Doc No. LITD 10 (24782) WC
Draft IS 16335: 2024
November 2024

BUREAU OF INDIAN STANDARDS
DRAFT FOR COMMENTS ONLY

मसौदा भारतीय मानक

पावर कंट्रोल सिस्टम - सुरक्षा आवश्यकताएँ

(*पहला पुनरीक्षण*)

Draft Indian Standard

Power Control Systems – Security Requirements

(*First Revision*)

ICS 33.200

LITD 10 Power System Control and Associated Communications Sectional Committee	Last Date for Comments: 18 January 2025

Contents

FOREWORD

This draft Indian Standard was adopted by the Bureau of Indian Standards, after the draft finalized by the Power System Control and Associated Communications Sectional Committee and approved by the Electronics and Information Technology Division Council.

The objective of this standard is to provide guidelines for the protection of critical assets for all entities involved in generation, transmission, distribution, grid operation and trading of electric power. Safety, security, and reliability have always been important issues in the design and operation of systems in the power industry. In recent years, information security has also come into prominence owing to the presence of multiple competing entities that need to exchange relevant information but at the same time protect confidential critical information infrastructure.

In preparing this standard, considerable text has been derived from NERC CIP, IEC 62443 and IEC 62351 standards. The Working Group members acknowledge and appreciate the efforts of the NERC Committee which draft the Critical Infrastructure Protection Standards.

The aspect of cyber security is fast changing and over a period of time the necessary standards and guidelines viz., IEC 62351 series, ISO/IEC 27000 series, IEC 62443 series, NERC CIP were revised/amended/new part(s) included and guidelines/order/regulation on the object were issued across the globe including India for providing best protection and for ascertaining grid resiliency. To incorporate these changes, IS 16353 has been revised. In the revised standard, some of the text have been modified to reflect the changes in the aforementioned standards/guidelines. A few new term & definitions have been added. Also a new clause on the requirements of supply chain risk management has been specified.

Doc No. LITD 10 (24782) WC
Draft IS 16335: 2024
November 2024

Indian Standard
Power Control Systems – Security Requirements

(*First Revision*)

1 SCOPE

1.1 Objective

This standard provides guidelines for identification and protection of critical assets for all entities involved in generation, transmission, distribution, grid operation and trading of electric power. The standard covers the following:

a) Critical Asset Identification and Monitoring
b) Security Management for Personnel and Assets
c) Electronic and Physical Security of Assets
d) Incident Reporting and Response and Recovery Planning
e) Auditing and Conformance Procedures

2 REFERENCES

The Standards listed in Annex A and Annex B contains provisions which, through reference in this text, constitute provisions of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision and parties to agreement based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated in Annex A and Annex B.

3 TERMINOLOGY

For the purpose of this standard the definitions given in IEC/TS 62351–2 and the following shall apply.

3.1 **Asset –** Anything that has value to the organization.

3.2 **External threat –** A threat originating outside a company, government agency, or institution.

3.3 **IT –** Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. *

3.4 **Internal threat –** A threat originating from inside the organization.

3.5 **OT –** Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. *

3.6 **Policy –** Overall intention and direction as formally expressed by management.

3.7 **Robustness –** The persistence of a system's characteristic behaviour under perturbations or conditions of uncertainty.

3.8 **Critical Asset –** Shall mean the facilities, systems and equipment which, if destroyed, degraded or otherwise declared unavailable, would affect the reliability or operability of the Power Supply System.

3.9 **Cyber Assets –** Shall mean the programmable electronic devices, including the hardware, software and data in those devices that are connected over a network, such as LAN, WAN and HAN

3.10 **Critical Cyber Assets –** Cyber assets essential to the reliable operation of critical asset.

*Reproduced from NIST Special Publication 800-37 Rev. 2

3.11 Acronyms

CEA	Central Electricity Authority
CERT	Computer Emergency Response Team
CERT In	Indian Computer Emergency Response Team
CIP	Critical Infrastructure Protection
DISCOM	Distribution Company
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISA	International Society of Automation
MMS	Manufacturing Message Specification
NCIIPC	National Critical Information Infrastructure Protection Centre
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standard And Technology
RFC	Request for Comment
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol

4 SECURITY OVERVIEW

4.1 The management of power system infrastructure has become reliant on the information infrastructure as automation continues to replace manual operation, market forces demand more accurate and timely information, and the power system equipment ages. Therefore, the reliability of the power system is increasingly affected by any problems that the information infrastructure might suffer. As the power industry relies increasingly on information to operate the power system, two infrastructures now have to be managed: Power System Infrastructure, and Information infrastructure.

In the past, information for managing these infrastructures was only available to a select set of people and these infrastructures were not a target for unauthorized access. Security was achieved through obscurity for the most part.

However, security by obscurity is no longer a valid concept. In particular, the electricity market is pressuring market participants to gain any edge they can. A tiny amount of information can turn a losing bid into a winning bid – or withholding that information from your competitor can make their winning bid into a losing bid. And the desire to disrupt power system operations can stem from simple teenager bravado, to competitive game-playing in the electrical marketplace, to actual terrorism. It is not only the market forces that are making security crucial, the sheer complexity of operating a power system has increased over the years, making equipment failures and operational mistakes more likely and their impact greater in scope and cost. In addition, the older, “obscure” frameworks are being replaced by standardized, well-documented frameworks that are more susceptible to hackers and industrial spies. Additionally, integrated operation of power and information systems has increased security vulnerability.

4.2 This has brought about a need for creating a security framework for all associated

infrastructures. For new developments that are happening in each field, security is now considered as a basic and required feature instead of an add-on.

Security entails a much larger scope than just the authentication of users and the encryption of communication. End-to-end security involves security policies, access control mechanisms, key management, audit logs, and other critical infrastructure protection issues. It also entails securing the information infrastructure itself.

4.3 Security threats can be classified into Inadvertent and Advertent Threats. They are further classified as follows:

a) Inadvertent Threats:
   1) Safety Failures
   2) Equipment Failures
   3) Carelessness
   4) Natural Disasters

b) Deliberate Threats:
   1) Disgruntled Employee
   2) Industrial Espionage
   3) Vandalism
   4) Cyber Hackers
   5) Malware (Viruses, Worms, etc.) and Hardware Trojan
   6) Theft
   7) Terrorism

The key point is that the overall security of power system operations is threatened not only by deliberate acts of espionage or terrorism but by many other, sometimes deliberate, sometimes inadvertent threats that can ultimately have devastating consequences.

4.4 The objective of the Cyber Security is the preservation of the following:

a) Confidentiality – preventing the unauthorized access to information
b) Integrity – preventing the unauthorized modification or theft of information
c) Availability – preventing the denial of service and ensuring authorized access to information
d) Non-repudiation or accountability – preventing the denial of an action that took place or the claim of an action that did not take place
e) Safety – Physical security of the equipment.

4.5 The security requirements and possible threats or types of attacks are illustrated in the Figure 1.

Figure 2 describes the overall security management: security requirements, threats, countermeasures, and management.

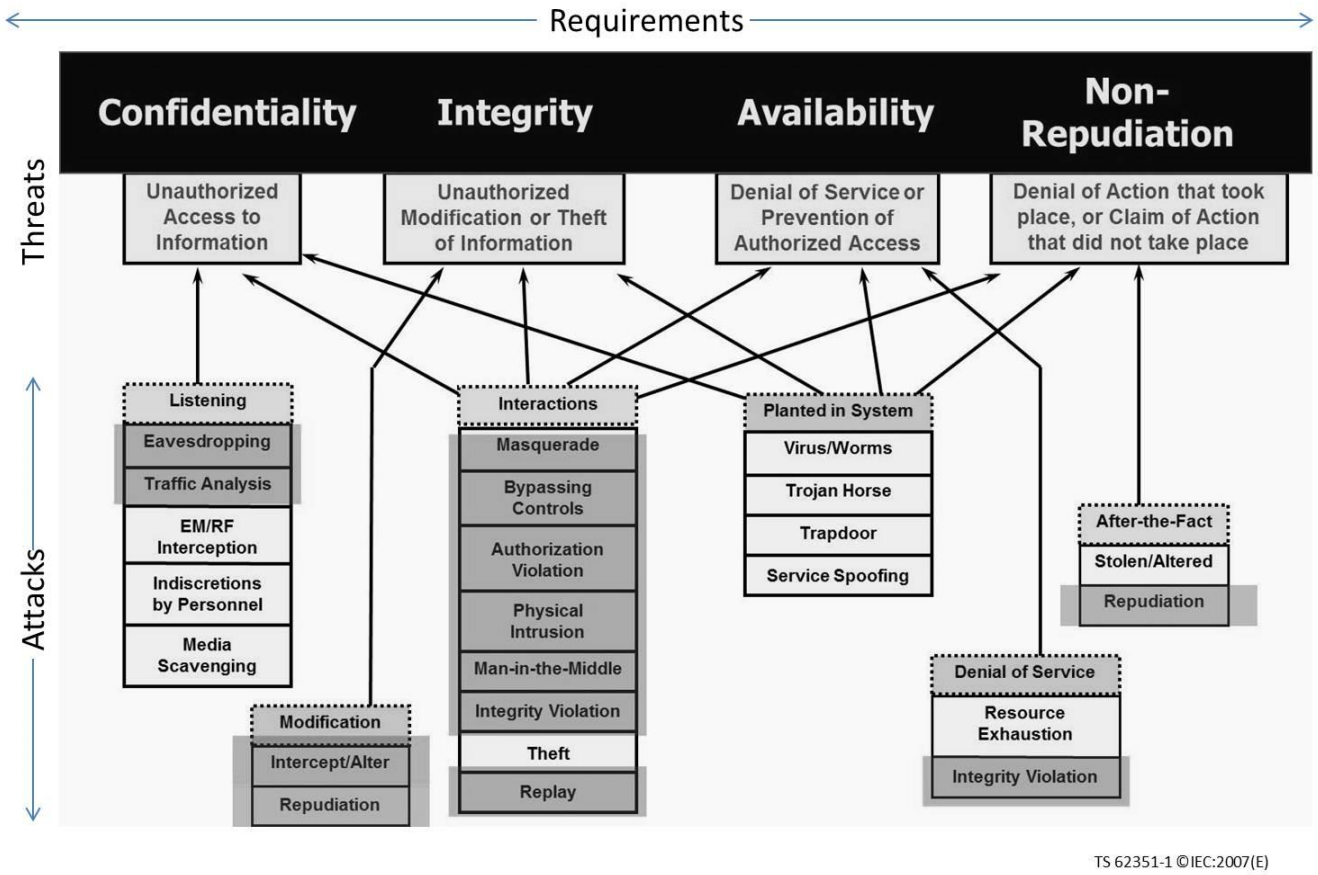

Fig. 1 Security Requirements, Threats, and Possible Attacks

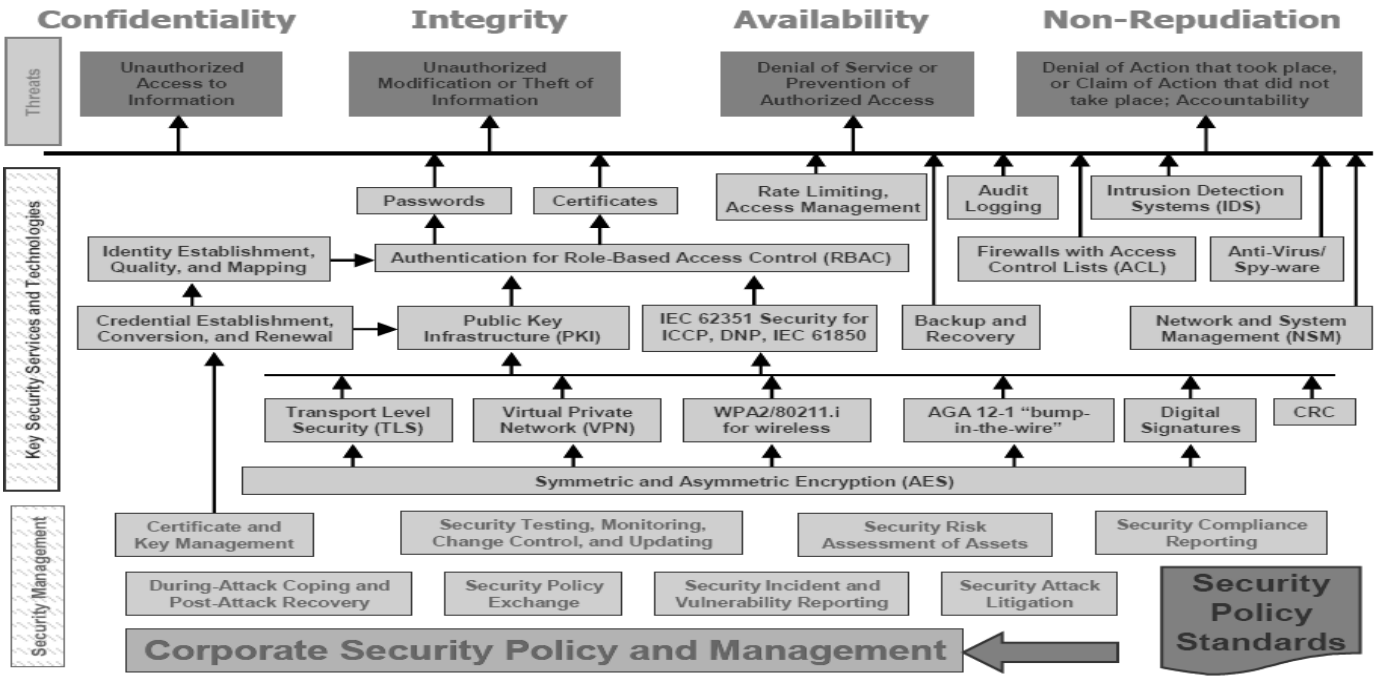

Fig. 2 Overall Security: Security Requirements, Threats Countermeasures and Management

5 SECURITY STANDARD REQUIREMENTS

Within the text of this Standard, "Responsible Entity" shall mean:

a) Generator Operators and Generator Owners
b) Transmission Utilities
c) Distribution Companies (DISCOMs)
d) Load Despatch Centres
e) Regional Power Committees (RPCs)
f) Power Trading Exchanges

In this standard, the term "years", when used to refer to periodicity, shall be interpreted as the financial reporting year that is followed by the Responsible Entity. When the standard refers to the term "every year", it shall indicate once a year in every financial year with the condition that the duration between two events is not more than 12 months.

The auditing and conformance requirements shall be in accordance with clause 6.

[The Violation Severity Levels in case any of the requirements of this Standard are not implemented and also are not currently incorporated in this standard.]

5.1 Critical Cyber Asset Identification

Identification and documentation of the critical cyber assets associated with the critical assets that support the reliable operation of the electric system shall be specified. At this stage of the standard, the process of identification of the critical cyber assets is left to the responsible entity and may follow as per directive of various concerned authorities (like CEA, NCIIPC, regulators etc.) as and when issued.

5.1.1 *Critical Asset Identification*

The responsible entity shall develop a list of its identified critical assets determined through an annual application of the risk assessment criteria. Utilities shall include criteria in their organizational cyber security policy document based on the applicable guidelines issued by appropriate bodies like regulators, etc. as on prevailing date. The Responsible Entity shall update this list once a year or whenever any change in the infrastructure is done, whichever is lesser.

5.1.2 *Critical Cyber Asset Identification*

From the list of critical assets, the Responsible Entity shall develop a list of associated critical cyber assets essential to the operation of the critical asset. The responsible entity shall update this list as necessary, and review it at least once every year.

For the purpose of this standard, critical cyber assets are further qualified to be those having at least one of the following characteristics:

a) The cyber asset uses a routable protocol to communicate outside the Electronic Security Perimeter
b) The cyber asset uses a routable protocol within a control centre
c) The cyber asset is Internet accessible
d) The cyber asset that has the many dependencies in the system
e) The cyber asset that stores critical sensitive data.

5.1.3 *Annual Approval*

The senior level management or delegated shall approve annually the list of critical assets and the list of critical cyber assets. The responsible entity shall keep a signed and dated record of the senior management or delegate(s)'s approval of the list of critical assets and the list of critical cyber assets (even if such lists are null).

5.2 Security Management Controls

Responsible Entities shall have minimum security management controls in place to protect critical cyber assets.

5.2.1 *Leadership*

The responsible entity shall assign a single senior level management representative with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, this standard.

a) The senior level management representative shall be identified by name, title, and date of designation.
b) Changes to the senior level management representative must be documented within thirty calendar days of the effective date.
c) The senior level management representative may delegate authority for specific actions to a named delegate or delegates. These delegations shall be documented and approved by the management.
d) The senior level management or delegate(s), shall authorize and document any exception from the requirements of the cyber security policy.

5.2.2 *Cyber Security Policy*

The responsible entity shall document and implement a cyber-security policy that represents management's commitment and ability to secure its critical cyber assets. the responsible entity shall, at minimum, ensure the following:

a) The cyber security policy addresses the requirements of this standard, including provision for emergency situations.
b) The cyber security policy is readily available to all personnel who have access to, or are responsible for, critical cyber assets.
c) The cyber security policy is reviewed and approved by the senior management assigned every year.
d) The cyber security policy shall leverage state of the art cyber security technologies and relevant processes at multiple layers to mitigate the cyber security risk.
e) The responsible entity shall incorporate procedure for identifying and reporting of sabotage in their cyber security policy.
f) The responsible entity shall document in their cyber security policy a cyber risk assessment and Mitigation Plans which shall clearly define the matrix for assessing the cyber risk of both IT and OT environment and risk acceptance criteria

5.2.3 *Exceptions*

Instances where the responsible entity cannot conform to its cyber security policy must be

documented as exceptions and authorized by the senior management or delegated executive duly identified and empowered by Head of the organisation as follows:

a) Exceptions to the responsible entity's cyber security policy must be documented within thirty days of being approved by the senior level management or delegated executive.
b) Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any related compensating measures.
c) Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior level management or delegated executive to ensure the exceptions are still required and valid. Such review and approval shall be documented.

5.2.4 *Information Protection*

The responsible entity shall implement and document a program to identify, classify, and protect information associated with critical cyber assets.

a) The critical cyber asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in **5.1**, network topology or similar diagrams, floor plans of computing centres that contain critical cyber assets, equipment layouts of critical cyber assets, disaster recovery plans / Cyber Crisis Management Plan (CCMP), incident response plans, and security configuration information.
b) The responsible entity shall classify information to be protected under this program based on the sensitivity of the critical cyber asset information.
c) The responsible entity shall, at least once every year, assess adherence to its critical cyber asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.
d) The responsible entity shall cover under this program the identification & analysis of behavioural anomaly in critical cyber assets.

5.2.5 *Access Control*

The responsible entity shall document and implement a program for managing access to protected critical cyber asset information.

a) The responsible entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
b) Personnel shall be identified by name, title, access authorization period (issue date and expiry date) and the information for which they are responsible for authorizing access.
c) The list of personnel responsible for authorizing access to protected information shall be verified every year.
d) The responsible entity shall review the access privileges to protected information to confirm that access

privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities. Review of access control shall be mandatorily done on any change in engagement of any employee / outsourced staff OR annually whichever is earlier.

e) The responsible entity shall assess and document at least annually the processes for controlling access privileges to protected information.

5.2.6 *Change Control and Configuration Management*

The responsible entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing critical cyber asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of critical cyber assets pursuant to the change control process.

The organization should develop configuration change management for systems in ICS environment, which shall include, but not limited to, following items:

a) Operating system(s) (including version) or firmware including virtualized environment.

b) Any logical network accessible ports

c) Any custom software installed

d) Any commercially available or open source application software installed.

The Responsible Entity shall authorize and document changes that deviate from the baseline configuration.

5.2.7 *Addressing Cyber Supply Chain Risk Management.*

The responsible entity shall define & implement procedures and processes to manage the cyber security risks associated with the Critical Cyber Assets / ICT products and services supply chain.

a) The responsible entity shall define & communicate its cyber security requirements to Critical ICT product suppliers and to IT services providers. The examples of Third-party IT services include data backup, cloud service provisioning, communication infrastructure support etc.

b) The responsible entity should obtain assurance that critical components and their origin can be traced throughout the supply chain.

c) The responsible entity should obtain assurance that critical cyber assets achieve required security levels, for instance, through formal certification like IS/IEC 62443-4 standards or an evaluation scheme like Common Criteria.

d) The responsible entity shall specify the measures of security performance in SLAs.

e) The responsible entity shall also specify the Confidentiality (C), Integrity (I), and Availability (A) obligation with exceptions if any in the Service Level Agreements (SLAs).

5.3 Personnel and Training

Personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, including contractors and service vendors, shall have an appropriate level of personnel risk assessment, training, and security awareness.

5.3.1 *Awareness*

The responsible entity shall establish, document, implement, and maintain a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access to critical cyber assets receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

a) Direct communications (e.g., emails, memos, computer based training in physical / online, etc.).
b) Indirect communications (e.g., posters, intranet, brochures, etc.)
c) Management support and reinforcement (e.g., presentations, meetings, etc.).
d) Table top exercises / mock drill.

5.3.2 *Training*

The responsible entity shall establish, document, implement, and maintain cyber security training program every year for personnel having authorized cyber or authorized unescorted physical access to critical cyber assets. The cyber security training program shall be reviewed every year, at a minimum, and shall be updated whenever necessary.

a) This program shall ensure that all personnel having such access to critical cyber assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.
b) Training shall cover the policies, access controls, and procedures as developed for the critical cyber assets, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
    1) Proper use of Critical Cyber Assets
    2) Physical and electronic access controls to Critical Cyber Assets
    3) Proper handling of Critical Cyber Asset information
    4) Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident
c) The responsible entity shall maintain documentation that training is conducted every year, including the date the training was completed and attendance records.

5.3.3 *Personnel Risk Assessment*

The responsible entity shall have a documented personnel risk assessment program, in accordance with central, state, municipal, local, and other applicable laws, for personnel having authorized cyber or authorized unescorted physical access to critical cyber assets. A personnel risk

assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

a) ensuring that each assessment conducted include, at least, identity verification and security verification. More detailed reviews, as permitted by law, may be conducted depending upon the criticality of the position.
b) updating each personnel risk assessment at least every three years after the initial personnel risk assessment or for cause.
c) documenting the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to critical cyber assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to this standard.

5.3.4 *Access*

The responsible entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets as follows:

a) The responsible entity shall review the list(s) of its personnel who have such access to critical cyber assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to critical cyber assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
b) The responsible entity shall revoke such access to critical cyber assets within four hours for personnel terminated for cause and within 24 hours for personnel who no longer require such access to critical cyber assets.

5.4 Electronic Security Perimeter

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. Responsible entity should continue to follow existing and future standards for data and communications security such as IEC 62351 series of standards.

5.4.1 *Access points for Electronic Security Perimeter*

The responsible entity shall ensure that every critical cyber asset resides within an electronic security perimeter. The responsible entity shall identify and document the electronic security perimeter(s) and all access points to the perimeter(s).

a) Access points to the electronic security perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the electronic security perimeter(s). Identified access point shall also include all assets being connected

temporarily / time to time basis through remote connectivity (such as VPN) and access the network resources.

b) For a dial-up accessible critical cyber asset that uses a non-routable protocol, the Responsible Entity shall define an electronic security perimeter for that single access point at the dial-up device.

c) Communication links connecting discrete electronic security perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the electronic security perimeter(s) shall be considered access points to the electronic security perimeter(s).

d) Any non-critical cyber asset within a defined electronic security perimeter shall be identified and protected pursuant to the requirements of this standard.

e) Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in this standard.

f) Maintain documentation of electronic security perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

g) Ensure that all documentation required by this Standard reflect current configurations and processes and shall review the documents and procedures referenced in this Standard at least once a year.

h) Update the documentation to reflect the modification of the network or controls as per change management policy.

5.4.2 *Electronic Access Controls*

The responsible entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the electronic security perimeter(s).

a) These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

b) at all access points to the electronic security perimeter(s), the responsible entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

c) Implement and maintain a procedure for securing dial-up access to the electronic security perimeter(s).

d) Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls including multi-

factor authentication at the access points to ensure authenticity of the accessing party, where technically feasible.

e) The required documentation shall, at least, identify and describe:
   1) the processes for access request and authorization.
   2) the authentication methods.
   3) the review process for authorization rights and role-based matrix.
   4) the controls used to secure dial-up accessible connections and remote connectivity through VPN.
   5) procedure for connectivity with cloud service providers.

f) Where technically feasible, and in order to make personnel accessing the system aware of the criticality of the cyber asset, electronic access control devices shall display an appropriate banner on the user screen upon all interactive access attempts. The responsible entity shall maintain a document identifying the content of the banner.

5.4.3 *Monitoring Electronic Access*

The responsible entity shall implement and document an electronic or manual process for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

a) For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process at each access point to the dial-up device, where technically feasible.

b) Where technically feasible, the security monitoring process shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every three months.

c) Retain electronic access logs for at least one year. Logs related to reportable incidents shall be kept in accordance with the requirements of **5.7**.

5.4.4 *Cyber Vulnerability Assessment*

The Responsible Entity shall perform a cyber-vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least once a year. The vulnerability assessment shall include, at a minimum, the following:

a) A document identifying the vulnerability assessment process. If a vulnerability is accepted for maintaining business operational requirements, then same shall be documented.

b) A review to verify that only ports and services required for operations at these access points are enabled

c) Discovery of all access points to the Electronic Security Perimeter

d) Review of controls for default accounts, passwords, and network management community strings
e) Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan

5.5 Physical Security of Critical Cyber Assets

This section is intended to ensure the implementation of a physical security program for the protection of critical cyber assets.

5.5.1 *Physical Security Plan*

The responsible entity shall document, implement, and maintain a physical security plan, approved by the senior management or delegate(s) that shall address, at a minimum, the following:

a) All cyber assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
b) Identification of all physical access points through each Physical Security Perimeter and measures to control entry at those access points.
c) Processes, tools, and procedures to monitor physical access to the perimeter(s).
d) Appropriate use of physical access controls including visitor pass management, CCTV Surveillance, response to loss, and prohibition of inappropriate use of physical access controls.
e) Review of access authorization requests and revocation of access authorization.
f) A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
    1) Check and authorization of all devices in possession of the visitors.
    2) Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters, official authorizing the visit, purpose of visit, and any other relevant information.
    3) Device sanitization such as scanning with anti-virus/anti-malware etc. of all equipment and tools or devices prior to connection with the cyber assets.
    4) Continuous escorted access of visitors within the Physical Security Perimeter.
g) Update of the physical security plan within one month of the completion of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the Physical Security Perimeter,

physical access controls, monitoring controls, or logging controls.

h) Annual review of the physical security plan.

j) Physical security training and drills.

5.5.2 *Protection of Physical Access Control Systems*

Cyber assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall be:

a) Protected from unauthorized physical access.

b) Afforded the protective measures specified in this standard (*Clauses* **5.5.3** *to* **5.5.7**).

5.5.3 *Protection of Electronic Access Control Systems*

Cyber assets used in the access control and/or monitoring of the electronic security perimeter(s) shall reside within an identified physical security perimeter.

5.5.4 *Physical Access Controls*

The responsible entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:

a) Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

b) Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.

c) Security Personnel: Personnel responsible for controlling physical access who may reside / positioned on-site or at a monitoring station.

d) Other Authentication Devices: Biometric, Facial recognition, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

e) Dual authentication: - Like biometric along with card key.

5.5.5 *Monitoring Physical Access*

The responsible entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the physical security perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in **5.7**. One or more of the following monitoring methods shall be used:

a) Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

b) Human Observation of Access Points: Monitoring of physical access points by authorized personnel.

5.5.6 *Logging Physical Access*

Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall retain physical access logs for at least one year. Logs related to reportable incidents shall be kept in accordance with the requirements of **5.7**.

The responsible entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the physical security perimeter(s) using one or more of the following logging methods or their equivalent:

a) Computerized Logging: Electronic logs produced by the responsible entity's selected access control and monitoring method.
b) Video Recording: Electronic capture of video images of sufficient quality to determine identity.
c) Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access.

5.5.7 *Maintenance and Testing*

The responsible entity shall implement appropriate maintenance and testing program to ensure that all physical security systems function properly. The program must include, at a minimum, the following:

a) Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
b) Retention of testing and maintenance records for the cycle determined by the Responsible Entity.
c) Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

5.6 Systems Security Management

Responsible entities shall 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).

The responsible entity shall review and update the documentation at least once a year. Changes resulting from modifications to the systems or controls shall be documented within one month of the change being completed.

5.6.1 *Test Procedures*

The responsible entity shall ensure that new cyber assets and significant changes to existing cyber assets within the electronic security perimeter do not adversely affect existing cyber security controls. For purposes of this Standard, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware and:

a) Create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

b) Document that testing is performed in a manner that reflects the production environment.
c) Document test results as well as reports/certificate of cyber test carried out for compliance of government orders and cyber security audits.
d) The responsible entity shall ensure that all Communicable devices are tested for communication protocol as per the ISO/IEC/IS standards.

5.6.2 *Ports and Services*

The responsible entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

a) Enable only those ports and services required for normal and emergency operations.
b) Disable other ports and services, including those used for testing purposes, prior to production use of all cyber assets inside the electronic security perimeter(s).
c) In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

5.6.3 *Security Patch Management*

The responsible entity shall establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all cyber assets within the electronic security perimeter(s).

a) Document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
b) Document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.
c) Document the rollback process after the unaccepted behaviour of the system due to patch management.
d) Responsible entity must use patches from legitimate sources.
e) Responsible entity must follow the patch management in accordance to its change management policy.

5.6.4 *Malicious Software Prevention*

The responsible entity shall use anti-virus software and other malicious software (“malware”) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all cyber assets within the electronic security perimeter(s).

a) Document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the responsible entity shall document compensating measure(s) applied to mitigate risk exposure.
b) Document and implement a process for the update of anti-virus and

malware prevention "signatures." The process must address testing and installing the signatures.

5.6.5 *Account Management*

The responsible entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

a) Ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
    1) Ensure that user accounts are implemented as approved by designated personnel.
    2) Establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of three months.
    3) Review, at least once a quarter, user accounts to verify access privileges are in accordance with this standard.
b) Implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
    1) The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
    2) The responsible entity shall identify those individuals with access to shared accounts.
    3) Where such accounts must be shared, the responsible entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
c) At a minimum, require and use passwords and implement, as technically feasible, policies for making the password hard to crack (such as periodic password changes, requiring combination of alphanumeric and special characters.

5.6.6 *Security Status Monitoring*

The responsible entity shall ensure that all cyber assets within the electronic security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security as follows:

a) Implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on

all Cyber Assets within the Electronic Security Perimeter.

b) The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
c) Maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in **5.7**.
d) Retain all logs for minimum six months.
e) Review logs of system events related to cyber security and maintain records documenting review of logs.

5.6.7 *Disposal or Redeployment*

The Responsible Entity shall establish and implement formal methods, processes, and procedures for disposal or redeployment of identified cyber assets within the electronic security perimeter(s).

a) Prior to the disposal or redeployment of such assets:
    1) Destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
    2) At a minimum, erase the data storage media to prevent unauthorized retrieval (in case of redeployment) of sensitive cyber security or reliability data.
b) Maintain records that such assets were disposed of or redeployed in accordance with documented procedures

5.7 Incident Reporting and Response Planning

This Section ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

5.7.1 *Security Incident Response Team*

A security incident is an event which results (or may result) in misuse, damage, denial of service, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

The responsible entity shall create a security incident response team. The members of this team can either be full-time or can have this responsibility as an additional responsibility along with their current role. At least one member of the Incident Response Team shall be reachable at all times.

All Security Incidents reported to the Team should be recorded.

5.7.2 *Cyber Security Incident Response Plan*

The responsible entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:

a) Procedures to characterize and classify events as reportable Cyber Security Incidents.
b) Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber

Security Incident handling procedures, and communication plans.

c) The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the appropriate local and central authorities.
d) Process for updating the Cyber Security Incident response plan within one month of any changes.
e) Process for ensuring that the Cyber Security Incident response plan is reviewed at least once a year.
f) Process for ensuring the Cyber Security Incident response plan is tested at least once a year. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.
g) Root cause analysis for all reportable events shall be carried out by the Responsible Entity.
h) The Responsible Entity shall mandatorily define in their Cyber Security Policy, criteria(s) identified on the basis of impact analysis, for declaring the occurrence of Cyber Security Incident(s) as a Cyber Crisis in the System owned or controlled by them.
j) The responsible entity shall maintain all cyber logs and cyber forensic of any incident as per guidelines issued by NCIIPC, CERT-In, CEA and any other government agencies / compliance enforcement bodies from time to time.

5.7.3 *Cyber Security Incident Documentation*

The responsible entity shall keep relevant documentation related to all reportable cyber security incidents for a minimum period of five years.

5.8 Recovery Plans for Critical Cyber Assets

This section 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.

5.8.1 *Recovery Plans*

The responsible entity shall create and conduct a review of recovery plan(s) for critical cyber assets at least once a year. The recovery plan(s) shall address at a minimum the following:

a) Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
b) Define the roles and responsibilities of responders.

5.8.2 *Exercises*

The recovery plan(s) shall be exercised at least once a year. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident.

5.8.3 *Change Control*

Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and

implementation of the recovery plan(s) within one month of the change being completed.

5.8.4 *Backup and Restore*

The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore critical cyber assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc. Information essential to recovery that is stored on backup media shall be tested at least once a year to ensure that the information is available. Testing can be completed off-site The responsible entity shall define the Recovery Time Objective (RTO) / Recovery Point Objective (RPO) parameters for recovery of data from its' DR site as per the ISO 22301 standard .

6 COMPLIANCE

6.1 Compliance Enforcement Authority

The designated authority as determined by appropriate body will act as a Compliance Enforcement Authority.

6.2 Auditing Requirements

The responsible entity can perform self-audits as mandated by this Standard and keep the necessary records as per **6.3.** In addition, Compliance Enforcement Authority should certify select agencies for compliance auditing. The responsible entity can utilize the services of these certified agencies for performing external audits.

The enforcement authority should audit the documents and records on at least bi-annual basis to ensure that the Responsible Entities are in compliance with this Standard. This audit should include on-site random checks to ensure compliance.

6.3 Records and Documents

The responsible entity shall keep all documentation required as part of this standard for a minimum period of 3 years. Documentation and data shall be retained for a longer time if required as part of any investigation.

This section summarizes the list of records and documents that Responsible Entity should maintain as per the various requirements in **5**. In case there is a difference of interpretation between this section and the corresponding Section **5**, the requirements given in Section **5** shall prevail:

i. List of Critical Assets as per along with the criteria for identification (*see* **5.1.1**).
ii. List of Critical Cyber Assets (*see* **5.1.2**).
iii. Approval Record (*see* **5.1.3**).
iv. Assignment of senior management representative and changes thereof, if any (*see* **5.2.1**).
v. Approved Cyber security policy including Cyber Risk Assessment and Mitigation Plan & Documented procedure for identifying and reporting of sabotage (*see* **5.2.2**).
vi. Approved Exception list (*see* **5.2.3**).
vii. Documented Information Protection program (*see* **5.2.4**).
viii. Documented Access Control program (*see* **5.2.5**).

ix. Change control and configuration management documentation including Baseline Document (*see* **5.2.6**).

x. Documented procedure & processes related to Cyber Supply Chain Risk Management (*see* **5.2.7**).

xi. Documentation of security awareness and reinforcement program (*see* **5.3.1**).

xii. Cyber security training program, review records, and training records (*see* **5.3.2**).

xiii. Personnel Risk Assessment program and records (*see* **5.3.3**).

xiv. List of personnel with access rights and associated review and revocation records, if any (*see* **5.3.4**).

xv. Electronic Security Perimeter, list of all Cyber Assets within the perimeter, and the cyber assets deployed for access control (*see* **5.4.1**).

xvi. Documentation of the electronic access controls to the Electronic Security Perimeter(s) (*see* **5.4.2**).

xvii. Documented monitoring and logging at access points to the Electronic Security Perimeter(s) (*see* **5.4.3**).

xviii. Vulnerability Assessment documentation and associated mitigation, if any (*see* **5.4.4**).

xix. Documented Physical Security Perimeter, Approved Physical Security Plan and associated implementation records (*see* **5.5.1**).

xx. Documented protection of physical perimeter(s) (*see* **5.5.2**).

xxi. Documentation certifying that electronic access controls for protection of Electronic Security Perimeter are within Physical Security Perimeter (*see* **5.5.3**).

xxii. Methods for controlling physical access to each access point of a Physical Security Perimeter (*see* **5.5.4**).

xxiii. Methods for monitoring physical access (*see* **5.5.5**).

xxiv. Methods for logging physical access and access logs for access to Physical Security Perimeter(s) (*see* **5.5.6**).

xxv. Implementation of physical security system maintenance and testing program (*see* **5.5.7**).

xxvi. Documentation of security test procedures (*see* **5.6.1**).

xxvii. Documentation to confirm only essential ports and services are open, and documented exceptions and mitigation (*see* **5.6.2**).

xxviii. Documentation and records of security patch management program (*see* **5.6.3**).

xxix. Documentation and records of malicious software prevention program (*see* **5.6.4**).

xxx. Documentation and records of account management program (*see* **5.6.5**).

xxxi. Documentation and records of security status monitoring program (*see* **5.6.6**).

xxxii. Documentation and records of program for the disposal or redeployment of Cyber Assets (*see* **5.6.7**).

xxxiii. Composition of the Security Incident Response Team and list of incidents reported to the Team (*see* **5.7.1**).

xxxiv. Approved Cyber Security Incident Response plan / CCMP, its review and all follow-up of incidents as required by law (*see* **5.7.2**).

xxxv. Documentation of all reportable cyber security incidents (*see* **5.7.3**).

xxxvi. Approved recovery plan (*see* **5.8.1**).

xxxvii. Documentation of exercise of recovery plan(s) (*see* **5.8.2**).

xxxviii. Documentation of changes to the recovery plan(s), and documentation of all associated communications (*see* **5.8.3**).

xxxix. Documentation regarding information backup, periodic testing of the backup, and storage of the backup (*see* **5.8.4**).

6.4 Testing and Conformance

The devices and systems deployed in field and control centre shall be trustworthy for its security requirements apart from security management systems processes adopted by the end users.

The objective of this clause is to describe the tests and conformance assessments to ensure the devices and systems will be secure as per the relevant product standards or user‘s technical specifications. Test requirements shall cover all the aspects of security specifications both functional and design requirements. Tests shall be conducted by user and supplier at various stages and wherever essential from a third party agency or accredited laboratory. Test results and all deviations from the test plans shall be required to be documented.

6.4.1 *Life cycles of security tests*

The testing process requires that various process functions of the devices, and equipment, and systems be tested or verified during the one or more stages in the production and installation cycle of the system. The testing process is classified in into three groups based on the security lifecycles of automation controls systems as detailed in the following sections.

6.4.1.1 *Devices and Systems*

This includes testing for the security compliance as per the respective product standards under laboratory conditions. This process is grouped in to three levels viz. functional security assessment, software development security assessment and the communication robustness testing. The communication robustness testing shall cover basic port testing and protocol specific testing. These tests shall be part of product certified design tests, factory test before the customer approval for shipment and field test during the installation and commissioning stage.

6.4.1.2 *Supplier Practices*

This is part of certified design test and these tests are performed by the supplier on specimens of generic type of production model equipment to establish the security conformance with its design standard.

Developmental security testing occurs at all post design phases of the system development life cycle. Information systems include information technology products (i.e. Hardware, software, and firmware components) that compose those systems. Information system developer is a general

term that includes developers or manufacturers of information technology products (including hardware, software, and firmware), systems integrators, vendors, and product resellers. Developer testing confirms that: the required security controls are implemented correctly and operating as intended; and the information system meets the established security requirements. Security test and evaluation plans provide the specific activities that developers plan to carry out including the types of analyses, testing, and reviews of software and firmware components, the degree of rigor to be applied in the analyses, tests, and reviews, and the types of artefacts produced during those processes. Contracts specify the acceptance criteria for security test and evaluation plans, flaw remediation processes, and evidence that plans and processes have been diligently applied. This control also applies to organizations conducting internal systems development and integration.

6.4.1.3 *Integrated system Deployment*

This stage involves during the commissioning, site acceptance test and the periodically testing for the implemented architecture. This includes not only making sure the deployment blocks attack, but also ensuring that the operation of the process is not negatively affected by the security deployment. The final stage is to manage the system on an on-going basis. Typical control networks will have multiple communication paths over many locations in the system. Ideally, the multiple systems security appliances should be managed from a single management console application.

As part of continuous life cycle management of the system, the organization employs an independent penetration agent or penetration team to conduct a vulnerability analysis on the OT system and IT system; and perform penetration testing on the IT system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities. Generally, penetration testing is not advisable on live OT systems.

ANNEX A
(Clause 2)

LIST OF REFERRED INDIAN STANDARDS

IS No.	Title
IS/IEC 62351 series	Power systems management and associated information exchange – Data and Communications security
IS/IEC 62443 series	Security for Industrial Automation and Control Systems

ANNEX B
(Clause 2)

LIST OF REFERRED INTERNATIONAL STANDARDS

ISO 22301 Security and resilience — Business continuity management systems — Requirements

BIBLIOGRAPHY

A-1 North American Electric Reliability Council (NERC) Critical Infrastructure Protection Standard:

CIP 002 - Cyber Security — BES Cyber System Categorization.
CIP 003 - Cyber Security — Security Management Controls.
CIP 004 - Cyber Security — Personnel and Training.
CIP 005 - Cyber Security — Electronic Security Perimeter(s).
CIP 006 - Cyber Security — Physical Security of BES Cyber Systems.
CIP 007 - Cyber Security — System Security Management.
CIP 008 - Cyber Security — Incident Reporting and Response Planning.
CIP 009 - Cyber Security — Recovery Plans for BES Cyber Systems.
CIP 010 - Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP 011 - Cyber Security — Information Protection
CIP 012 - Cyber Security – Communications between Control Centers.
CIP 013 - Cyber Security - Supply Chain Risk Management
CIP 014 - Physical Security

A- 1.1 RFC 2828 Internet Security Glossary.

A-1.2 NIST IR 7628 Guidelines for Smart Grid Cyber security.

A- 1.3 NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations.

A- 1.4 NIST SP 800-82 Guide to Operational Technology (OT) Security.

A- 1.5 NIST Special Publication 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

LITD 10/PANEL – 2 Security Panel Composition

Organization	*Representative(s)*
Central Power Research Institute, Bengaluru	SHRI V. SHIVAKUMAR (*Convenor*)
Hitachi Energy, Bengaluru	SHRI S R VIJAYAN
Central Electricity Authority, New Delhi	SHRI M A K P SINGH
Central Power Research Institute, Bengaluru	SHRI M. PRADISH
Centre for Development of Advanced Computing, Pune	SHRI B. S. BINDHUMADHAVA SHRI R. K. SENTHIL KUMAR (*Alternate*)
Ernst and Young LLP, Gurugram	SHRI HEM THUKRAL
GE Energy Management System, New Delhi	MS PREETIKA DOGRA MS VAIBHAVI KALE (*Alternate*)
IEEE India, Bengaluru	SHRI RAVINDRA DESAI
India Smart Grid Forum, New Delhi	SHRI REJI KUMAR PILLAI
Indian Electrical and Electronics Manufacturers Association, New Delhi	SHRI AKEEL KHAN
Kamani Engineering Corporation, Mumabi	DR TUSHAR TEREDESAI
Karnataka Power Transmission Corporation Limited, Bengaluru	SHRI S. B. CHANDRASHEKARAIAH
Narnix Technolabs Private Limited, New Delhi	SHRI NARANG N KISHORE
Power Grid Corporation of India, Gurugram	SHRI ANAND SHANKAR SHRI D MURALIKRISHNA *(Alternate)*
Schneider Electric India Private Limited, Gurugram	SHRI MAYANK SHARMA
Siemens Limited, Mumbai	SHRI VIKRAM GANDOTRA SHRI ROHIT SHARMA *(Alternate)*

Tata Power Delhi Distribution Limited, New Delhi SHRI ANIL KUMAR OJHA

COMMITTEE COMPOSITION

LITD 10 Power System Control and Associated Communication Sectional Committee

Organization	*Representative(s)*
Central Electricity Authority, New Delhi (New Delhi)	SHRI ASHOK KUMAR RAJPUT (*Chairperson*)
Hitachi Energy, Bengaluru	SHRI S. R. VIJAYAN
Bhakra Beas Management Board, Chandigarh	SHRI NAVEEN GUPTA
CSIR - National Physical Laboratory, New Delhi	DR SAOOD AHMAD DR AVNI KHATKAR
Central Electricity Authority, New Delhi	SHRI L.K.S. RATHORE MS PRIYAM SRIVASTAVA *(Alternate I)* SHRI R. P. PRADHAN *(Alternate II)*
Central Power Research Institute, Bengaluru	DR AMIT JAIN SHRI V. SHIVAKUMAR *(Alternate I)* SHRI M. PRADISH *(Alternate II)*
Grid India, New Delhi	SHRI K MURALIKRISHNA SHRI PRAMOD KUMAR *(Alternate)*
IEEE India, Bengaluru	SHRI RAVINDRA DESAI
India Smart Grid Forum, New Delhi	SHRI REJI KUMAR PILLAI SHRI ANAND SINGH *(Alternate)*
Indian Electrical and Electronics Manufacturers Association, New Delhi	SHRI UTTAM KUMAR SHRI VIVEK ARORA *(Alternate)*
Indian Institute of Technology, Hyderabad	DR PRADEEP KUMAR YEMULA
Karnataka Power Transmission Corporation Limited, Bengaluru	SHRI S. B. CHANDRASHEKARAIAH SHRI MADHU B P*(Alternate I)* SHRI MATI LAKSHMI M S *(Alternate II)*

Kalki Communication Technologies Private Limited, Bengaluru	SHRI JOSE THOMAS SHRI VINOO S WARRIER *(Alternate)*
Narnix Technolabs Private Limited, New Delhi	SHRI NARANG N KISHORE
Power Grid Corporation of India, Gurugram	SHRI A. K. MISHRA SHRI ANAND SHANKAR *(Alternate I)* DR SUNITA CHOHAN *(Alternate II)*
Scope T & M Private Limited, Mumbai	SHRI VIVEKANAND SINDKAR SHRI KUNAL JAGPAT *(Alternate)*
Secure Meters Limited, Gurugram	SHRI RAJNISH AMETA SHRI ANIL MEHTA *(Alternate I)* SHRI MADHUR KUMAR SRIVASTAVA *(Alternate II)*
In Personal Capacity	SHRI N. S. SODHA MS BINDOO SRIVASTAVA SHRI P. K. AGARWAL
BIS Director General	SMT REENA GARG, SCIENTIST 'G'/SENIOR DIRECTOR AND HEAD (ELECTRONICS AND INFORMATION TECHNOLOGY) [REPRESENTING DIRECTOR GENERAL (Ex-officio)]

Member Secretary
MS ALISMITA KHAG
SCIENTIST 'C'/DEPUTY DIRECTOR
(ELECRTONICS AND INFORMATION TECHNOLOGY), BIS