CYBER SECURITY FOR POWER SECTOR

Shiva Suman, CPES,
Director, CEA
shivvasuman@nic.in

Thought of the day

We are to

‘Love the People and Use the Things’

But not to

‘Love the Things and Use the People’

Generation

Conventional: Thermal, Nuclear, Large Hydro etc..,

Non Conventional : Wind, Solar, Small Hydro, Bio-Power, U & I Waste, Geothermal, Tidal etc..,

Location specific

Transmission

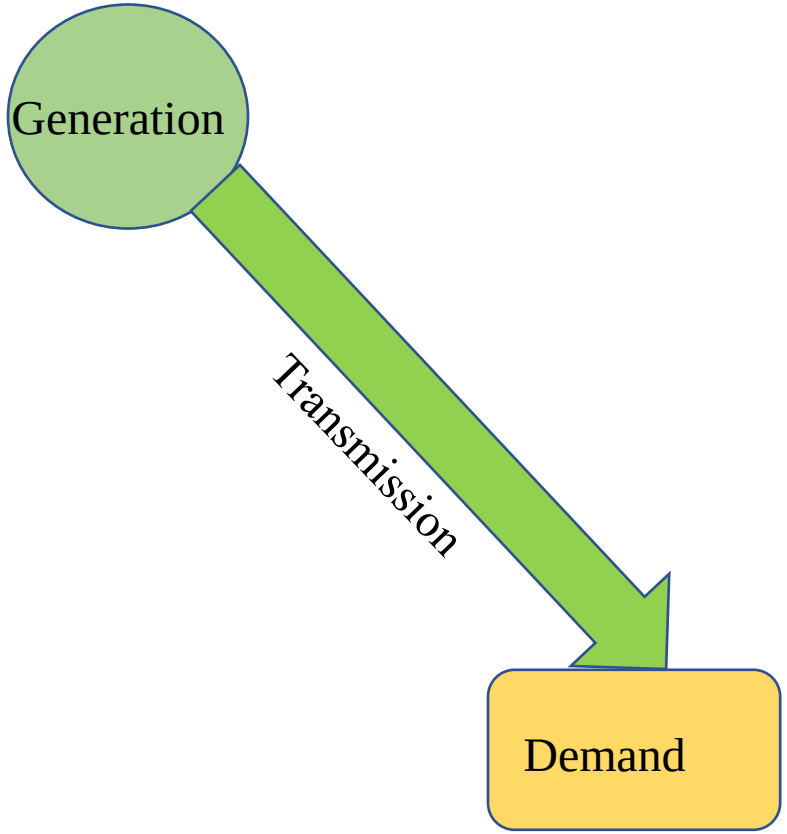
Inter connecting generation and distribution

as high V as possible

Distribution

Demand of consumers

Location specific



Generation = Consumption (at each instance)

Consumption is not flat – peak and off peak

Power Sector

Combination of multiple electrical elements

Reliable, Efficient and Safe operation

Cost Effective and Quality power supply

Planning; Operation & Maintenance

Realtime load generation balance

Schedule and dispatch of power

Communication exchange among entities

Exchange of data from IT to OT and vice versa

Passive components

Active devices – data collection, process, generate signal, control devices

Operation Technology - programmable hardware

direct monitoring or control of physical devices

detects changes

causes changes

OT impacts physical devices

Relay, RTU, PLC, IED, Smart Meter, BCU, Gateway, Smart Inverter

ICS – SCADA (Remote monitoring of dispersed assets),

DCS (control within a facility)

Water Tank Analogy

Manual

Mechanical

Motorized

Automatic – Monitor

Control – wired – Copper

Control – wired – over TCP

Control – wireless – over TCP / cellular

Basics of cyber security

Security - Ability to avoid being harmed by any risk, danger or threat.

Cyber Security

Event – Alert – Incident – Sabotage – Crisis

Confidentiality – Integrity – Availability

Threat – ability to exploit the vulnerability

Attackers – Motivation – Financial; Non financial – practice, revenge, nation

Attackers ahead of Defenders – Legal frameworks, Ethics, Limited resources

Types of Attacks

- Phishing – impersonate communication
- Unauthorized scan
- Vulnerability – weakness or gap of system - open to attack
- Malicious code
- Website defacement - an attack resulting in visual change
- Website intrusion
- DoS – choking the bandwidth – no response to legitimate requests
- DDoS – DoS by multiple computers of a botnet
- Ransomware
- Data breach
- Advance Persistent Threat (APT) - a group having the capability and the intent to persistently and effectively target a specific entity
- Insider attacks

Different phases of attack – Cyber kill chain

- Reconnaissance – scan
- Weaponization - develop malware
- Delivery - inject the payload
- Installation - install and execute the payload
- Exploitation - exploit vulnerabilities for persistence
- Lateral Movement - enhance the reach
- Command & Control - establish outbound connection
- Exfiltration - collect the data and transfer
- Impact - ransomware, sabotage, DDoS

Detecting attacks earlier in the kill chain minimizes damage

Dwell time = Time gap between compromise to detection

Contain time = Time gap between detection to containment

Recovery time = Time gap between containment to recovery

Unauthorized access time to asset = Dwell time + Contain time

Three (3) Pillars of Cyber Security

- People – often weakest – strongest with training and awareness
- Process – procedures and policies guide people to interact with technology
- Technology – tools and systems necessary to defend cyber threats

Countermeasures

Layer	Measures
Policies, Procedures & Awareness	User Education
Physical Security	Guards, locks, tracking devices
Perimeter	Firewalls, VPN, IDS/IPS, NIDS
Internal Network	Network segments
Host	OS hardening, authentication, patch management, HIDS, HIPS
Application	Application hardening, antivirus
Data	Access Control, Encryption

International Standards

NIST CSF – Guidelines by National Institute of Science & Technology, USA's Cyber Security Framework to mitigate and mange cyber risks – 3 components

Profile - Gather information, create a profile, analyse gaps, prepare action plan, implement action plan

Core - Identify – People, Assets, Capabilities

Protect – safeguard the critical assets

Detect – timely discovering the incident

Respond – action against detected incident & contain the impact

Govern – policy formulation, roles & responsibilities

Tiers - Tier 1 (Partial), Tier 2 (Risk Assessment), Tier 3 (Repeatable) and Tier 4 (Adoptive)

ISO 27000 standards

- ISO 27001 - Information Security Management System Certification
- ISO 27002 - Guidelines to select, implement and manage controls
- ISO 27019 – Information security controls for energy sector

ISO / IEC 15408 - Common Criteria - IT products meet set of standards – certificate

NERC CIP (North America Electric Reliability Corp - Critical Infrastructure Protection)

- Cyber security and physical security standards for large scale electrical systems

EU NIS – Legal framework to protect critical sectors from cyber security

IEC 62443 - Guidelines for securing industrial automation and control systems (IACS) throughout lifecycle

Global level

Cyber attacks – 800000+

Ransomware – 68 %
Network breach - 18 %
Data exfiltration - 4 %

Continent wise

Africa - 28 %; Latin America – 25 %; APAC – 24 %
EU - 13 %; North America - 11 %

Industry Wise

Manufacturing – 29 %; Healthcare – 11 %; Finance – 7 %; Energy 1 %

Segments of Power Sector

Thermal

Hydro

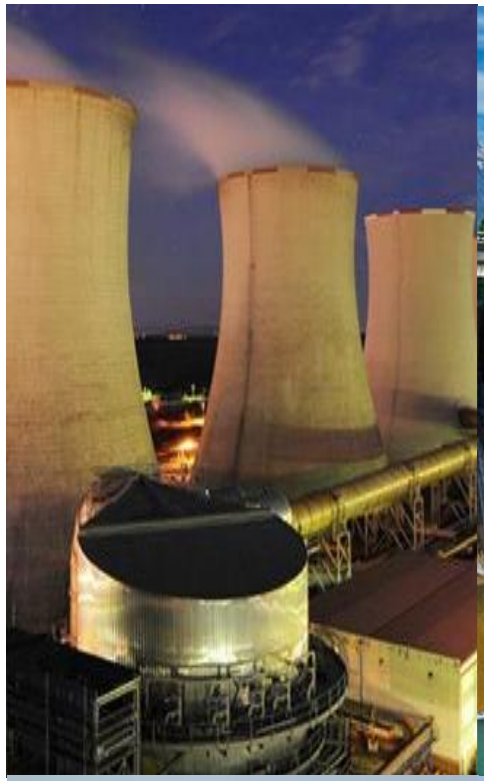
Renewables

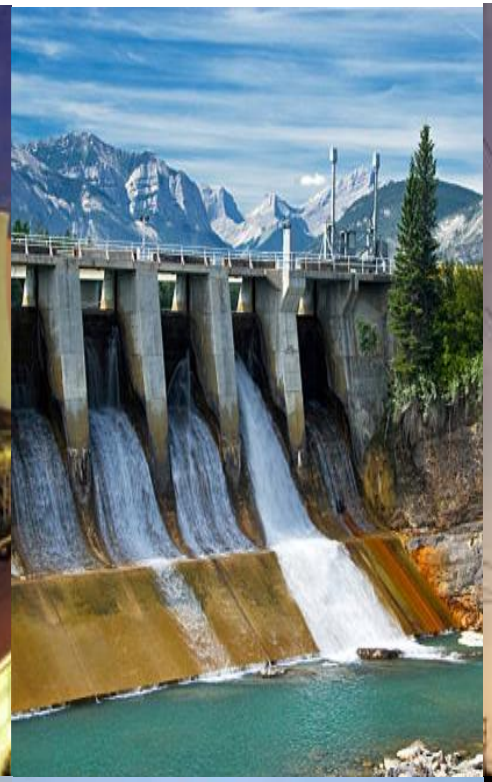
Transmission

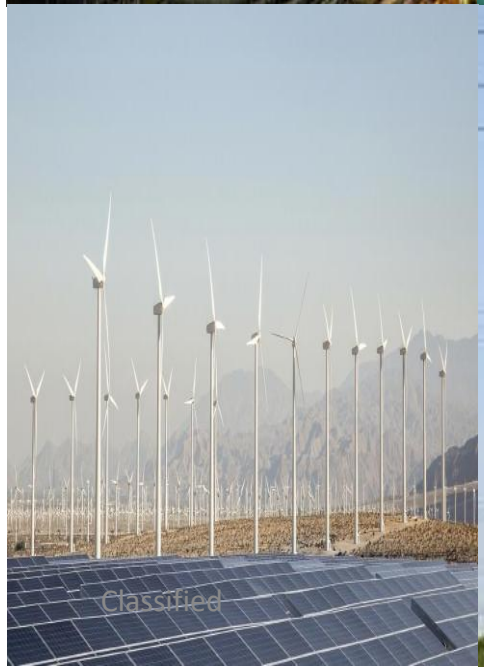
Distribution

Load Dispatch

Sub Sector	Utilities
Grid Operation	35
Distribution	81
Thermal	47
Hydro	35
Trans	56
RE	34
Total	288







Institutions

CERT – In : Indian Computer Emergency Response Team (CERT-In) - Section 70B of IT Act, 2000

National agency for responding to cyber security incidents

Cyber Swachhta Kendra (CSK)

citizen-centric service

detect malicious programs

free tools to remove

National Cyber Coordination Centre (NCCC)

the control room to scan / examine the cyberspace

detect cyber security threats.

shares the metadata with concerned entities

CERT – In empaneled 237 organization for Cyber Security Audit

(2023 – 9772; 2024 – 12176; and 2025 – 18667)

NCIIPC - National Critical Information Infrastructure Protection Centre

Section 70A of IT Act, 2000

Protection of critical information infrastructure

Indian Cybercrime Coordination Centre (I4C), MHA

Cybercrimes

National Cyber Security Coordinator (NCSC) under NSCS

Coordination amongst different cyber security agencies

Critical Sectors

Vital for National Security, Economy and Public Health

BFSI – Banking, Financial Services and Insurance
Power & Energy
Health
Telecommunication
Defence
Transportation
Government

National Cyber Security Policy, 2013

create mechanisms for Security threat early warning, vulnerability management and response - State and Sectoral CERTs

West Bengal – 08.07.2019

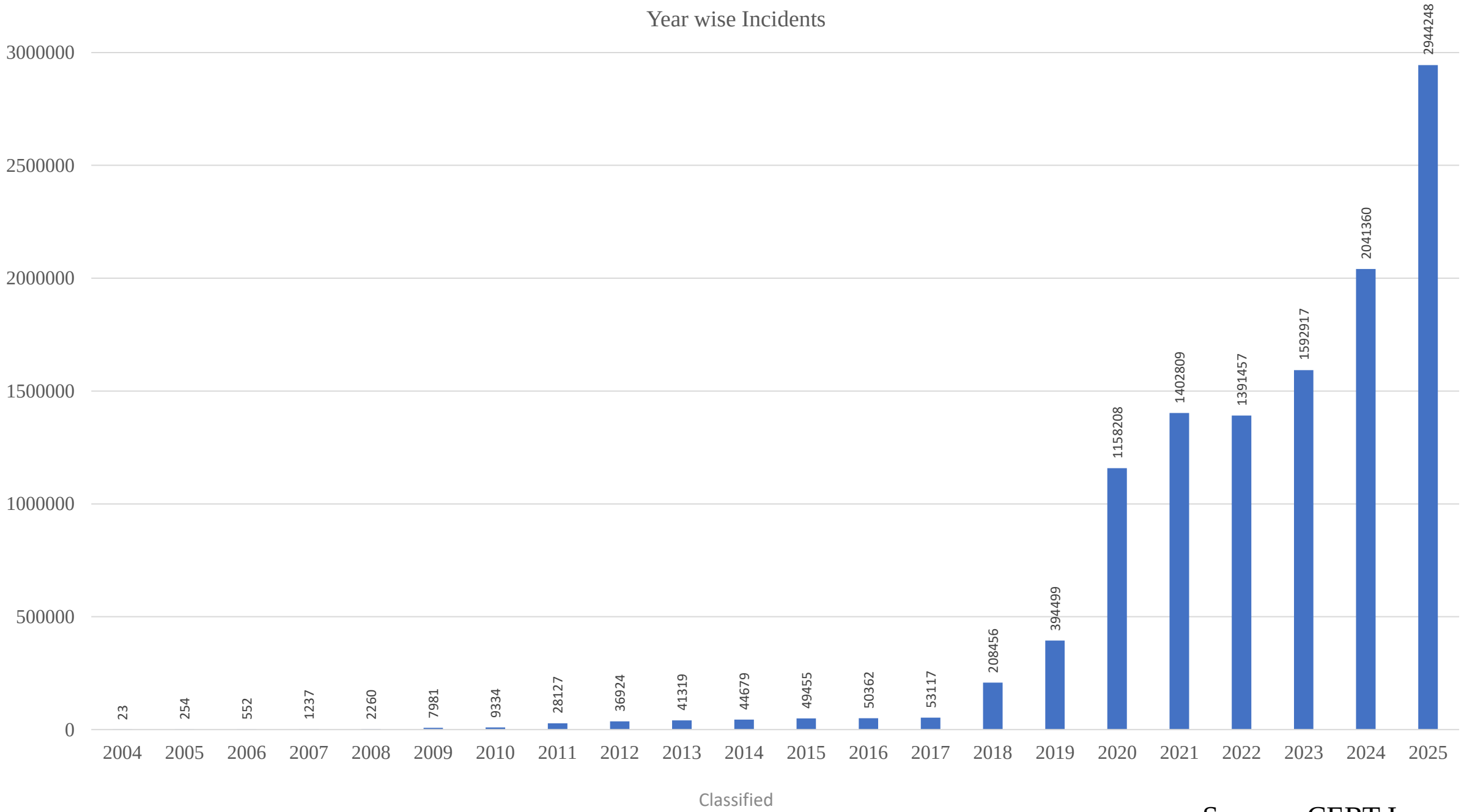
CERT – Fin – 15.05.2020

CSIRT – Power – 05.04.2023

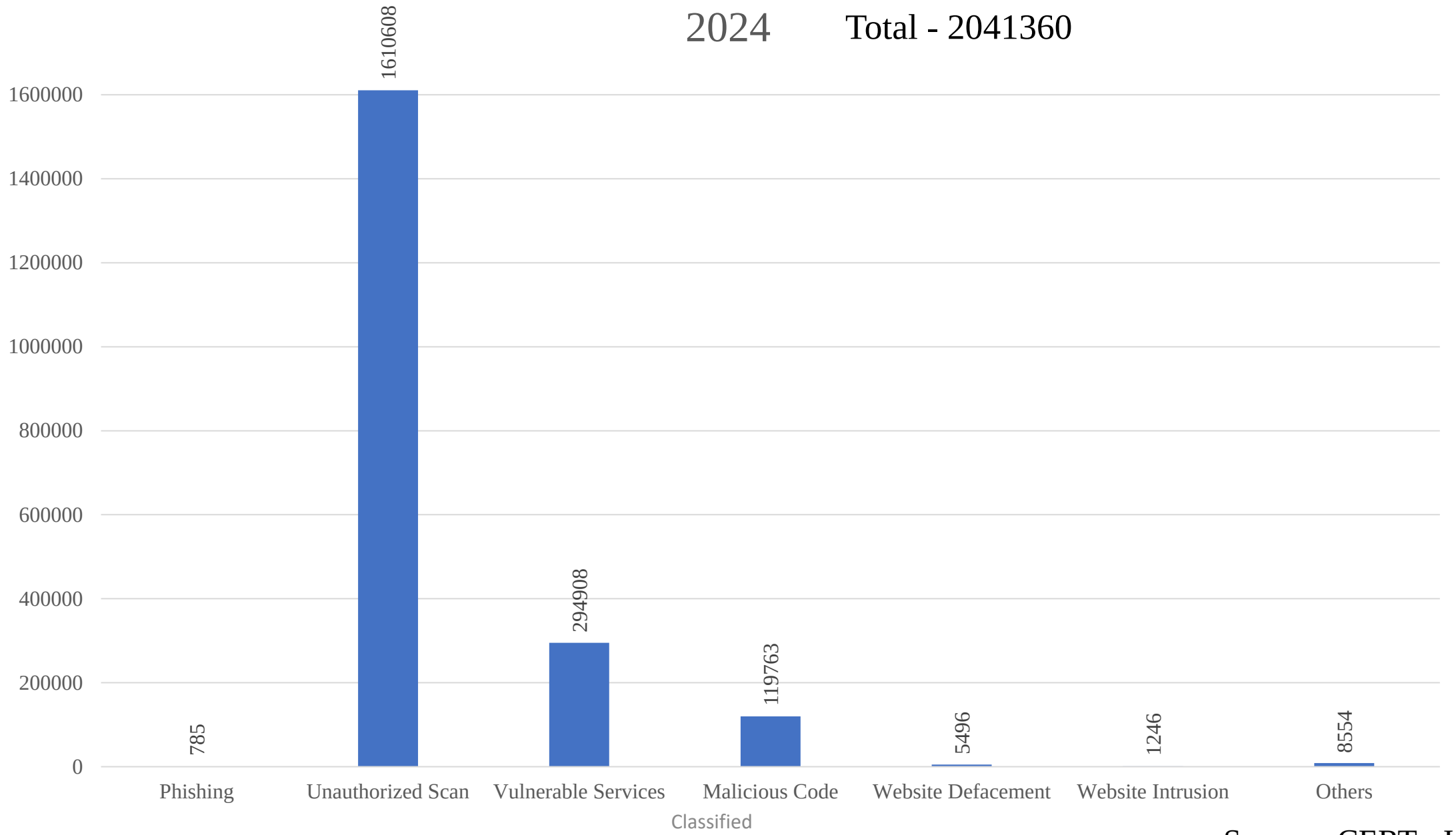
Year wise Incidents

Year	Incidents	Year	Incidents	Year	Incidents
2004	23	2011	28127	2018	208456
2005	254	2012	36924	2019	394499
2006	552	2013	41319	2020	1158208
2007	1237	2014	44679	2021	1402809
2008	2260	2015	49455	2022	1391457
2009	7981	2016	50362	2023	1592917
2010	9334	2017	53117	2024	2041360

Source : CERT - In



Source : CERT-In



Source : CERT - In

IT and OT

Information Technology (IT)

- Focus: Data confidentiality & integrity
- Priority: CIA (Confidentiality first)
- Environment: Offices, data centres
- Lifecycle: 3-5 years refresh
- Patching: Regular & automated
- Downtime: Scheduled maintenance
- Protocols: TCP/IP, HTTP, SQL

Operational Technology (OT)

- Focus: Process availability & safety
- Priority: AIC (Availability first)
- Environment: Gen, Trans, DISCOMs
- Lifecycle: 25+ years
- Patching: Rare, requires shutdowns
- Downtime: Extremely costly / impacts grid
- Protocols: Modbus, DNP3, protocols under 61850, 104 (60870 – 5), OPC

OT security – importance

- Impacts real time operation
- Compromised OT - physical harm, explosions, loss of life
- Disruption in critical services
- Downtime – loss in production – financial impact
- Damage – additional capital
- National Security
- Cascading effect

OT challenges

Legacy systems

Protocols security concerns - plain text, vulnerabilities

Patching frequency – compatibility – downtime

IT – OT convergence

Limited monitoring and security tools

Supply chain issues – dependency on foreign products / components

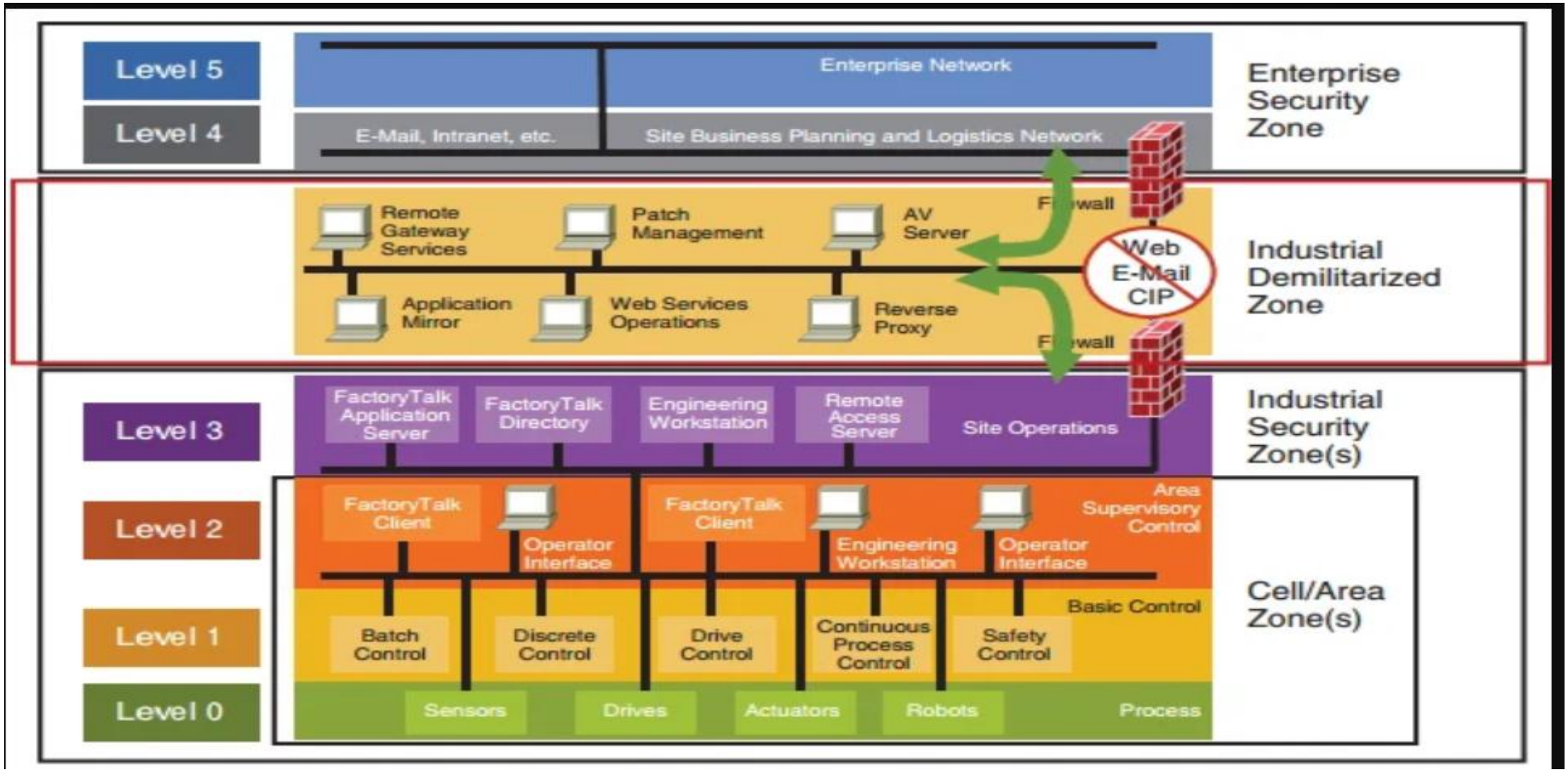
Third party services

Testing challenges

Purdue Model

Level 5	**Enterprise Network**	Internet, Cloud, public facing applications
Level 4	**Business Planning & Logistics**	IT Servers, Business Apps, Database, ERP, Email etc,
Level 3.5	**DMZ (Demilitarized Zone)**	Firewalls, Jump Servers, Data Diodes
Level 3	**Site Operations**	SCADA Servers, Historians, Patch Management
Level 2	**Area Supervisory Control**	HMI, Engineering Workstations, OPC
Level 1	**Basic Control**	PLCs, RTUs, DCS Controllers, Safety
Level 0	**Physical Process**	Sensors, Actuators, Valves, Motors

Purdue Model



Security Measures

- Whitelisting of devices (IP, Port)
- Access Control - MFA, RBAC (least privilege)
- Continuous Monitoring
- Secure Remote Access (Emergency & Trouble shooting) - Encrypted VPN + MFA, jump servers etc,
- Patching – Offline, jump server, authentication, integrity verification
- Segmentation
- Cyber security Audit – Risk assessment
- Testing compliance
- Reduce dependency on third party
- IT – OT airgap; Unidirectional gateways for IT – OT convergence
- Backup & Recovery –online & offline back ups
- OT Security Training – Mock-drills
- Standards – NIST 800 - 82, IEC 62443

CSIRT – Power

Established – 05.04.2023

Inaugurated – 23.09.2024

24 x 7 Operations

Security Operation Centre

Digital Forensic Lab

Malware Lab

Coordinating with utilities, CERT – In, NCIIPC, NSCS, MHA etc

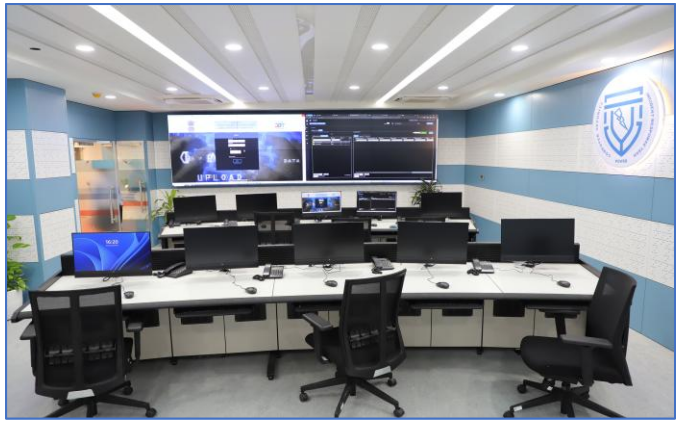
Support from 6 sub-sectoral CERTs

Gaps observed

Appointment of CISOs - Roles & Responsibilities of CISOs
Cyber Security Policy
Sector Specific Guidelines and SOPs
No. of onboard utilities
Monitoring and institutional mechanism
Deployment and configuration issues
Insecure Remote Access
IT - OT convergence and interconnection of OT with Grid
Hardware and software vulnerabilities
Testing
Third party dependency
Incident handling, response and management
Scope and quality of audit and closure of Audit findings
Support of - details about EOL and EOS - availability of security patches
Data residency
Collection of logs and artifacts
Awareness – limited resources - expertise

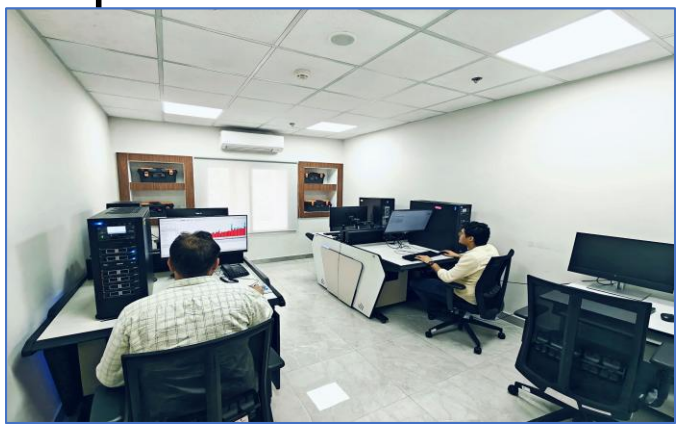
Incident Response

- Sector specific traffic monitoring
- Generate alerts
- Closure of vulnerabilities
- Incident Analysis – Triage
- Model BoQ for SoC and NoC



Digital Forensic Analysis

- Collection of Artifacts – Disk Image & RAM Dump
- In-depth Analysis
- Root Cause Analysis
- Malware Analysis



Policies & Regulatory Matters

Regulations, Testing, Threat Intelligence, CII, CCMP, R & D, Policies, Advisories, etc,

Capacity Building

Training, sub-sector specific training

Workshops / Awareness, Tailored training, Mockdrills

Cyber Security Audit

Audit, Risk Assessment, code assessment

Guidelines for scope of audit and Quality

Impact

Malicious IPs - 175

Malicious Domains – 168

Malware Files – 104

Malware Families – 25

APT Groups – 02

C2 IPs & Domains (IoCs) – 38

CISO – 281

CSK onboard – 247

Audit - 119 (IT) & 91 (OT)

CII assessment – 96

CCMP – 162 (additionally 51 entities in process of it)

800+ professionals were trained; created awareness for 700+ professional

CEA (Cyber Security for Power Sector) Regulations, 2026

No. of utilities onboard

Updated network architectures

Monitoring - SoC and NoC for LDCs

Reduced detection time and containment time

Scope & Quality of audit; No. of audits and closure of findings

Reduced attack surface - Quarterly bulletin, Vulnerabilities closure

Facilitating log and artifacts retention

36 + one to one meetings cum engagements - for sensitizing, incident, forensic analysis, infrastructure review etc.

Focus Areas

Secure IT and OT convergence, Compliance of testing orders, SBoM, HBoM, Data Residency, Secure remote access and operation, ERs for devices, Implementation of Regulations, Capacity building, log retention, dependency on third party etc,

Services Provided

Alerts Generation

Capacity Building – Tailored training, Mockdrills, Awareness

Quarterly Bulletin – Threat Intelligence

Onsite support in Incident Management

Forensic Analysis

Malware Analysis

Cyber Security Audit – Risk Assessment

Review of Network Architecture

Advisories, SoPs and Guidelines

CCMP

Closure of audit observations

Seqrite 2026 - Cyber Security Maturity Model (India)

10 Parameters

Process; People; Technology; Data Security; Malware Protection

Access Control; Secure Configuration; Software Update & Patch Management; Back Up & Restore; and Incident Response

Classification

- BFSI; Energy
- Automobile and Manufacturing
- Education, Telecom and Healthcare

Takeaways

Defence in depth

Different layers and phases of attack

Minimize the attack surface

Identify Assets

Risk assessment

Deploy Security Controls

Monitor Assets

Close Vulnerabilities

Detect & Verify Abnormalities

Identify Infection

Collect the artifacts

Contain the infection

Recover from infection

Restore system

Review and update

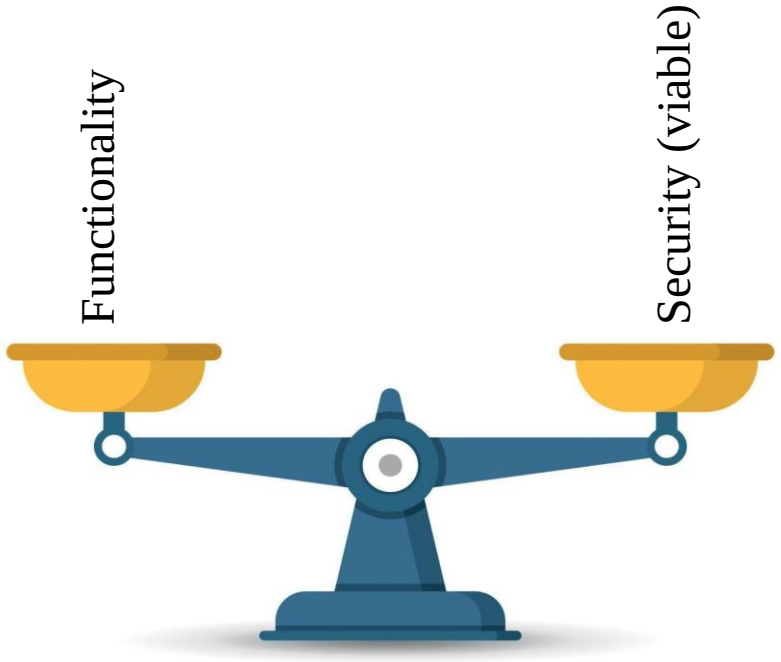
Requirements

Awareness

Capability

Willingness

Budget



Cyber Security Regulations, 2026

Effective from 01.04.2027

Applicable – All entities (Gen - 50 MW & above plants);

CSIRT – Power role

CISO – ring fencing

ISD – within India

Critical and non-critical systems

Data residency

Annual cyber security audit – IT and OT

Cyber security requirements in FAT and SAT

Log and artifacts retention

Cross border entities

Control & operation within national boundaries – isolated from internet

Perimeter security devices for OT environment

Protection of communication channel between two entities

CISO – citizen and resident of India

Cyber Security Policy

Personnel risk assessment of third party manpower

Phase out obsolete / legacy assets

Separate reference time source for OT

Retention of critical documents – FAT, SAT, Remote access, changes etc,

OEM compliances – support

Time bound closure of audit findings

Self Audit – compliance of regulations

THANK YOU

Toll Free No. 1800 111 410 www.csirt-power.gov.in helpdesk.csirtpower@gov.in