Host Utilities

TATA

TATA POWER

BSES

BSES Rajdhani Power Limited

BSES

BSES Yamuna Power Limited

NPCL

NOIDA POWER COMPANY LIMITED

SESSION PARTNER

Hitachi Energy

ORGANIZER

ISGF

India Smart Grid Forum

Supporting Ministries

सत्यमेव जयते

MINISTRY OF POWER

GOVERNMENT OF INDIA

सत्यमेव जयते

MINISTRY OF NEW AND RENEWABLE ENERGY

GOVERNMENT OF INDIA

सत्यमेव जयते

DEPARTMENT OF SCIENCE & TECHNOLOGY

सत्यमेव जयते

NITI Aayog

सत्यमेव जयते

MINISTRY OF POWER

GOVERNMENT OF INDIA

CENTRAL ELECTRICITY AUTHORITY

India SMART UTILITY Week 2025

Session : Building resilient utilities

Building Resiliency Against Cyber Attacks

Presented By

Vijayan SR, Principal Technical Consultant, Grid Automation, Hitachi Energy

Cybersecurity Risks in Critical Infrastructure

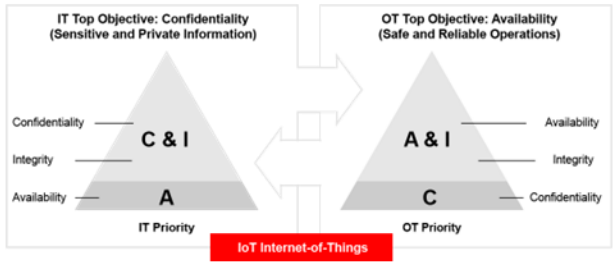
Main Factors Contributing to Cybersecurity Risks

Digitalization

- From air gapped to connected systems
- Increased attack surface
- Coexistence with legacy OT products

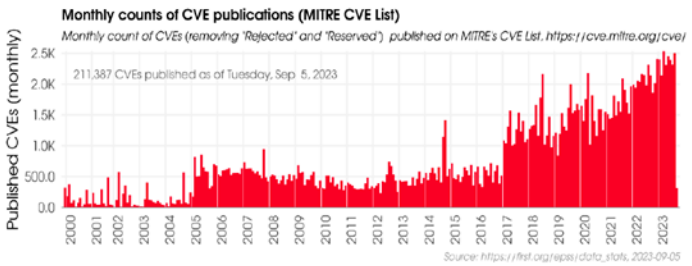
IT/OT Convergence

- Off the shelf products
- From proprietary to standardized protocols
- Unauthorized lateral access to OT systems via IT networks



Threat Landscape

- Hacktivists actors
- State-backed APTs
- Increase number of vulnerabilities



Human

- Human error
- Social engineering
- Phishing attacks
- Remote work
- Internal threats

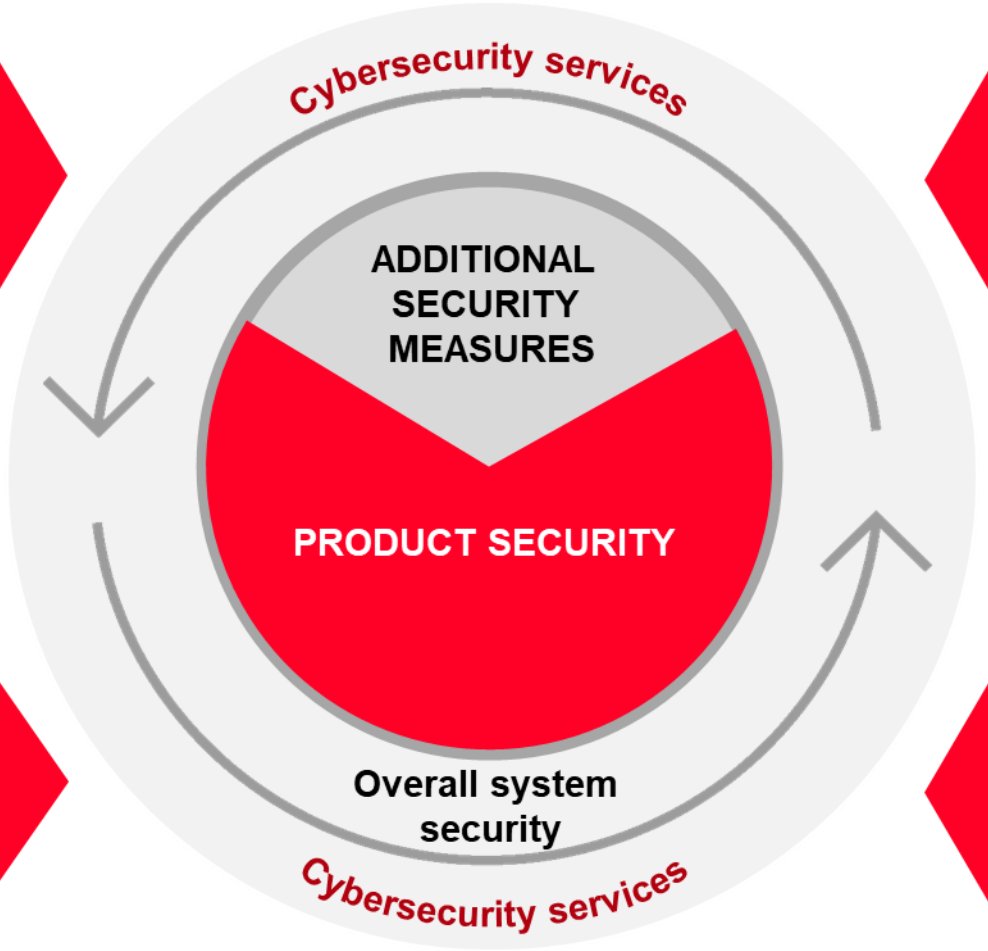
Cybersecurity Risks in Critical Infrastructure

Evolving threats

Threats are constantly evolving with new technologies and attack methods.

Keeping up with the changes

The environment in which the system operates can change (additional device, company priorities, ownership, etc.).



Aging system

The operated equipment is aging (e.g., EOL OS) or no longer complies with security requirements, with the risk of system unavailability due to HW outages or missing backups.

Changing regulations

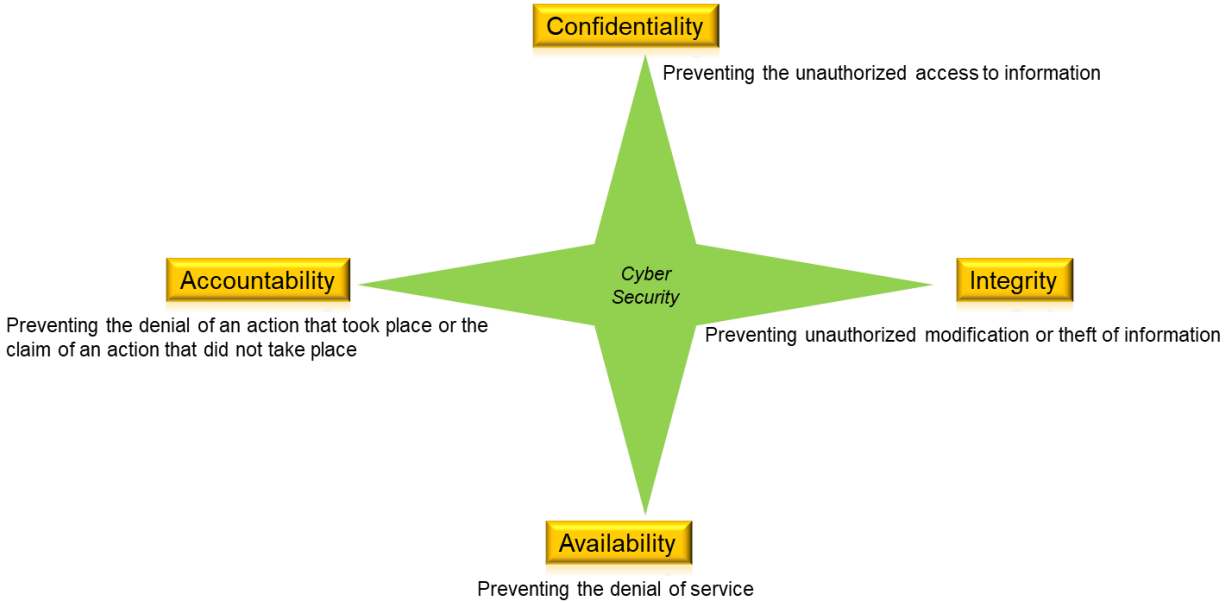
Legislation, customer internal regulations, and legal requirements continue to develop.

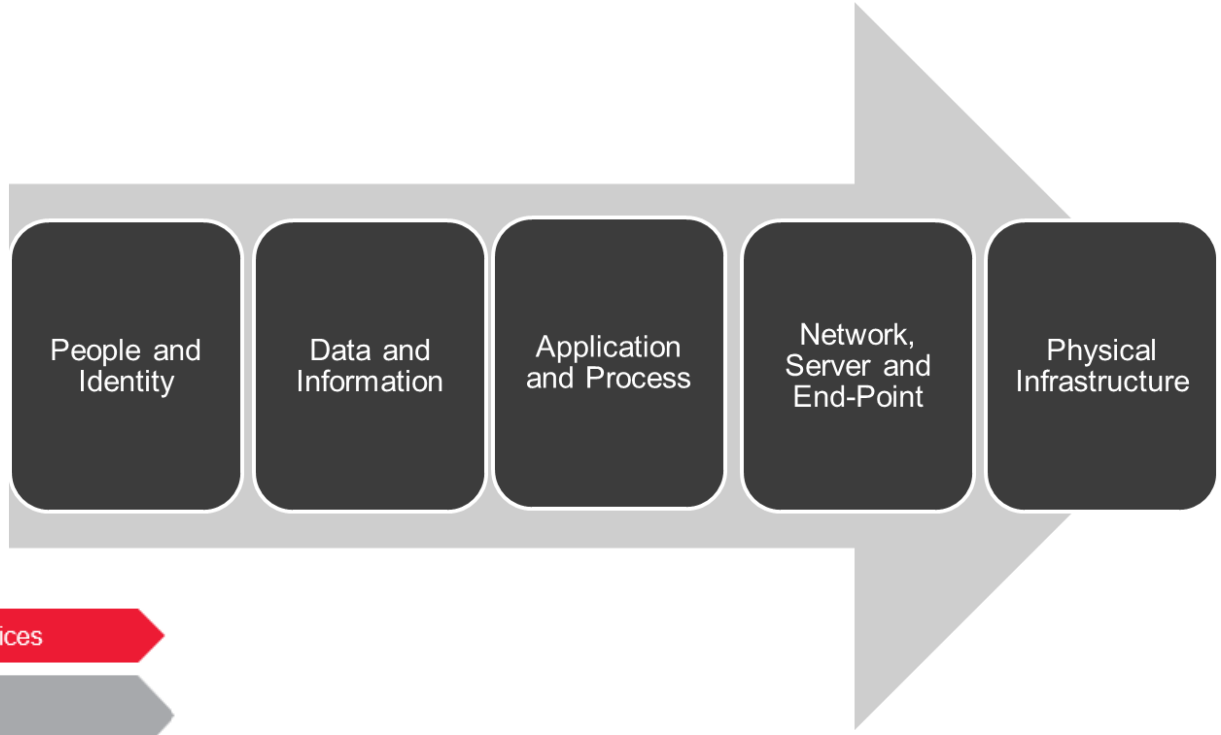
Cyber Security Mitigation

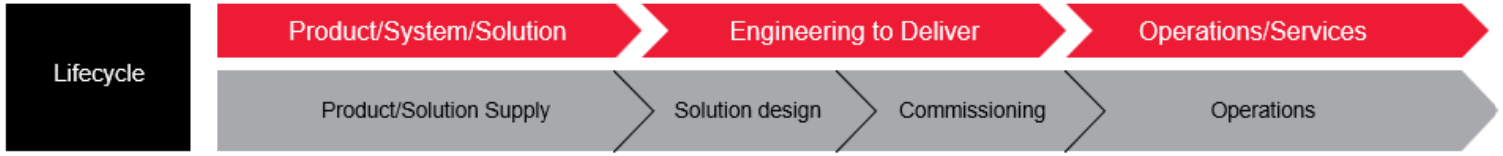
What does it mean?

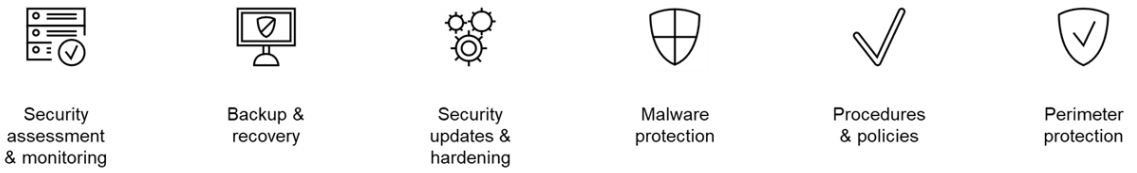
"Measures taken to protect power and automation systems against unauthorized access, attacks, disruption or loss."

Cyber Security Mitigation

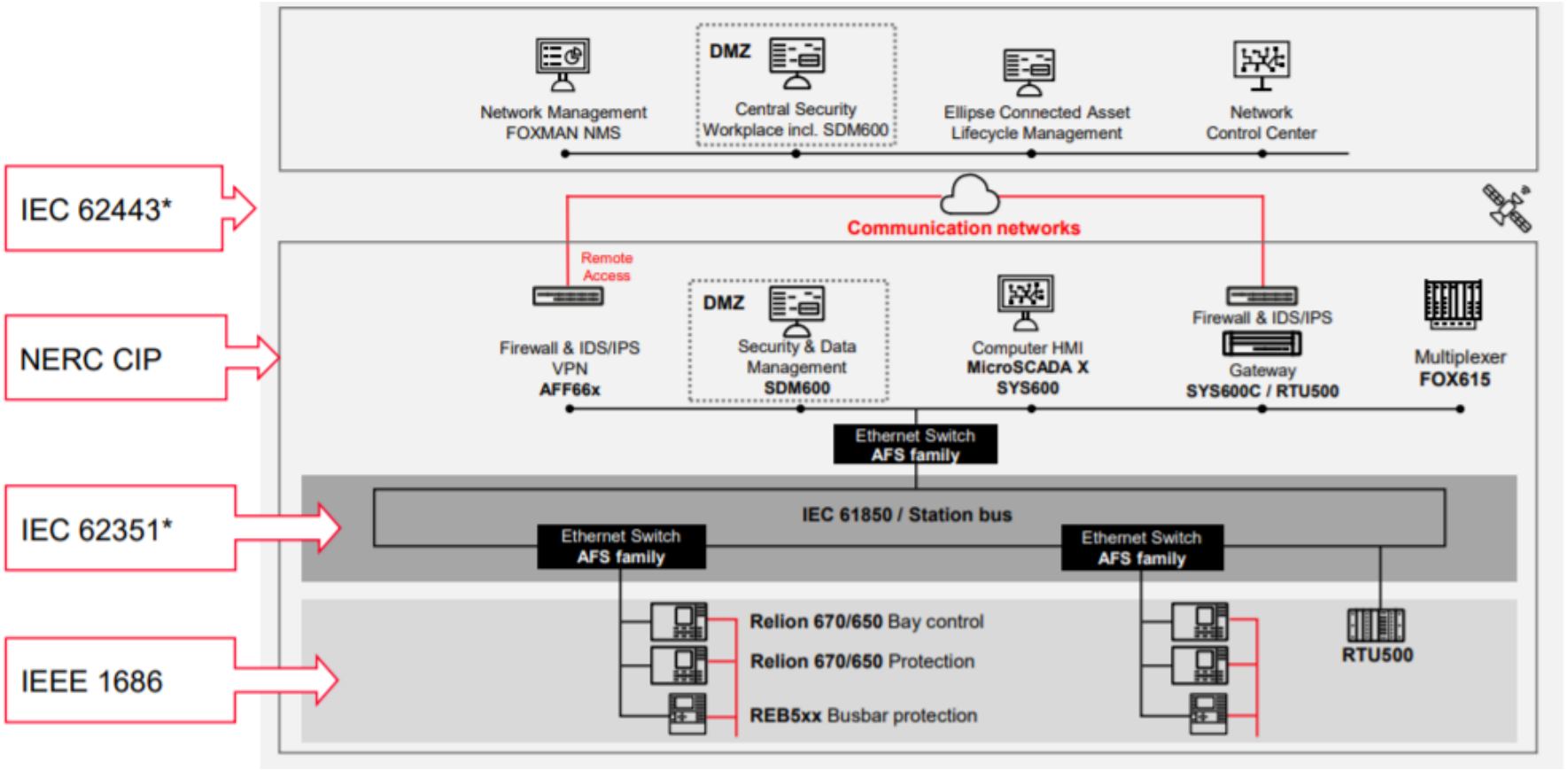








Cybersecurity Standards



Technical Aspects

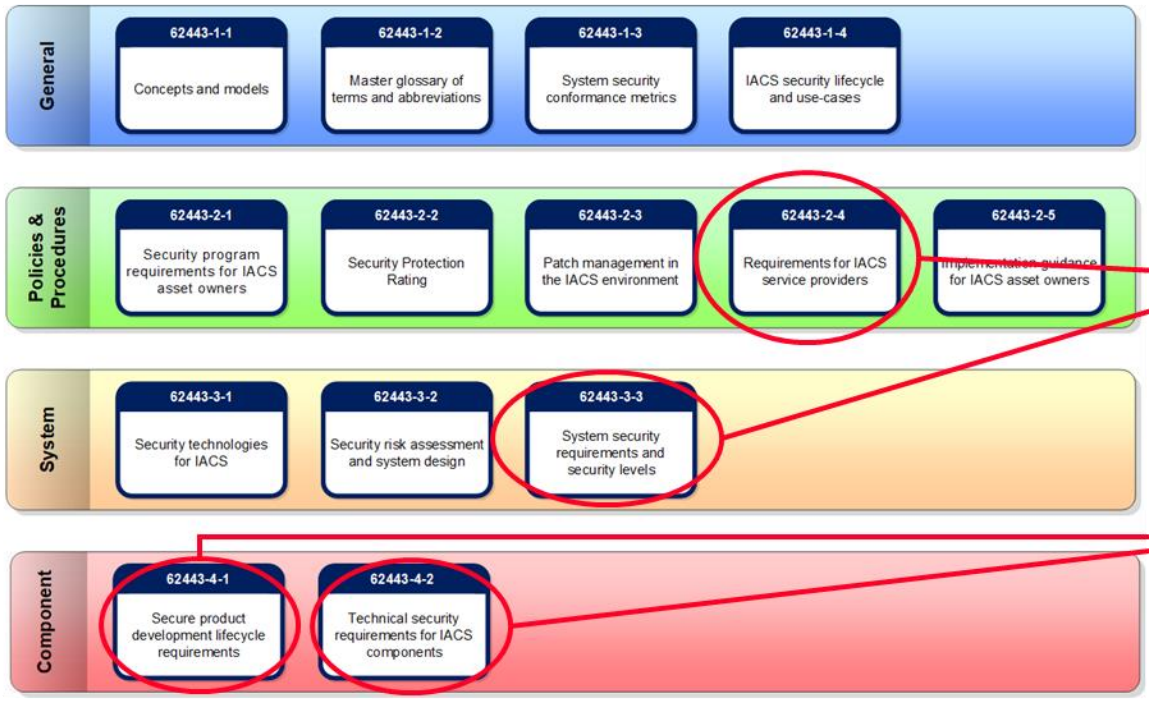
- IEC 62351, ISO/IEC 62443, and IEEE 1686 are mainly relevant for Hitachi Energy as manufacturer

Management Aspects

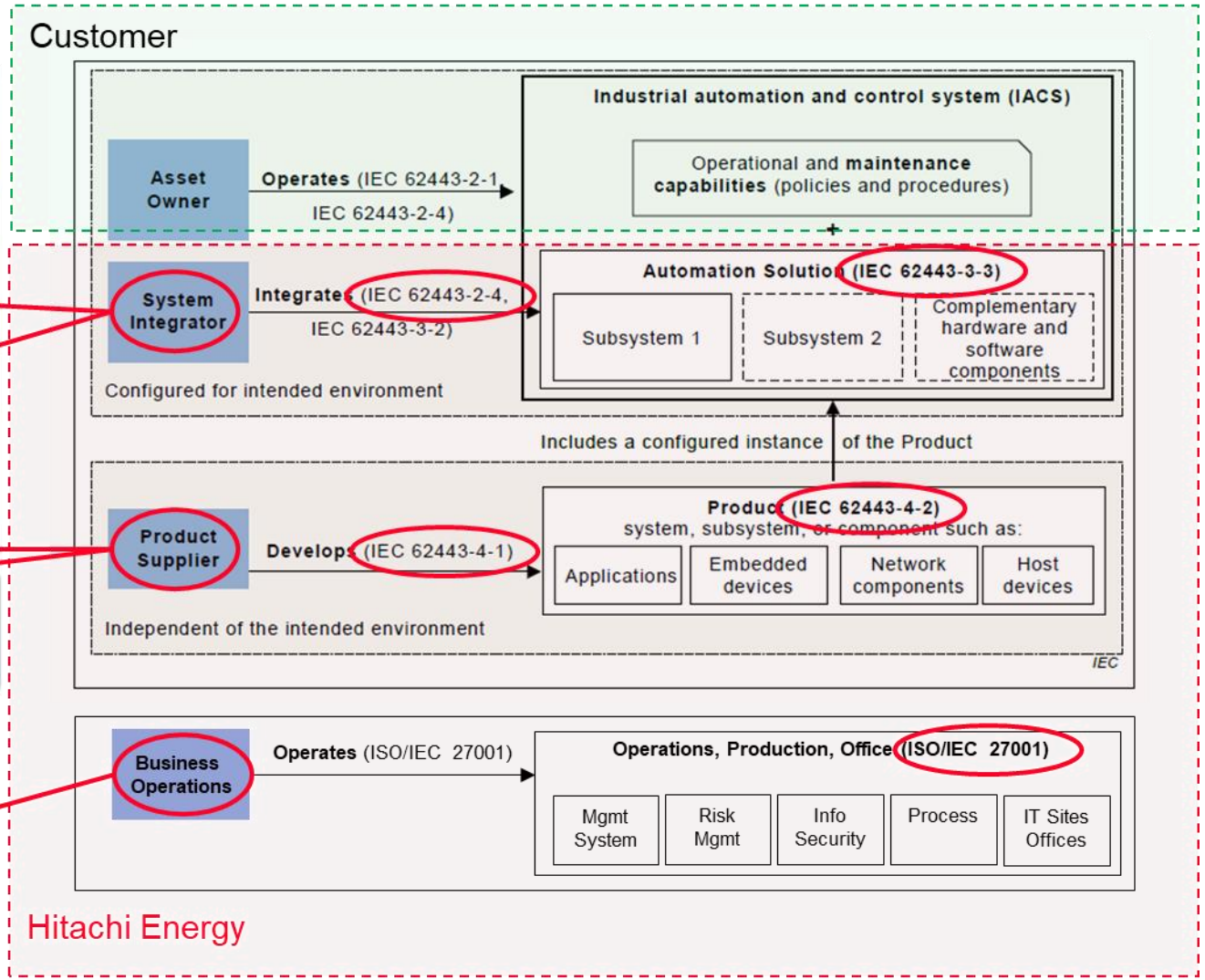
- IEC 62443 (former ISO 99), NERC-CIP, and ISO 27000 address the processes of an organization

Cybersecurity Standards

From the IEC 62443 Family:



From the ISO/IEC 27000 Family:



Cyber Security Mitigation

- Zoning & Perimeter Protection
- Secure Communication
- Account Management
- Malware Protection
- Patch Management

L3 – Communication Level:

- Secure communication (Encryption, real-time)

L2 – Station Level:

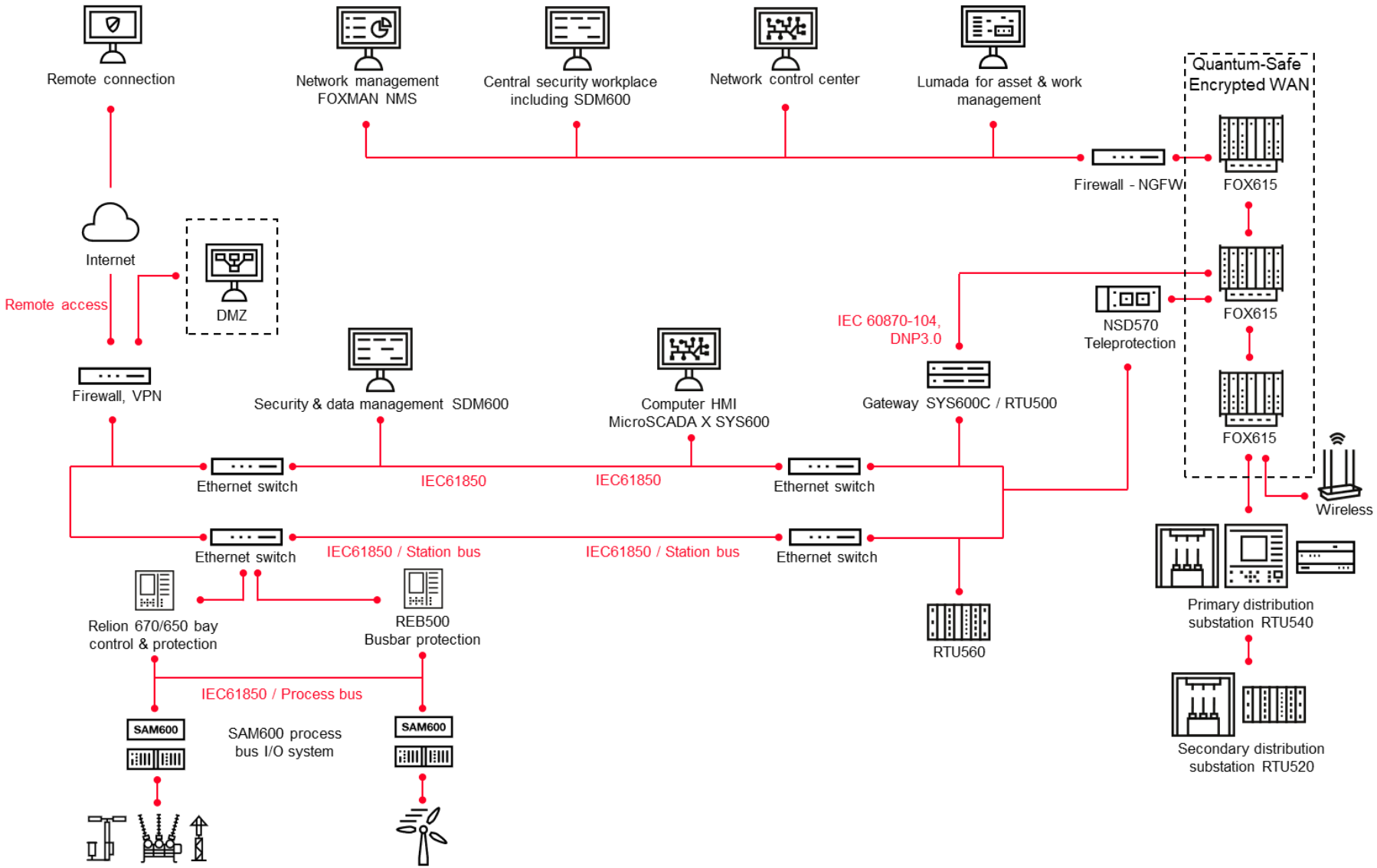
- Zoning & Perimeter Protection
- Malware Protection
- Patch Management
- Backup & Recovery
- Account Management
- Security Logging & Monitoring
- System Hardening

L1 – Bay Level:

- Zoning & Perimeter Protection
- Secure Communication
- Account Management
- Security Logging & Monitoring
- Product Hardening

L0 – Process Level:

- Zoning & Perimeter Protection
- Product Hardening



Three steps to cyber security protection

01. Assess

- Hitachi Energy carries out a cybersecurity assessment and an interview with you to understand your processes and procedures.
- A detailed cybersecurity assessment report is then produced and provided to you along with a set of recommended actions for improved cybersecurity.

02. Implement

- Hitachi Energy provides recommended actions for you to implement based on the cybersecurity assessment and our domain expertise.
- Upon agreement Hitachi Energy implements the recommendations to your system, ensuring your critical systems are more secure.

03. Sustain

- By appointing Hitachi Energy as your cybersecurity partner; you enter a care agreement which ensures you benefits from Hitachi Energy' huge domain expertise across the globe.
- Your power systems will be regularly assessed and monitored by the cybersecurity service team for any potential cybersecurity infringements.

Cybersecurity vigilance is a long term sustained approach

KEY TAKEAWAYS / RECOMMENDATIONS

Detect, Protect and Respond (Assess, Implement, Sustain)

The implementation should be able to minimize the attack surface, detect possible attacks and respond in an appropriate manner to minimize the impacts

Defense in Depth

No single security measure itself is foolproof as vulnerabilities and weaknesses could be identified at any time. In order to reduce these risks, implementing multiple protections in series avoids single point of failure.

Technical, Procedural and Managerial measures

Technology is insufficient on its own to provide robust protection. Cyber security policies and processes must be implemented in the organization to best be able to assess and mitigate the risks and respond to incidents.

Implementing solutions around cyber security has to be a continuous process. It's not only important to protect a system from the current vulnerabilities, but is also equally important to have mechanisms (technical and process) in place to quickly detect and effectively react to any incidents and isolate security breaches.

There is no such thing as 100% security.

CYBERSECURITY IS NOT A DESTINATION BUT AN EVOLVING TARGET.

Host Utilities

TATA

TATA POWER

BSES

BSES Rajdhani Power Limited

BSES

BSES Yamuna Power Limited

NPCL

NOIDA POWER COMPANY LIMITED

SESSION PARTNER

ADD LOGO OR DELETE IF NO PARTNER

ORGANIZER

ISGF

India Smart Grid Forum

Supporting Ministries

सत्यमेव जयते
MINISTRY OF POWER
GOVERNMENT OF INDIA

सत्यमेव जयते
MINISTRY OF NEW AND RENEWABLE ENERGY
GOVERNMENT OF INDIA

सत्यमेव जयते
DEPARTMENT OF SCIENCE & TECHNOLOGY

सत्यमेव जयते
NITI Aayog

सत्यमेव जयते
MINISTRY OF POWER
GOVERNMENT OF INDIA
CENTRAL ELECTRICITY AUTHORITY

India SMART UTILITY Week 2025

THANK YOU

For discussions/suggestions/queries email: isuw@isuw.in

www.isuw.in

Links/References (If any)