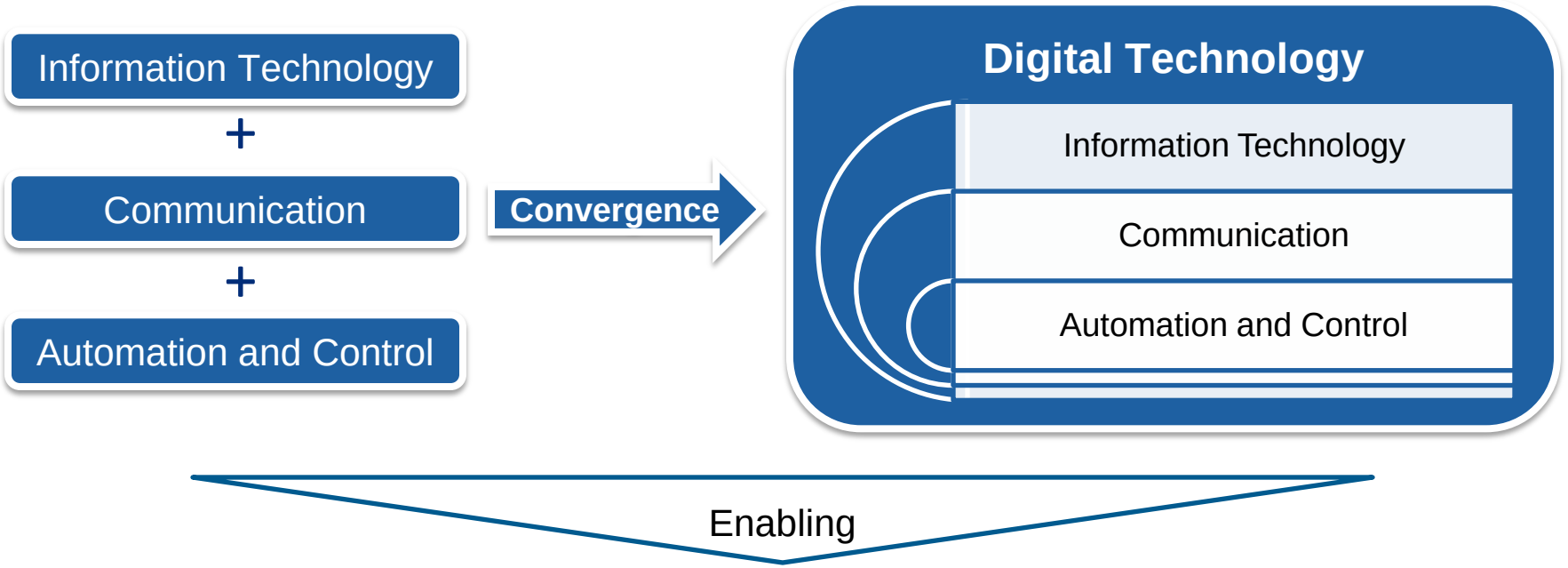
Communication Networks and Cyber Security”

Mitul Thapliyal
Principal – Infosys Ltd

Contents

- Introduction
- Power sector's key security concerns
- How to address these concerns
- CIPS based approach for handling security

Technology convergence is changing the way we manage our power system



- Pervasive intelligent devices across the power system
- Move from monitoring to control (bidirectional information flow)
- Automated systems for managing grid (outage management, distribution automation, AMI etc.)
- Participation from consumers, suppliers, grid managers, generators, distributed energy generators

Power sector's key security concerns

1. Identity Management - User and Role
   - Single Sign On for usability viz. increased vulnerability
   - Remote login
   - Password sharing

2. Information flooding requiring real time responses : too many notifications to users
   - Pressure on Quality of response and reaction time
   - Reflexes of user need to be much faster.
   - Data and Information Security

3. Depth of Authentication prior to accepting control/configuration commands…and feedback loops

4. Security Governance of Distributed Intelligence

5. Public shared infrastructure – service quality and security

6. Communication latencies – security hazard?

7. Privacy concerns of users

8. Recovery in event of Security incidents/Disasters

AMI/Smart Metering is most vulnerable because of accessibility

How to address these concerns – There are many Security Compliance Standards and Technologies

- IEC and CIPS standards available – a few are directly usable, some need adaptation and some are evolving.
- NIST has come out with Guidelines for Smart Grid Cyber Security (NISTIR 7628).
- NIST's CSWG will now address combined power systems; information technology (IT) and communication systems in order to maintain the reliability of the Smart Grid; the physical security of all components; the reduced impact of coordinated cyber-physical attacks; and the privacy of consumers.
- CIGRE D2.24 Working Group is defining security standards for the next generation of Energy Management Systems (EMS) and related real-time grid and market systems.
- ISGF has formed a Work group focusing on Security.
- BIS LITD10 Workgroup on Security is working on developing Security Standards for India.

CIPS based approach for handling security

Introduction

- About NERC

  North American Electric Reliability Corporation (NERC), formerly North American Electric Reliability Council is a non-profit organization formed in 1965 as a voluntary organization of the electric Utilities in the USA and Canada. In July 1996, US FERC granted legal authority to NERC for enforcing reliability standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. NERC is committed to ensure the reliability of the bulk power system in North America. NERC develops and enforces reliability standards, monitors the bulk power system and trains industry personnel.

- About Critical Infrastructure Protection Standards(CIPS)

  The NERC-CIP standards touch utilities' computers related operation of the grid, data collection and data dissemination throughout the enterprise. First CIP standards were submitted by NERC in August 2006, which replaced NERC's voluntary industry UA 1200 guidelines. All CIP standards make it mandatory to document and review all procedures and policies every year. Utilities and other bulk power industry participants that violate any standards are likely to face enforcement actions including fines of up to $1 million a day. Documenting and demonstrating compliance with these standards on an ongoing basis is a daunting task unless a utility employs a rigorous approach leveraging technology to make the job easier

How to define a Critical Facility?

Any facility or combination of facilities, if severely damaged or destroyed would:

- have a significant impact on the ability to serve large quantities of customers for an extended period of time,
- have a detrimental impact to the reliability or operability of the energy grid, or
- cause significant risk to National security, National economic security, or public health and safety.

List of CIP Standards along with web link

Number	Title/Summary	Adoption Date	Link
CIP-001-2a	**Sabotage Reporting** Disturbances or unusual occurrences, suspected or determined to be caused by sabotage, shall be reported to the appropriate systems, governmental agencies, and regulatory bodies.	02.16.2011	pdf
CIP-002-4	**Cyber Security - Critical Cyber Asset Identification** NERC Standards CIP-002-4 through CIP-009-4 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System. These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets. Standard CIP-002-4 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of the criteria in Attachment 1 (of the standard).	01.24.2011	pdf

Note: Only latest version and adoption date of that version are shown here.

List of CIP Standards along with web link……(cont.)

Number	Title/Summary	Adoption Date	Link
CIP-003-4	**Cyber Security - Security Management Controls** Standard CIP-003-4 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.	01.24.2011	pdf
CIP-004-4	**Cyber Security - Personnel & Training** Standard CIP-004-4 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.	01.24.2011	pdf
CIP-005-4a	**Cyber Security - Electronic Security Perimeter(s)** Standard CIP-005-4a requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-4a should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.	01.24.2011	pdf
CIP-006-4c	**Cyber Security - Physical Security of Critical Cyber Assets** Standard CIP-006-4c is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-4c should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.	01.24.2011	pdf

List of CIP Standards along with web link……(cont.)

Number	Title/Summary	Adoption Date	Link
CIP-007-4	**Cyber Security - Systems Security Management** Standard CIP-007-4 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.	01.24.2011	pdf
CIP-008-4	**Cyber Security - Incident Reporting and Response Planning** Standard CIP-008-4 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.	01.24.2011	pdf
CIP-009-4	**Cyber Security - Recovery Plans for Critical Cyber Assets** Standard CIP-009-4 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009-4 should be read as part of a group of standards numbered Standards CIP-002-4 through CIP-009-4.	01.24.2011	

How to use CIPS?

- Use these as guidelines to describe
  - general approaches
  - considerations
  - practices
  - planning philosophies

- Do not use this as a “cookbook” for protection.
- Create you own standards based on CIPS

Six phase process for adopting CIPS in your Utility

Phase 1: Get Started	Phase 2: Create Documentation System and Train Security Personnel	Phase 3: Secure Physical and Cyber Assets	Phase 4: Create Incident Reporting and Recovery System	Phase 5: Implement Compliance Technology	Phase 6: Prepare for Audit
• **Step 1:** Build a Team and Select an Approach • **Step 2:** Identify Assets and Perimeters (CIP-002, 005, 006)	• **Step 3:** Assess Documentation Requirements (CIP-002, 009) • **Step 4:** Train Security Management Controls Personnel (CIP-003, 004)	• **Step 5:** Assess Physical Security Readiness (CIP-006) • **Step 6:** Assess Cyber Security Readiness (CIP-005 ,007)	• **Step 7:** Implement Incident Reporting and Recovery Plans (CIP-008 ,009)	• **Step 8:** Implement Technology to Automate Compliance Requirements • **Step 9:** Implement Process to Collect Compliance Documentation	• **Step 10:** Conduct a Pre-Audit Assessment and Audit

Thanks