
Electrical System
Generator
Penstock
Turbine
Downstream outlet

The Growing Threat of Cyber Attacks on Critical Infrastructures

The growing threat of cyber attacks on critical infrastructure poses a significant and evolving challenge to societies worldwide. Several factors contribute to the increasing risk of cyber attacks on critical infrastructure-

- **Interconnected Systems**
- **Rapid Technological Advancements**
- **Sophisticated Threat Actors**
- **Lack of Cybersecurity Preparedness**
- **Supply Chain Vulnerabilities**
- **Geopolitical Tensions**

Understanding the Threat of Cyber Security

Cybersecurity Challenges in Hydro Power Plants

Cybersecurity Challenges in Hydro Power Plants

Hydropower plants faces various cybersecurity challenges that need to be addressed to ensure the reliable and secure operation of its facilities.

- **SCADA and Industrial Control Systems (ICS) Vulnerabilities**
- **Legacy Systems and Out-dated Technology**
- **Remote Access and Connectivity**
- **Insider Threats**
- **Supply Chain Security**
- **Cyber-Physical Threats**
- **Threats- Ransomware, data breaches, and system vulnerabilities.**

Cyber Security Measures in Hydropower Plants

Cyber Security Measures in Hydropower Plants

- **Risk Assessment**: Conduct a comprehensive risk assessment to identify potential vulnerabilities and threats to the hydropower system. This assessment should include both internal and external factors that could impact the cybersecurity of the facility.
- **Network Segmentation**: Implement network segmentation to separate critical operational systems from non-critical systems and administrative networks. This helps contain potential cyber attacks and prevents them from spreading to vital elements of the hydropower system.
- **Access Control**: Implement strict access control measures to limit access to critical systems and data only to authorized personnel. This includes strong authentication mechanisms such as multi-factor authentication and role-based access control.
- **Encryption**: Encrypt sensitive data both in transit and at rest to prevent unauthorized access or tampering. This includes encrypting communication channels and storage systems used in the hydropower facility.

Cyber Security Measures in Hydropower Plants

- **Patch Management:** Establish a robust patch management process to regularly update and patch software and firmware vulnerabilities in control systems and other critical components of the hydropower infrastructure.
- **Security Monitoring:** Implement continuous security monitoring solutions such as intrusion detection systems (IDS) and security information and event management (SIEM) systems to detect and respond to cyber threats in real-time.
- **Capacity Building/Employee Training:** Provide regular cybersecurity awareness training to all personnel involved in operating and maintaining the hydropower facility. This training should cover best practices for identifying and mitigating cyber threats, as well as procedures for reporting security incidents.
- **Incident Response Plan:** Develop and regularly update an incident response plan that outlines procedures for responding to cybersecurity incidents, including containment, eradication, and recovery steps.

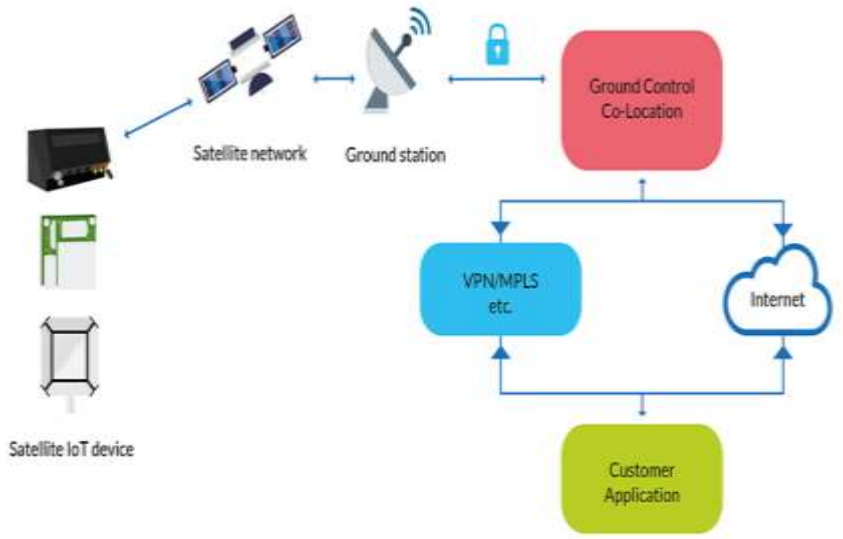
Cyber Security Measures in Hydropower Plants

- **Vendor Risk Management**: Ensure that third-party vendors and suppliers adhere to strict cybersecurity standards and protocols to prevent supply chain attacks that could compromise the hydropower system.
- **Regulatory Compliance**: Stay updated with relevant cybersecurity regulations and standards applicable to the hydropower industry and ensure compliance with them to mitigate legal and regulatory risks associated with cybersecurity breaches.
- **Physical Security**: Implement physical security measures to protect critical infrastructure components from unauthorized access or tampering, including access controls, surveillance systems, and perimeter security.
- **Cybersecurity Culture**: Foster a culture of cybersecurity awareness and accountability throughout the organization, emphasizing the importance of cybersecurity in protecting the integrity and reliability of hydropower operations.

Cyber Security Measures in Hydropower Plants

Protect Data Integrity

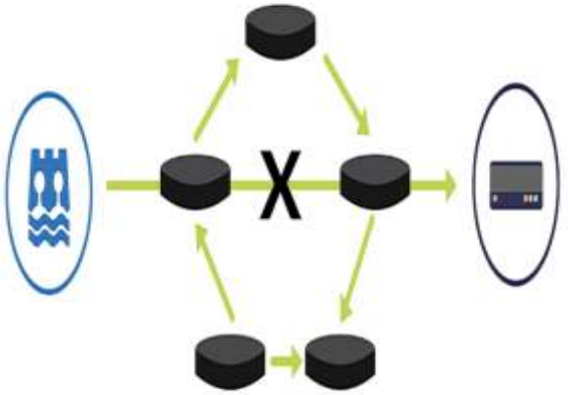
- An integral aspect of security involves safeguarding data through encryption, authentication protocols, and stringent control over physical facility access.
- Utilizing firewalls and VPNs can be effective in securing data during transmission over public internet infrastructure.



Enhance Physical Security

- Robust physical security measures not only act as a deterrent to potential threats but also represent the initial defense against cyber attacks.
- Stringently controlling and monitoring physical access to facilities substantially minimizes the risk of malicious actors gaining direct entry to sensitive systems and data.

Cyber Security Measures in Hydropower Plants



Ensure Resilience through Redundancy and Backup

- Redundancy and backup systems play a critical role in fortifying network infrastructure against unexpected vulnerabilities and disruptions.
- Using duplicate or alternative pathways for data transmission and network operations, redundancy measures guarantee an immediate and smooth transition to a secondary, secure option should the primary system or connection fail.
- This approach not only reduces the risk of single points of failure but also amplifies the overall system reliability.

By implementing these measures and continuously monitoring and adapting to emerging cyber threats, hydropower facilities can enhance their resilience against cyber attacks and safeguard vital elements of their infrastructure.

Cyber Security Measures in Hydropower Plants

Managed Detection and Response (MDR)

- MDR is a 24-hour cyber security service that combines modern security technology with human analysis, artificial intelligence and automation to rapidly detect, analyse, investigate and actively respond to threats, rather than simply generating alerts.
- MDR solution also allows businesses to develop a reference security architecture that facilitates the safeguarding of on-premise and legacy systems, SaaS solutions and cloud-based infrastructure applications. It also helps security teams to protect against and respond effectively to emerging security and user identity threats while reducing the dwell time of any breaches.
- For hydropower operators, MDR provides correlated visibility across OT and IT networks, effectively joining the dots and enabling security teams to focus on strategic priorities rather than chasing down the latest security vulnerabilities.

Application of AI in Cybersecurity of Hydropower Plant

Application of AI in Cybersecurity of Hydropower Plant

Artificial Intelligence (AI) plays a crucial role in enhancing cybersecurity efforts, offering advanced capabilities to detect, prevent, and respond to cyber threats:

- **Network Anomaly Detection:**
  - An AI system is employed to continuously monitor network traffic within a hydro power plant's control systems.
  - The AI detects unusual patterns or anomalies that could indicate a cyber attack or unauthorized access. The system triggers alerts or automatically takes preventive measures to mitigate the threat, preventing potential damage or disruption.

AI Revolution: Artificial Intelligence in Energy

Application of AI in Cybersecurity of Hydropower Plant

- **Predictive Maintenance and Security Patching:**
  - AI algorithms analyze historical data and system vulnerabilities to predict potential weak points in the hydro power plant's control systems.
  - The AI system recommends proactive security measures, such as applying patches to vulnerable software or upgrading certain components, reducing the risk of exploitation by cyber threats.
- **Behavioral Analytics for Users Access:**
  - AI driven behavioral analytics are employed to monitor user activities and access patterns within the Hydropower Plant’s IT infrastructure.
  - The AI system identifies deviations from normal user behavior, helping to detect insider threats or unauthorized access.
  - Timely interventions prevents potential breaches and sabotages

AI Revolution: Artificial Intelligence in Energy

Application of AI in Cybersecurity of Hydropower Plant

- **Threat Intelligence Integration:**
  - Hydro power plants integrate AI systems with threat intelligence feeds to stay updated on the latest cybersecurity threats.
  - The AI continuously evaluates incoming threat intelligence data and adapts the plant's cybersecurity measures accordingly.
  - This proactive approach helps in preventing attacks that leverage newly identified vulnerabilities.
- **Incident Response Automation:**
  - AI is utilized to automate incident response procedures in case of a cybersecurity incident.
  - The AI system identifies and contains the impact of a cyber attack in real-time, minimizing downtime and potential damages.
  - The automated incident response helps in swiftly isolating affected systems and initiating recovery procedures.

Challenges

in implementing

AI for cybersecurity in hydro power plants

Challenges in implementing AI for cybersecurity in hydro power plants

Implementing AI for cybersecurity in hydro power plants comes with its own set of challenges, considering the critical nature of these facilities and the potential consequences of cyber threats.

Complexity of Industrial Control Systems (ICS):

- Hydro power plants typically rely on complex Industrial Control Systems (ICS) to manage and control various processes. Integrating AI into these systems without disrupting their functionality can be challenging.

Legacy Systems and Equipment:

- Many hydro power plants may still use legacy systems and equipment that were not designed with cybersecurity in mind. Retrofitting these systems to incorporate AI-based security measures can be difficult and may require significant investment.

Challenges in implementing AI for cybersecurity in hydro power plants

Interconnected and Interoperability:

- Hydro power plants are often part of a larger energy grid and are interconnected with other systems. Ensuring interoperability between different components and systems while implementing AI for cybersecurity is crucial to prevent vulnerabilities.

Resource Constraints:

- Hydro power plants, especially those in remote locations, may have limited resources in terms of both budget and skilled personnel. Implementing and maintaining AI solutions require significant resources, and resource constraints may hinder effective cybersecurity measures.

False Positives and Negatives:

AI systems may generate false positives (incorrectly identifying a normal activity as a threat) or false negatives (failing to detect an actual threat).

The consequences of either type of error can be severe, and achieving a high level of accuracy is essential.

Challenges in implementing AI for cybersecurity in hydro power plants

Adaptability to Evolving Threats:

- Cyber threats are constantly evolving, and attackers may employ sophisticated techniques.
- Ensuring that AI systems can adapt to new and emerging threats is crucial for maintaining effective cybersecurity.

Regulatory Compliance:

- Hydro power plants are subject to various regulations and standards related to cybersecurity.
- Ensuring that AI solutions meet these compliance requirements can be challenging and may involve navigating complex regulatory landscapes.

Challenges in implementing AI for cybersecurity in hydro power plants

Human Factor:

- Employees within hydro power plants may not be adequately trained to understand and manage AI-based cybersecurity systems.
- Providing the necessary training and creating a cybersecurity-aware culture is essential to mitigate the human factor in cybersecurity.

Supply Chain Risks:

- The supply chain for equipment and software used in hydro power plants may introduce vulnerabilities.
- Ensuring the security of the entire supply chain, including third-party vendors, is crucial to prevent potential exploits.

Privacy Concerns:

- Hydro power plants may collect and process sensitive data.
- Ensuring the privacy of this data while implementing AI solutions is essential, especially considering the increasing focus on data protection regulations.

Best Practices

Best Practices…

Implement AI-Based Intrusion Detection Systems (IDS):

- Deploy AI-powered intrusion detection systems to monitor network traffic and detect anomalies or suspicious activities.
- Utilize machine learning algorithms to continuously analyze patterns and behaviours, enabling early detection of potential cyber threats.

Utilize AI for Threat Intelligence:

- Leverage AI to gather, analyse, and interpret threat intelligence data from various sources.
- Implement machine learning models that can predict emerging cyber threats and vulnerabilities, allowing for proactive defence measures.

Behavioral Analytics:

- Employ AI-driven behavioral analytics to establish a baseline of normal activities within the hydro power plant's network.
- Identify deviations from the baseline that may indicate potential security incidents or unauthorized access.

Best Practices…

Secure Communication Channels:

- Implement AI algorithms to monitor and secure communication channels within the power plant's control systems.
- Utilize encryption and AI-driven anomaly detection to protect against eavesdropping and man-in-the-middle attacks.

Asset and Vulnerability Management:

- Use AI to automate the identification and tracking of assets within the power plant's infrastructure.
- Implement vulnerability assessment tools with AI capabilities to identify and prioritize potential weaknesses in the system.

Continuous Monitoring and Response:

- Implement AI-driven continuous monitoring solutions to ensure real-time visibility into the hydro power plant's cybersecurity posture.
- Develop automated response mechanisms to address identified threats promptly.

Employee Training and Awareness:

- Train employees on cybersecurity best practices and the potential risks associated with cyber threats.
- Utilize AI-based training modules to simulate phishing attacks and other common threats, helping employees recognize and respond appropriately.

Incident Response Planning with AI:

- Develop and regularly update an incident response plan that incorporates AI-based tools for rapid threat detection and containment.
- Conduct regular drills to ensure a coordinated and effective response to cybersecurity incidents.

Secure Supply Chain:

- Implement AI-driven supply chain security measures to assess and monitor the cybersecurity posture of third-party vendors and partners.
- Verify the security practices of suppliers to prevent potential vulnerabilities in the supply chain.

- **Regulatory Compliance:**
  - Stay informed about relevant cybersecurity regulations and standards as applicable to the energy sector.
  - Use AI tools to automate compliance monitoring and reporting to ensure adherence to cybersecurity requirements.

Conclusion

Conclusion

- ✓The integration of artificial intelligence (AI) applications in hydro power plants marks a significant stride towards enhancing cybersecurity in critical infrastructure.
- ✓Shifting from reactive to proactive
- ✓The vulnerabilities associated with the increasing digitization and interconnectedness of these facilities demand innovative solutions, and AI emerges as a powerful ally in fortifying defences against cyber threats.
- ✓Machine Learning, Anomaly detection, predictive analytics contribute to a proactive approach, allowing for the identification of unusual patterns and potential breaches before they can compromise the integrity and functionality of the plant.
- ✓AI applications offer the advantage of continuous learning and adaptation, staying ahead of the ever-evolving nature of cyber threats.
- ✓The predictive capabilities of AI empower hydro power plant operators to anticipate potential vulnerabilities and take preemptive actions to safeguard critical infrastructures.
- ✓Collaborative efforts between industry stakeholders, cybersecurity experts, and AI developers are essential to fostering a robust cybersecurity ecosystem for hydro power plants.

Solution agencies -AI for Cybersecurity

- **Siemens Cybersecurity Solutions:** Siemens, a global technology company, provides industrial cybersecurity solutions that leverage AI and machine learning to hydro power plants.
- **ABB Ability™ Cyber Security for Power Plants:** ABB is another major player in the energy sector that offers cybersecurity solutions for Power Plants incorporates AI and machine learning to detect abnormal patterns in network behavior and identify potential cyber threats.
- **Darktrace in Energy Sector:** Darktrace is a cybersecurity company that uses AI to detect and respond to cyber threats in real-time to energy sectors including hydro power plants
- **Fortinet's Security Fabric for Energy and Utilities:** Fortinet provides a Security Fabric that integrates AI and machine learning to protect critical infrastructure, including energy and utilities.
- **GE Developing AI to Safe Operation of Critical Energy Infrastructure**- GE represents a new paradigm in protecting industrial assets and systems from malicious cyber-attacks with an additional layer of protection beyond the traditional IT/OT firewalls by combining AI and machine learning technologies with sensing and controls to rapidly detect, locate and neutralize cyber-attacks.

Artificial Intelligence in Energy

Case Study

Cyber Security Compliance for Dam Gate Automation

at

Tidong-I HEP Project, Kinnaur, Himachal Pradesh

Reference

Tidong Power Generation Private Limited (here after referred as TPGPL) PO No TPGPL/21-22 dt 12th Nov 2021 awarded to M2MLogger, for

“Design, Engineering, Material supply, installation, testing and commissioning work of electrical, instrumentation, real time measurement and acquisition of data for ecological discharge, water level, temperature, water flow, gate positions etc and remote supervision and control of Hydro Mechanical Gates from local and Barrage control rooms”.

Scope of Work

The contractor’s scope of work shall include the design manufacture, shop assembly, shop testing, delivery to project site, unloading and storage at site, site transportation, complete erection, installation, testing, commissioning and provide all necessary assistance with all required inputs for exchange of signals about information and control of HM (Hydro Mechanical) Gates, Sacrificial/ecological discharge, Silt level, water flow, water level and temperature etc.

Problem Statement

- The contract including all its Annexures requires M2MLoger to supply, test, install and commission System for control Dam Gates with detailed signal exchange list.
- The TPGPL SCADA installed at control room will use the signal list to carry out operations.
- The contract, as per Quotation QU2200023A dated 16 Sep 2021, Special Point of Note #6, clearly mentions that “All signals are being collected at each PDB and then transmitted via RS485 MODBUS RTU protocol to main control room for display and further transmission”.
- The contract does not mention any Cyber Security compliance requirement for the system to be supplied.
- The detailed drawings were approved by TPGPL appointed consultant “Indo Canadian Consultancy Services. Ltd., Noida” as per the below schedule:

Problem Statement (contd…)

- The detailed drawings were approved by TPGPL appointed consultant “Indo Canadian Consultancy Services. Ltd., Noida” as per the below schedule:

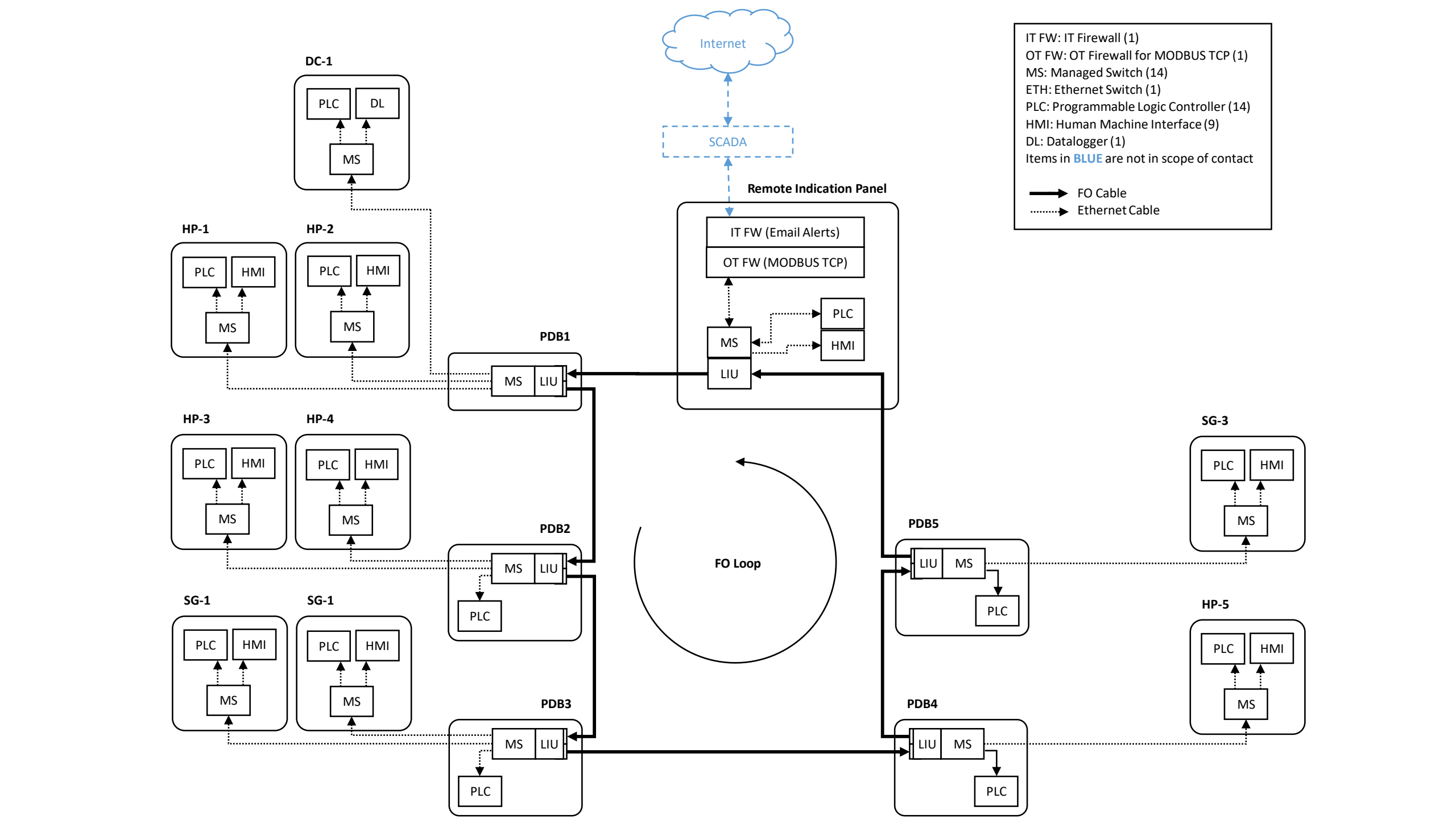
#	Drawing No.	Doc. Name	Revision	Cat. of Approval	TPGPL Letter Ref.	TPGPL Letter Date
1	CD-01	Communication Diagram	7	Cat-I	LE-TPGPL-M2M-0022	28-Mar-23
2	BL-01	Architecture Diagram	4	Cat-I	LE-TPGPL-M2M-0012	21-Jul-22
3	SL-01	Single Line Diagram	2	Cat-I	LE-TPGPL-M2M-0007	27-Apr-22
4	Main PDB	Main Power Panel (Main PDB)	1	Cat-I	LE-TPGPL-M2M-0018	20-Dec-22
5	RIP	Remote Indication / Control Panel (RIP)	2	Cat-I	LE-TPGPL-M2M-0022	28-Mar-23
6	HP-1 to HP-5	Rope Drum Hoist Panel (HP-1 to HP-5)	3	Cat-I	LE-TPGPL-M2M-0021	18-Mar-23
7	SG-1 to SG-3	Screw Hoist Panel (SG-1 to SG-3)	1	Cat-I	LE-TPGPL-M2M-0018	20-Dec-22
8	PDB-1	Local Power Distribution Cum Control Panel (PDB-1)	1	Cat-I	LE-TPGPL-M2M-0018	20-Dec-22
9	PDB-2	Local Power Distribution Cum Control Panel (PDB-2)	2	Cat-I	LE-TPGPL-M2M-0021	18-Mar-23
10	PDB-3	Local Power Distribution Cum Control Panel (PDB-3)	2	Cat-I	LE-TPGPL-M2M-0022	28-Mar-23
11	PDB-4	Local Power Distribution Cum Control Panel (PDB-4)	2	Cat-I	LE-TPGPL-M2M-0022	28-Mar-23
12	PDB-5	Local Power Distribution Cum Control Panel (PDB-5)	2	Cat-I	LE-TPGPL-M2M-0022	28-Mar-23

Problem Statement (contd…)

- On 10 Aug 2023, M2MLogger receives email intimation from TPGPL regarding Malicious code certificate requirement in view of guideline NH/IT&C/2021/1156 dated 27th Dec 2021 titled “Testing of power system equipment for use in the Supply System and Network in the country for Cyber Security”.
- On consultation with Schneider India Pvt. Ltd., the OEM for PLC, M2MLogger did not receive any Cyber Security Compliance Certificate of PLCs.
- M2MLogger reached out to CPRI on 6th Sep 2023, which is the designated laboratory under Ministry of Power Order No 12/34/2020-T&R dated 8th June 2021 for Cyber Security conformance testing of PLCs.
- The CPRI reaffirmed via email dated 8th Sep 2023 that CPRI is authorized to conduct conformance testing for RTU/PLC which uses communication protocols namely IEC 60870-5-101 & IEC 60870-5-104 and IEDs for protocol IEC 61850.

Problem Statement (contd…)

- M2MLogger reached out NHPC CISO and thereafter to CEA CISO for a reasonable resolution to matter that will enable us to supply and commission the system.
- On subsequent meetings with CEA CISO and team, M2MLogger carried out modification to scheme so that system is resilient to Cyber Security threats.
- The TPGPL has repeatedly requested either compliance or exemption certificate from concerned authorities for the execution of contract.
- The TPGPL has denied issuing any Variation Order for the escalation in cost due additional Cyber Security Compliance (which was not in scope of work), citing this is not a requirement from TPGPL but a requirement under Indian Law.


Internet
SCADA
DC-1
PLC
DL
MS
Remote Indication Panel
IT FW (Email Alerts)
OT FW (MODBUS TCP)
PLC
HMI
MS
LIU
HP-1
HP-2
HP-3
HP-4
PDB1
PDB2
PDB3
PDB4
PDB5
FO Loop
SG-1
SG-3
HP-5
IT FW: IT Firewall (1)
OT FW: OT Firewall for MODBUS TCP (1)
MS: Managed Switch (14)
ETH: Ethernet Switch (1)
PLC: Programmable Logic Controller (14)
HMI: Human Machine Interface (9)
DL: Datalogger (1)
Items in BLUE are not in scope of contact
FO Cable
Ethernet Cable

Proposed steps for Cyber-resilience in consultation with CEA

- **Firewall**:
  - IT Firewall between SCADA and OT Firewall, with 6 months storage and email alerts provision.
  - OT firewall between IT Firewall and Remote Indication Panel, with 6 months storage and MODBUS TCP rules.
- **Firewall Rules** (Between SCADA and Remote Indication Panel):
  - ACL and MAC rules to limit source and destination IP Address and/or MAC ID and port.
- **Defence-in-Depth**:
  - Network Segmentation from SCADA to Remote Indication Panel.
  - VLAN segmentation from Remote Indication Panel to all field Managed Switches.
  - ACL and MAC based rules between Remote Indication Panel and Field Managed Switches to limit source and destination IP Address and/or MAC ID and port.
  - Use of non-standard and possibly different TCP port number for each connection. Standard port for MODBUS TCP is 502.

Proposed steps for Cyber-resilience in consultation with CEA (contd…)

- **Physical Security:**
  - Disable all unused ports on Managed Switches and Firewall.
  - HMI to be configured in read-only mode.
  - Critical Dam gates to be identified and configured to operate in Offline mode only by default.
  - To operate Critical Dam gates in Online mode there must be Two level approval for SCADA users.
- **Operational Policies (for TPGPL)**
  - Two Level approval system to operate Critical gates.
  - Password Rotation Policy (every 30/90 days) for:
    - Firewall
    - Managed Switches
    - PLC
  - User Authentication Policy for SCADA users.
  - User Authorization Policy for SCADA user’s read and write privileges.
  - Regular Audit and Monitoring of firewall log and Email alerts.
  - Regular VA & PT for entire network.

Proposed steps for Cyber-resilience in consultation with CEA (contd…)

- Firewall Logs
  - Inbuilt storage
  - Daily logs email.
  - Email based alert.
- VA & PT of network once commissioned.

Cyber Secured India