INDIAN REGISTER OF SHIPPING

CLASSIFICATION NOTES

Type Approval of Cyber Secured Control System Components

Revision 1
March 2024

IRCLASS
Indian Register of Shipping

CLASSIFICATION NOTES

Type Approval of Cyber Secured Control System Components

Revision 1, March 2024

TABLE 1 – AMENDMENTS INCORPORATED IN THIS EDITION

These amendments are applicable to components whose application for certification is received on or after 1 July 2024

Clause	Subject/ Amendments
Section 1: Introduction	
1.4	IEC 62443-3-3 is added to the list of references.
Section 2: Documentation for Type Approval	
2.1.1.2	The hardware and software details to be included in the asset inventory for Computer-Based Systems (CBS) are listed.
2.1.1.6	Installation and Operation Manual is added to the list of required documents.
Section 3: Approval Philosophy	
Table 3.2.1	Security Level (SL-E) is introduced.
3.2.3	Reference to the applicable requirements for Security Level (SL-E) is provided.
Section 4: Design Assessment and Document Review	
4.3.3	Performance test protocol for SL-E security level is specified.
Table 4.3.3.1 (new)	Security capabilities required for all CBSs are specified.
Table 4.3.3.2 (new)	Additional security capabilities required for CBSs with network communication are specified.

CLASSIFICATION NOTES

Type Approval of Cyber Secured Control System Components

Revision 1, March 2024

Contents

Section

Section 1
Introduction

1.1 Application

1.1.1 The requirements in this Classification Note are applicable to Type Approval of cyber secured control system components, used in ships and/ or offshore structures classed or intended to be classed with IRS.

1.1.2 This Classification Note indicates the security requirements for cyber components used in control systems. The requirements are based on IEC 62443 Series and are in addition to those specified in Classification Note: *Type Approval of Electrical Equipment used for Control, Monitoring, Alarm and Protections Systems for use in Ships* and are to be applied when specifically requested by the manufacturer for a particular security level defined in Section 3.2.

1.2 Nomenclature

IEC – International Electro technical Commission

ISA - International Society for automation

1.3 Definitions

1.3.1 Control system components can be any one of the following

- **Authentication**: Provision of assurance that a claimed characteristic of an identity is correct
- **Device:** An asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset.
- **PLC:** A programmable logic controller (PLC), or programmable controller is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes.
- **Router**: A router is hardware device designed to receive, analyze and move incoming packets to another network.
- **Network Switch**: A network switch is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device.
- **Network device:** Device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process. Eg. firewalls, routers, switches
- **Firewall:** A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- **Gateway:** A network infrastructure device used for connecting secure/controlled network to insecure/uncontrolled networks, e.g. a router including firewall (including wireless gateway).
- **Node:-** An end-device connected to the secure/controlled network
- **Embedded Device:** Special purpose device running embedded software designed to directly monitor, control or actuate an industrial process.

- **Host device:** General purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers Eg: Operator stations, engineering stations etc.

- **Software application:** One or more software programs and their dependencies that are used to interface with the process or the control system itself. Eg. Configuration Software.

- **Industrial automation and control system (IACS):** Collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

- **Mobile code:** Program transferred between a remote, possibly a “untrusted” system across a network via removable media that can be executed unchanged on a local system without explicit installation or execution by the recipient

- **Non-repudiation:** Ability to prove the occurrence of a claimed event or action and its originating entities

- **Security level:** Measure of confidence that the application or device is free from vulnerabilities and functions in the intended manner

1.4 References

- **IEC 60945 -** Maritime navigation and radio communication equipment and systems – General requirements – Methods of testing and required test results

- **UR E10**

- **IEC 62443 Series**

- **ISA 62443-4-2**: Security for industrial automation and control systems -Technical security requirements for IACS components

- IEC 62443-3-3 - Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

- **IRS Classification Note -** *Type Approval of Electrical Equipment used for Control, Monitoring, Alarm and Protections Systems for use in Ships*

Section 2

Documentation for Type Approval

2.1 Documentation

2.1.1 The following documents, drawings and details, as relevant and applicable, are required to be submitted to IRS for review by the manufacturer:

2.1.1.1 Schematic diagram/ documents of the component showing the following details:

(a) Block diagram showing interconnection between various units;
(b) User interface of and user input devices;
(c) Description of power supply;
(d) Software details (e.g. version of software);
(e) Hardware details;
(f) Inbuilt fault detection provision.

2.1.1.2 The asset inventory for computer-based systems (CBS) is to include the following information:

- List of hardware components (e.g. host devices, embedded devices, network devices) Name
- Brand/manufacturer
- Model/ type
- Short description of functionality/purpose
- Physical interfaces (e.g., network, serial)
- Name/type of system software (e.g., operating system, firmware)
- Version and patch level of system software
- Supported communication protocols

List of software components (e.g., application software, utility software)
- The hardware component where it is installed
- Brand/manufacturer
- Model/type
- Short description of functionality/purpose
- Version of software

2.1.1.3 Proposed type test program and test reports;

2.1.1.4 Performance test protocol

2.1.1.5 Details of main production facilities

2.1.1.6 Documents related to quality control including:

(a) Organizational structure related to quality control;
(b) Document control;
(c) In-house test and inspection procedures;
(d) Production quality assurance system;
(e) Valid ISO certificate from an accredited body or evidence of quality system for design, manufacturing and testing of cyber secured control system components
(f) Installation and Operation manuals

Section 3

Approval Philosophy

3.1 Foundational Requirements (FR)

3.1.1 The following are the seven foundational requirements against which the systems would be evaluated.

a) FR1 Identification and authentication control (IAC),
b) FR2 Use control (UC),
c) FR3 System integrity (SI),
d) FR4 Data confidentiality (DC),
e) FR5 Restricted data flow (RDF),
f) FR 6 Timely response to events (TRE),
g) FR 7 Resource availability (RA).

3.2 Component requirements (CR) and Security levels (SL)

3.2.1 The seven foundational requirements may be further expanded into a series of component requirements (CR). Each CR has a baseline requirement and zero or more requirement enhancements (REs) to strengthen security. The baseline requirement and REs, if present, are then mapped to the control system capability security level, the requirements specify four security levels in line with IEC 62443-3-3.

The individual CR and associated RE assignments are thus based on an incremental increase in overall component security for that particular FR. The system integrator/ designer has to choose the specific security level for the control system component depending on the defense in depth and network segmentation contemplated for the particular device.

Security levels (SL) are defined below in Table 3.2.1:

Table 3.2.1 : Security Levels (SL)

SL-E	Systems and equipment for computer-based systems complying with the requirements as specified in Part 4, Chapter 7, Section 8 of the *Rules and Regulations for the Construction and Classification of Steel Ships* (hereinafter referred to as, the Rules).
SL 1	Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
SL 2	Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation
SL 3	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, control system specific skills and moderate motivation.
SL 4	Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, control system specific skills and high motivation.

3.2.2 A manufacturer intending to get the control system equipment or system type approved as cyber secured component is to meet following requirements:

a) Hardware is to comply with applicable requirements of environmental standards in accordance with Classification Note: *Type Approval of Electrical Equipment used for Control, Monitoring, Alarm and Protections Systems for use in Ships*

b) The system is to comply with functional requirements specific for various security levels as per IEC 62443.

3.2.3 Systems and equipment for computer-based systems complying with requirements as specified in Part 4, Chapter 7, Section 8 of the Rules will be certified for Security Level SL-E.

3.3 Types of Control system components

This Classification Note provides component requirements for four types of components:

a) Software Application

b) Embedded Device

c) Host Device

d) Network Device

Specific requirements applicable for each of the above components are indicated at Cl. 4.3.2.8 to 4.3.2.11 of this Classification Note.

Section 4

Design Assessment & Document review

4.1 Design assessment

4.1.1 The design assessment is to ensure that the design of the product conforms to the requirements as specified in the reference standards indicated in Section 1.4. The assessment will comprise of review of documents indicated in Section 2.

4.2 Quality system

4.2.1 Manufacture quality plan and documentation of procedures which are required in the complete manufacturing and assembly process is to be reviewed

4.3 Test protocols

4.3.1 The equipment has to undergo following tests

a) Type tests
b) Performance /functional tests

4.3.2 Test protocol specifying the relevant IEC clauses (as appropriate) and the test methodology are to be submitted to IRS, for approval, prior to conducting the tests.

4.3.1 Type tests program

4.3.1.1 The environmental tests are to be carried out in accordance with Table 4.3.1.

Table 4.3.1 : Environmental Tests

SN	Environmental Test	Ref. Specifications/ IRS Class. Note[1]	Comment
01	High voltage	Sec 3/ Annex 1/ Test No. 10	
02	Dry heat	IEC 60068-2-2	
03	Damp heat	IEC 60068-2-30 test Db	
04	Vibration	IEC 60068-2-6 Test Fc	
05	Salt mist	IEC 60068-2-52 Test Kb	
06	Cold	IEC 60068-2-1	
07	Electromagnetic field	IEC 61000-4-3	
08	Flame retardant	IEC 60092-101 OR IEC 60695-11-5	
09	Conducted Emission	Sec 3/ Annex 1/ Test No. 20	
10	Radiated emission	Sec 3/ Annex 1/ Test No. 19	
11	Electrical Fast Transients / Burst	IEC 61000-4-4	
12	Surge	IEC 61000-4-5	

13	Inclination	IEC 60092-504	
14	External power supply failure	Sec 3/ Annex 1/ Test No. 3	
15	Immunity to electrostatic discharge	IEC 61000-4-2	
16	Insulation resistance	Sec 3/ Annex 1/ Test No. 9	
[1]*Type Approval of Electrical Equipment used for Control, Monitoring, Alarm and Protection, Systems for Use in Ships, Section 3, Annexure 1.*			

Note: The above tests are to be carried out in either of the following:

a. NABL accredited laboratory if tested in India
b. In manufacturer's in-house test facility if the same is approved either by NABL or by Government of India, if tested in India.
c. In a lab or in-house test facility accredited as per ISO/IEC 17025 standard, if tested outside India.

4.3.1.2 The report of the above tests will be reviewed for compliance with relevant standards.

4.3.2 Performance test protocol for SL-1, SL-2, SL-3 and SL-4

4.3.2.1 Performance test protocol and desired results are to be reviewed against IEC 62443-4-2. The seven FRs, associated CRs and requirement enhancement for different security levels are to be defined in the performance test protocol, as applicable.

4.3.2.2 FR1 Identification and authentication control

The purpose of this functional requirement is to identify and authenticate all users, software process and devices before allowing them to access the assets or systems. The goal of the control is to protect device system from unauthorized users, software and devices. The FR1 is further subdivided (14 sub levels) and mapped against CR and SL as shown below:

FR1.1 Human user identification and authentication

Reference clause and description of requirement
CR.1.1:- Capability to identify and authenticate all human users. Common user identification and authentication may be accepted.
CR.1.1(1):- Unique identification and authentication for individual human users
CR.1.1(2):- Multifactor authentication for individual human users.

Security Levels	Applicable clauses for Security Levels
SL-1	CR.1.1
SL-2	CR 1.1 (1)
SL-3, SL-4	CR 1.1 (1) (2)

FR1.2 Software process and device identification and authentication

Reference clause and description of requirement
CR 1.2 :- Capability to identify itself and authenticate with any other components
CR 1.2 (1) :- Unique identification and authentication with other components

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	CR 1.2
SL-3,SL-4	CR 1.2 (1)

FR1.3 Account management

Reference clause and description of requirement
CR 1.3:- Capability to integrate into a system that supports the management of all devices connected in system.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 1.3

FR1.4 Identifier management

Reference clause and description of requirement
CR 1.4:- Capability to integrate into a system that supports the management of identifiers.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2 SL-3, SL-4	CR 1.4

FR1.5 Authenticator management

Reference clause and description of requirement
CR 1.5:- Capability to support the use of initial authenticator content, support changes to default authenticators and protect unauthorized disclosure and modification when stored, used and transmitted.
CR 1.5 (1):- Authentication using hardware mechanisms.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2	CR 1.5
SL-3, SL-4	CR 1.5 (1)

FR1.6 Wireless access management

Reference clause and description of requirement
The wireless access management requirements are network component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12

FR1.7 Strength of password-based authentication

Reference clause and description of requirement
CR 1.7:- Capability to enforce configurable password strength.
CR 1.7(1):- Restrictions on use of old password. Enforce password minimum and maximum lifetime restrictions for human users
CR 1.7(2):- Password minimum and maximum lifetime restrictions for all users

Security Levels	Applicable clauses for Security Levels
SL-1,SL-2	CR 1.7
SL-3	CR 1.7 (1)
SL-4	CR 1.7 (1) (2)

FR1.8 Public key infrastructure certificates.

Reference clause and description of requirement
CR 1.8:- Component shall have the capability to operate within the scope of the PKI

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	CR 1.8

FR1.9 Strength of public key authentication.

Reference clause and description of requirement
CR 1.9:- Capability to validate certificates a) By checking the validity of the signature and certificate b) By constructing a certification path to an accepted certification authority c) Establish user (human, software process or device) control of the corresponding private key, through authentication
CR 1.9(1):- ISO/IEC 19790 Level 3 security for public key authentication
CR 1.9(2):- ISO/IEC 19790 Level 4 security for public key authentication

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	CR 1.9
SL-3	CR 1.9 (1)
SL-4	CR 1.9 (1) (2)

FR1.10 Authenticator feedback

Reference clause and description of requirement
CR 1.10:- Capability to obscure feedback of authentication information during the authentication process.

Security Levels	Applicable clauses for Security Levels
SL-1,SL-2, SL-3, SL-4	CR 1.10

FR 1.11 Unsuccessful login attempts

Reference clause and description of requirement
CR 1.11:- Capability to limit number of consecutive invalid access

Security Levels	Applicable clauses for Security Levels
SL-1,SL-2 , SL-3,SL-4	CR 1.11

FR1.12 System use notification

Reference clause and description of requirement
CR 1.12:- Capability to display a system use notification message (Warnings, system use policy etc.) before authenticating.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2 , SL-3, SL-4	CR 1.12

FR1.13 Access via un-trusted networks

Reference clause and description of requirement
The access via un-trusted networks requirements are component specific and can be located as requirements for each specific component type in Clauses 4.3.2.9 through 4.3.2.12

FR1.14 Strength of symmetric key authentication

Reference clause and description of requirement
CR 1.14:- a) establish the mutual trust using the symmetric key b) store securely the shared secret c) Restrict access to the shared secret d) ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3
CR 1.14(1):- hardware security for symmetric keys based authentication.

Security Levels	Applicable clauses for Security Levels
SL-1	Nil
SL-2	CR 1.14
SL-3, SL-4	CR 1.14 (1)

4.3.2.3 FR2 User control

This FR prescribes requirements for assigning the privileges for authenticated users to carry out a requested action and also to monitor the use of such privileges assigned to them. The FR 2 is further subdivided (13 sub levels) and mapped against CR and SL as shown below:

FR2.1 Authorization enforcement

Reference clause and description of requirement
CR 2.1 :- Authorization enforcement mechanism for all human users based on their assigned responsibilities
CR2.1(1) :- Authorization enforcement for all users
CR2.1(2) :- Permission mapping to roles

CR2.1(3) :-Supervisor override: Component shall support a supervisor manual override for a configurable time or sequence of events.
CR2.1(4) :-Dual approval: Component shall support dual approval when action can result in serious impact on the industrial process.

Security Levels	Applicable clauses for Security Levels
SL-1	CR 2.1
SL-2	CR 2.1 (1) (2)
SL-3	CR 2.1 (1) (2) (3)
SL-4	CR 2.1 (1) (2) (3) (4)

FR2.2 Wireless use control

Reference clause and description of requirement
CR 2.2:-If a component supports usage through wireless interfaces it shall provide the capability to authorize, monitor and enforce usage restrictions according to commonly accepted industry practices.

Security Levels	Applicable clauses for Security Levels
SL-1,SL-2, SL-3, SL-4	CR 2.2

FR2.3 Use control for portable and mobile devices

Reference clause and description of requirement
CR 2.3 If a component utilizes portable and mobile devices , it shall provide the capability to automatically enforce configurable usage restrictions that including context specific authorization, restricting code and data transfer to/from portable and mobile devices

Security Levels	Applicable clauses for Security Levels
SL-1,SL-2, SL-3, SL-4	CR 2.3

FR2.4 Mobile code

Reference clause and description of requirement
The mobile code requirements are component specific and can be located as requirements for each specific device type in Cl. 4.3.2.9 through 4.3.2.12

FR2.5 Session lock

Reference clause and description of requirement
CR 2.5:- If a component provides a HMI, a) A session lock after a configurable time period b) The session lock shall remain in effect until re-establishes access using appropriate identification and authentication procedures.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 2.5

FR2.6 Remote session termination

Reference clause and description of requirement
CR 2.6:- Capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.

Security Levels	Applicable clauses for Security Levels
SL-1	Nil
SL-2, SL-3, SL-4	CR 2.6

FR2.7 Concurrent session control

Reference clause and description of requirement
CR 2.7:- Capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).

Security Levels	Applicable clauses for Security Levels
SL-1	Nil
SL-2	Nil
SL-3, SL-4	CR 2.7

FR2.8 Auditable events

Reference clause and description of requirement
CR 2.8 :-The component shall provide the capability to generate audit records relevant to security.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 2.8

FR2.9 Audit storage capacity

Reference clause and description of requirement
CR 2.9:- Capability of component a) to allocate audit record storage capacity b) to protect failure of component when it reaches or exceeds the audit storage capacity
CR 2.9 (1):-Warn when audit record storage capacity threshold reached

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2	CR 2.9
SL-3, SL-4	CR 2.9 (1)

FR2.10 Response to audit processing failures

Reference clause and description of requirement
CR 2.10 :-Capability of component a) to protect against the loss of essential services and functions in the event of an audit processing failure. b) to support appropriate actions in response to an audit processing failure

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 2.10

FR2.11 Time stamps

Reference clause and description of requirement
CR 2.11:- capability to create timestamps (including date and time) for use in audit records
CR 2.11(1):- Time synchronization
CR 2.11(2):-Protection of time source integrity

Security Levels	Applicable clauses for Security Levels
SL-1	CR 2.11
SL-2, SL-3	CR 2.11
SL-4	CR 2.11(1) (2)

FR2.12 Non-repudiation

Reference clause and description of requirement
CR 2.12:- Component shall provide the capability to determine whether a given human user took a particular action.
CR 2.12 (1):- Non-repudiation for all users

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3	CR 2.12
SL-4	CR 2.12 (1)

FR2.13 Use of physical diagnostic and test interfaces

Reference clause and description of requirement
The use of physical diagnostic and test interfaces are component specific and can be located as requirement for each specific component types in Clauses 4.3.2.9 through 4.3.2.12

4.3.2.4 FR 3 System integrity

This foundational requirement prevents unauthorised changes to components and ensures the integrity. The FR 3 is further subdivided (14 sub levels) and mapped against CR and SL as shown below:

FR3.1 Communication integrity

Reference clause and description of requirement
CR 3.1:- Capability to protect integrity of transmitted information
CR 3.1(1):- Communication authentication: capability to verify the authenticity of received information during communication.

Security Levels	Applicable clauses for Security Levels
SL-1	CR 3.1
SL-2, SL-3, SL-4	CR 3.1 (1)

FR3.2 Malicious code protection

Reference clause and description of requirement
The malicious code protection requirements are component specific and can be located as requirements for each specific device type in 4.3.2.9 through 4.3.2.12

FR3.3 Security functionality verification

References clause and description of requirement
CR 3.3 :- Capability to support verification of the intended operation of security functions according to IEC-62443-3-3
CR 3.3 (1):- Security functionality verification during normal operation

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3	CR 3.3
SL-4	CR 3.3 (1)

FR3.4 Software and information integrity

References clause and description of requirement
CR 3.4 :- Capability to perform or support integrity checks
CR 3.4 (1):- Capability to perform or support authenticity checks of software and information
CR 3.4 (2):- Automated notification of integrity violations

Security Levels	Applicable clauses for Security Levels
SL-1	CR 3.4
SL-2	CR 3.4 (1
SL-3, SL-4	CR 3.4 (1) (2)

FR3.5 Input validation

References clause and description of requirement
CR 3.5:- Capability to validate the syntax, length and content of any input

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 3.5

FR3.6 Deterministic output

References clause and description of requirement
CR 3.6:- Capability to set outputs to a predetermined state.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 3.6

FR3.7 Error handling

References clause and description of requirement
FR 3.7:- Capability to identify and handle error conditions.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 3.7

FR 3.8 Session integrity

References clause and description of requirement
CR 3.8:- Capability to protect the authenticity of communications sessions including Invalidate session identifiers upon user logout, generate a unique session identifier for each session.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	CR 3.8

FR3.9 Protection of audit information

References clause and description of requirement
CR 3.9:- Capability to protect audit information and audit.
CR 3.9 (1):- Audit records on write-once media

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2,SL-3	CR 3.9
SL-4	CR 3.9 (1)

FR3.10 Support for updates

References clause and description of requirement
Support for update requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12

FR3.11 Physical tamper resistance and detection

References clause and description of requirement
Physical tamper resistance and detection requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12

FR3.12 Provisioning product supplier root of trust

References clause and description of requirement
Provisioning product supplier root of trust requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12

FR3.13 Provisioning asset owner root of trust

References clause and description of requirement
Provisioning asset owner root of trust requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12

FR3.14 Integrity of boot process

References clause and description of requirement
Integrity of boot process requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12

4.3.2.5 FR4 Data confidentiality

This FR ensures to protect the data confidentiality i.e. unauthorised data disclosure is prevented. The FR 4 is further subdivided (3 sub levels) and mapped against CR and SL as shown below:

FR4.1 Information confidentiality

Reference clause and description of requirement
CR 4.1:- Capability to protect the confidentiality of information

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 4.1

FR4.2 Information persistence

Reference clause and description of requirement
CR 4.2:- Capability to erase all information when released from active service and/or decommissioned.
CR 4.2 (1):-Capability to protect against unauthorized and un intended information transfer via volatile shared memory resources.
CR 4.2 (2):- Capability to verify that erasure of information occurred.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	CR 4.2
SL-3, SL-4	CR 4.2 (1) (2)

FR4.3 Use of cryptography

Reference clause and description of requirement
CR 4.3:- Cryptographic security mechanisms shall be according to internationally recognized and proven security practices and recommendations.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 4.3

4.3.2.6 FR5 Restricted data flow

The information in an organisation is to be restricted and as per laid down policy on information sharing. This FR prescribes methods to restrict the data flow between various zones, networks, boundaries. Through risk analysis, the system designer is to identify and implement various methods/ controls to comply with this FR. The FR 5 is further subdivided (3 sub levels) and mapped against CR and SL as shown below:

FR5.1 Network segmentation

Reference clause and description of requirement
CR 5.1:-The component shall support a segmented network.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 5.1

FR5.2 Zone boundary protection

Reference clause and description of requirement
The zone boundary protection requirements are network component specific and can be located as requirements for network devices later in Clause 4.3.2.12

FR5.3 General purpose person-to-person communication restrictions

References clause and description of requirement
The general purpose person-to-person communication restriction requirements are network component specific and can be located as requirements for network devices later in Clause 4.3.2.12

4.3.2.7 FR6 Timely response to events

Policies and procedures are to be established to respond to a cyber-event and modes of communication to be used. The requirements intend to ensure that response actions are taken in a timely manner and data on cyber event is collected and analysed. The FR 6 is further subdivided (2 sub levels) and mapped against CR and SL as shown below:

FR6.1 Audit log accessibility

References clause and description of requirement
CR 6.1:- Capability for authorized humans and/or tools to access audit logs on a read-only basis.
CR 6.1 (1):- Programmatic access to audit

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2	CR 6.1
SL-3, SL-4	CR 6.1 (1)

FR6.2 Continuous monitoring

References clause and description of requirement
CR 6.2:- Capability to be continuously monitored to detect, characterize and report security breached in a timely manner.

Security Levels	Applicable clauses for Security Levels
SL-1	Nil
SL-2, SL-3, SL-4	CR 6.2

4.3.2.8 FR7 Resource Availability

Availability of resources is a critical aspect in control systems. The aim of the FR is to ensure that due to denial of service attacks, essential systems are available by ensuring operation even in degradation mode. The FR 7 is further subdivided (8 sub levels) and mapped against CR and SL as shown below:

FR7.1 Denial of service protection

References clause and description of requirement
CR 7.1:- Capability to maintain essential functions in a degraded mode as the result of a DoS event.
CR 7.1 (1):-Capability to manage communication load.

Security Levels	Applicable clauses for Security Levels
SL-1	CR 7.1
SL-2, SL-3, SL-4	CR 7.1 (1)

FR7.2 Resource management

References clause and description of requirement
CR 7.2:- Capability to limit the use of resources by security functions.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 7.2

FR7.3 Control system backup

References clause and description of requirement
CR 7.3:- Capability to participate in system level backup operations
CR 7.3 (1):-Capability to validate the integrity of backed up information prior to the initiation of restore.

Security Levels	Applicable clauses for Security Levels
SL-1	CR 7.3
SL-2, SL-3, SL-4	CR 7.3 (1)

FR7.4 Control system recovery and reconstitution

References clause and description of requirement
CR 7.4 Component shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 7.4

FR7.5 Emergency power

References clause and description of requirement
CR 7.5 :-Capable of running from an emergency power supply without affecting the existing security state or a documented degraded mode

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 7.5

FR7.6 Network and security configuration settings

References clause and description of requirement
CR 7.6:- Capability to be configured according to recommended network and security configurations. Capability to Interface to the currently deployed network and security configuration settings.
CR 7.6 (1):- Capability to generate a report listing the currently deployed security settings in a machine-readable format

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2	CR 7.6
SL-3, SL-4	CR 7.6 (1)

FR 7.7 Least functionality

References clause and description of requirement
CR 7.7:- Capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	CR 7.7

FR 7.8 Control system component inventory

References clause and description of requirement
CR 7.8:- Components shall provide the capability to support a control system component inventory according to IEC-62443-3-3 SR 7.8

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	CR 7.8

4.3.2.9 Software Application requirements (SAR)

SAR 1 (Ref 2.4 Mobile code)

References clause and description of requirement
SAR 2.4:- In the event that an application utilizes mobile code technologies that application shall provide the capability to:- a) Control execution of mobile code; b) Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application. c) Control the execution of mobile code based on the result of an integrity check prior to the code being executed.
SAR 2.4 (1):-Mobile code authenticity check -The application shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the result of authenticity check prior to code being executed.

Security Levels	Applicable clauses for Security Levels
SL-1	SAR 2.4
SL-2, SL-3, SL-4	SAR 2.4 (1)

SAR 2 (Ref 3.2 Protection from malicious code)

References clause and description of requirement
SAR 3.2:-The application product supplier shall qualify and document which malicious code protection mechanisms are compatible with the application and note any special configuration requirements

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	SAR 3.2

4.3.2.10 Embedded device requirements (EDR)

EDR 1(Ref 2.4 Mobile code)

References clause and description of requirement
EDR 2.4 :- In the event that an embedded device utilizes mobile code technologies, shall provide the capability to: a) Control execution of mobile code b) Control which users (human, software process, or device) are allowed to transfer mobile code to the device c) Control the execution of mobile code based on the result of an integrity check prior to the code being executed.
ECR 2.4 (1):- Mobile code authenticity check prior to code being executed

Security Levels	Applicable clauses for Security Levels
SL-1,	EDR 2.4
SL-2, SL-3, SL-4	EDR 2.4 (1)

EDR 2 (Ref 2.13 Use of Physical diagnostic and test interfaces)

References clause and description of requirement
EDR 2.13:- Embedded device shall protect against unauthorized use of physical factory diagnostic and test interfaces.
EDR 2.13(1): Embedded device shall provide active monitoring of the devices diagnostic and test interfaces and generate an audit log entry when attempts to access these interfaces are detected.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	EDR 2.13
SL-3, SL-4	EDR 2.13(1)

EDR 3 (Ref 3.2 Protection from malicious code)

References clause and description of requirement
EDR 3.2:-The embedded device shall provide the capability to protect from installation and execution of unauthorized software.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	EDR 3.2

EDR 4 (Ref 3.10 Support for updates)

References clause and description of requirement
EDR 3.10:- The embedded device shall support the ability to be updated and upgraded.
EDR 3.10(1) :- update authenticity and integrity: the embedded device shall validate the authenticity and integrity of any software update or upgrade prior to installation

Security Levels	Applicable clauses for Security Levels
SL-1	EDR 3.10
SL-2, SL-3, SL-4	ECR 3.10(1)

EDR 5 (Ref 3.11 Physical tamper resistance and detection)

References clause and description of requirement
EDR 3.11:- The embedded device shall provide tamper resistance and detection mechanism to protect against unauthorized physical access into device.
EDR 3.11(1) :- Notification of a tampering attempt

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	EDR 3.11
SL-3, SL-4	EDR 3.11(1)

EDR 6(Ref 3.12 Provisioning product supplier root of trust)

References clause and description of requirement
EDR 3.12:- Capability to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data to be used as one or more “roots of trust “at the time of manufacture of the device.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	EDR 3.12

EDR 7 (Ref 3.13 Provisioning asset owners root of trust)

References clause and description of requirement
EDR 3.13:- The embedded device shall provide a) The capability to provision and protect the confidentiality, integrity and authenticity of asset owner’s keys and data to be used as one or more “roots of trust”. b) The capability to provision without reliance on components that may be outside of device security zone.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	EDR 3.13

EDR 8 (Ref 3.14 Integrity of the boot process)

References clause and description of requirement
EDR 3.14:- The embedded devices shall verify the integrity of firmware, software and configuration data needed for the component boot and runtime process prior to use.
EDR 3.14(1):-Verify Authenticity of boot process

Security Levels	Applicable clauses for Security Levels
SL-1	EDR 3.14
SL-2, SL-3, SL-4	EDR 3.14(1)

4.3.2.11 Host device requirements (HDR)

Host device is a general purpose device running a general purpose operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more applications, data stores or functions.

HDR 1(ref 2.4 Mobile code)

References clause and description of requirement
HDR 2.4:-In the event that a host device utilizes mobile code technologies, that host device shall provide the capability to: a) Control execution of mobile code b) Control which users (human, software process, or device) are allowed to transfer mobile code to the host devices. c) Control the execution of mobile code based on the result of an integrity check prior to the code being executed.
HDR 2.4 (1):- Mobile code authenticity check prior to code being executed

Security Levels	Applicable clauses for Security Levels
SL-1	HDR 2.4
SL-2, SL-3, SL-4	HDR 2.4 (1)

HDR 2 (Ref 2.13 Use of Physical diagnostic and test interfaces)

References clause and description of requirement
HDR 2.13:- Host device shall protect against unauthorized use of physical factory diagnostic and test interfaces.
HDR 2.13(1): Host device shall provide active monitoring of the devices diagnostic and test interfaces and generate an audit log entry when attempts to access these interfaces are detected.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	HDR 2.13
SL-3, SL-4	HDR 2.13(1)

HDR 3 (Ref 3.2 Protection from malicious code)

References clause and description of requirement
HDR 3.2:- There shall be mechanisms on host devices that are qualified by the IACS supplier to provide protection from malicious code.
HDR 3.2(1):- Automatically report version of code protection

Security Levels	Applicable clauses for Security Levels
SL-1	HDR 3.2
SL-2, SL-3, SL-4	HDR 3.2(1)

HDR 4 (Ref 3.10 Support for updates)

References clause and description of requirement
HDR 3.10:- The host devices shall support the ability to be updated and upgraded.
HDR 3.10(1) :- update authenticity and integrity: The host device shall validate the authenticity and integrity of any software update or upgrade prior to installation.

Security Levels	Applicable clauses for Security Levels
SL-1	EDR 3.10
SL-2, SL-3, SL-4	EDR 3.10(1)

HDR 5 (Ref 3.11 Physical tamper resistance and detection)

References clause and description of requirement
HDR 3.11:- Host device shall provide tamper resistance and detection mechanism to protect against unauthorized physical access into device.
HDR 3.11(1) :- Notification of a tampering attempt

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	HDR 3.11
SL-3, SL-4	HDR 3.11(1)

HDR 6 (Ref 3.12 Provisioning product supplier root of trust).

References clause and description of requirement
HDR 3.12:- Capability to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	HDR 3.12

HDR 7(Ref 3.13 Provisioning asset owners root of trust.)

References clause and description of requirement
HDR 3.13:- Host devices shall provide a) The capability to provision and protect the confidentiality, integrity and authenticity of asset owner’s keys and data to be used as one or more “roots of trust”. b) The capability to provision without reliance on components that may be outside of device security zone.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	HDR 3.13

HDR 8 (Ref 3.14 Integrity of the boot process)

References clause and description of requirement
HDR 3.14:- Host devices shall verify the integrity of firmware, software and configuration data needed for the component boot and runtime process prior to use.
HDR 3.14(1):- Verify authenticity of boot process

Security Levels	Applicable clauses for Security Levels
SL-1	HDR 3.14
SL-2, SL-3, SL-4	HDR 3.14(1)

4.3.2.12 Network device requirements (NDR)

NDR 1 (Ref 1.6 Wireless access management)

Reference clause and description of requirement
NDR 1.6:- Capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.
NDR 1.6(1):-Unique identification and authentication:- Capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

Security Levels	Applicable clauses for Security Levels
SL-1	NDR 1.6
SL-2, SL-3, SL-4	NDR 1.6(1)

NDR 2 (Ref 1.13 Access via untrusted networks)

References clause and description of requirement
NDR 1.13:- Capability to monitor and control all methods of access to the network device via untrusted networks.
NDR 1.13(1):- Capability to deny access requests via untrusted networks unless approved.

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2	NDR 1.13
SL-3, SL-4	NDR 1.13(1)

NDR 3 (Ref 2.4 Mobile code)

References clause and description of requirement
NDR 2.4:-In the event that a network device utilizes mobile code technologies, that network shall provide the capability to: **a)** Control execution of mobile code **b)** Control which users (human, software process, or device) are allowed to transfer mobile code to/from the network device **c)** Control the execution of mobile code based on the result of an integrity check prior to the code being executed.
NDR 2.4 (1):- Mobile code authenticity check prior to code being executed

Security Levels	Applicable clauses for Security Levels
SL-1	NDR 2.4
SL-2, SL-3, SL-4	NDR 2.4 (1)

NDR 4 (Ref 2.13 Use of Physical diagnostic and test interfaces)

References clause and description of requirement
NDR 2.13:- Network device shall protect against unauthorized use of physical factory diagnostic and test interfaces.
NDR 2.13(1): Network device shall provide active monitoring of the devices diagnostic and test interfaces and generate an audit log entry when attempts to access these interfaces are detected.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	NDR 2.13
SL-3, SL-4	NDR 2.13(1)

NDR 5 (Ref 3.2 Protection from malicious code)

References clause and description of requirement
NDR 3.2: The network device shall provide for malicious code protection either directly or via a compensating control

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	NDR 3.2

NDR 6 (Ref 3.10 Support for updates)

References clause and description of requirement
NDR 3.10:- The Network devices shall support the ability to be updated and upgraded.
HDR 3.10(1) :- The network device shall validate the authenticity and integrity of any software update or upgrade prior to installation.

Security Levels	Applicable clauses for Security Levels
SL-1	NDR 3.10
SL-2, SL-3, SL-4	NDR 3.10(1)

NDR 7 (Ref 3.11 Physical tamper resistance and detection)

References clause and description of requirement
NDR 3.11:- Network device shall provide tamper resistance and detection mechanism.
NDR 3.11(1) :- Notification of a tampering attempt

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2	NDR 3.11
SL-3, SL-4	NDR 3.11(1)

NDR 8 (Ref 3.12 Provisioning product supplier root of trust.)

References clause and description of requirement
NDR 3.12:- Capability to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	NDR 3.12

NDR 9 (Ref 3.13 Provisioning asset owners root of trust).

References clause and description of requirement
NDR 3.12:- Network devices shall provide a) The capability to provision and protect the confidentiality, integrity and authenticity of asset owner’s keys and data to be used as one or more “roots of trust”. b) The capability to provision without reliance on components that may be outside of device security zone.

Security Levels	Applicable clauses for Security Levels
SL-1	NA
SL-2, SL-3, SL-4	NDR 3.13

NDR 10 (Ref 3.14 Integrity of the boot process)

References clause and description of requirement
NDR 3.14:- The network devices shall verify the integrity of firmware, software and configuration data needed for the component boot and runtime process prior to use.
NDR 3.14(1):- Verify authenticity of boot process

Security Levels	Applicable clauses for Security Levels
SL-1	NDR 3.14
SL-2, SL-3, SL-4	NDR 3.14(1)

NDR 11 (Ref 5.2 Zone boundary protection)

References clause and description of requirement
NDR 5.2:- Capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.
NCR 5.2 (1):-Deny all, permit by exception
NCR 5.2(2):- capability to prevent any communication through the control system boundary
NCR 5.2 (3):-Fail Close- prevents communication through the control system boundary during failure of boundary protection system.

Security Levels	Applicable clauses for Security Levels
SL-1	NDR 5.2
SL-2	NDR 5.2 (1)
SL-3	NDR 5.2 (1) (2) (3)
SL-3	NDR 5.2 (1) (2) (3)

NDR 12 (ref 5.3 General purpose, person-to-person communication restrictions)

References clause and description of requirement
NDR 5.3:- Capability to prevent general purpose, person-to-person messages from being received from users or systems external to the control system

Security Levels	Applicable clauses for Security Levels
SL-1, SL-2, SL-3, SL-4	NDR 5.3

4.3.3 Performance test protocol for SL-E

4.3.3.1 The requirements in this sub-section are based on selected requirements in IEC 62443-3-3 standard. The following security capabilities are required for all CBSs in the scope specified in Part 4, Chapter 7, Section 8 of the Rules.

Table 4.3.3.1: Required security capabilities for all CBSs

Item No	Objective	Requirements
Protect against casual or coincidental access by unauthenticated entities		
1	Human user identification and authentication	The CBS shall identify and authenticate all human users who can access the system directly or through interfaces (IEC 62443-3-3/SR 1.1)
2	Account management	The CBS shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing account (IEC 62443-3-3/SR 1.3)
3	Identifier management	The CBS shall provide the capability to support the management of identifiers by user, group and role. (IEC 62443-3-3/SR 1.4)
4	Authenticator management	The CBS shall provide the capability to: - Initialize authenticator content - Change all default authenticators upon control system installation - Change/refresh all authenticators - Protect all authenticators from unauthorized disclosure and modification when stored and transmitted. (IEC 62443-3-3/SR 1.5)
5	Wireless access management	The CBS shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication (IEC 62443-3-3/SR 1.6)
6	Strength of password-based authentication	The CBS shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. (IEC 62443-3-3/SR 1.7)

7	Authenticator feedback	The CBS shall obscure feedback during the authentication process. (IEC 62443-3-3/SR 1.10)
Protect against casual or coincidental misuse		
8	Authorization enforcement	On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege. (IEC 62443-3-3/SR 2.1)
9	Wireless use control	The CBS shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the system according to commonly accepted security industry practices (IEC 62443-3-3/SR 2.2)
10	Use control for portable and mobile devices	When the CBS supports use of portable and mobile devices, the system shall include the capability to a) Limit the use of portable and mobile devices only to those permitted by design b) Restrict code and data transfer to/from portable and mobile devices Note: Port limits / blockers (and silicone) could be accepted for a specific system (IEC 62443-3-3/SR 2.3)
11	Mobile code	The CBS shall control the use of mobile code such as java scripts, ActiveX and PDF. (IEC 62443-3-3/SR 2.4)
12	Session lock	The CBS shall be able to prevent further access after a configurable time of inactivity or following activation of manual session lock. (IEC 62443-3-3/SR 2.5)
13	Auditable events	The CBS shall generate audit records relevant to security for at least the following events: access control, operating system events, backup and restore events, configuration changes, loss of communication. (IEC 62443-3-3/SR 2.8)
14	Audit storage capacity	The CBS shall provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management. Auditing mechanisms shall be implemented to reduce the likelihood of such capacity being exceeded. (IEC 62443-3-3/SR 2.9)
15	Response to audit processing failures	The CBS shall provide the capability to prevent loss of essential services and functions in the event of an audit processing failure. (IEC 62443-3-3/SR 2.10)
16	Timestamps	The CBS shall timestamp audit records. (IEC 62443-3-3/SR 2.11)
Protect the integrity of the CBS against casual or coincidental manipulation		
17	Communication integrity	The CBS shall protect the integrity of transmitted information. Note: Cryptographic mechanisms shall be employed for wireless networks. (IEC 62443-3-3/SR 3.1)
18	Malicious code protection	The CBS shall provide capability to implement suitable protection measures to prevent, detect and mitigate the effects due to malicious code or unauthorized software. It shall have the feature for updating the protection mechanisms (IEC 62443-3-3/SR 3.2)
19	Security functionality verification	The CBS shall provide the capability to support verification of the intended operation of security functions and report when anomalies occur during maintenance (IEC 62443-3-3/SR 3.3)

20	Deterministic output	The CBS shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack. The predetermined state could be: – Unpowered state, – Last-known value, or – Fixed value (IEC 62443-3-3/SR 3.6)
Prevent the unauthorized disclosure of information via eavesdropping or casual exposure		
21	Information confidentiality	The CBS shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit. Note: For wireless network, cryptographic mechanisms shall be employed to protect confidentiality of all information in transit. (IEC 62443-3-3/SR 4.1)
22	Use of cryptography	If cryptography is used, the CBS shall use cryptographic algorithms, key sizes and mechanisms according to commonly accepted security industry practices and recommendations. (IEC 62443-3-3/SR 4.3)
Monitor the operation of the CBS and respond to incidents		
23	Audit log accessibility	The CBS shall provide the capability for accessing audit logs on read only basis by authorized humans and/or tools. (IEC 62443-3-3/SR 6.1)
Ensure that the control system operates reliably under normal production conditions		
24	Denial of service protection	The CBS shall provide the minimum capability to maintain essential functions during DoS events. Note: It is acceptable that the CBS may operate in a degraded mode upon DoS events, but it shall not fail in a manner which may cause hazardous situations. Overload-based DoS events should be considered, i.e. where the networks capacity is attempted flooded, and where the resources of a computer is attempted consumed. (IEC 62443-3-3/SR 7.1)
25	Resource management	The CBS shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion. (IEC 62443-3-3/SR 7.2)
26	System backup	The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the CBS without affecting normal operations (IEC 62443-3-3/SR 7.3)
27	System recovery and reconstitution	The CBS shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure. (IEC 62443-3-3/SR 7.4)
28	Alternative power source	The CBS shall provide the capability to switch to and from an alternative power source without affecting the existing security state or a documented degraded mode. (IEC 62443-3-3/SR 7.5)
29	Network and security configuration settings	The CBS traffic shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the supplier. The CBS shall provide an interface to the currently deployed network and security configuration settings. (IEC 62443-3-3/SR 7.6)

30	Least Functionality	The installation, the availability and the access rights of the following shall be limited to the strict needs of the functions provided by the CBS: - operating systems software components, processes and services - network services, ports, protocols, routes and hosts accesses and any software (IEC 62443-3-3/SR 7.7)

4.3.3.2 The following additional security capabilities are required for CBSs with network communication to untrusted networks. CBSs with communication traversing the boundaries of security zones are also to meet requirements for network segmentation and zone boundary protection.

Table 4.3.3.2: Additional security capabilities for CBSs with network communication to untrusted networks

Item No	Objective	Requirements
31	Multifactor authentication for human users	Multifactor authentication is required for human users when accessing the CBS from or via an untrusted network. (IEC 62443-3-3/SR 1.1, RE 2)
32	Software process and device identification and authentication	The CBS shall identify and authenticate software processes and devices (IEC 62443-3-3/SR 1.2)
33	Unsuccessful login attempts	The CBS shall enforce a limit of consecutive invalid login attempts from untrusted networks during a specified time period. (IEC 62443-3-3/SR 1.11)
34	System use notification	The CBS shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel. (IEC 62443-3-3/SR 1.12)
35	Access via Untrusted Networks	Any access to the CBS from or via untrusted networks shall be monitored and controlled. (IEC 62443-3-3/SR 1.13)
36	Explicit access request approval	The CBS shall deny access from or via untrusted networks unless explicitly approved by authorized personnel on board. (IEC 62443-3-3/SR 1.13, RE1)
37	Remote session termination	The CBS shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session. (IEC 62443-3-3/SR 2.6)
38	Cryptographic integrity protection	The CBS shall employ cryptographic mechanisms to recognize changes to information during communication with or via untrusted networks. (IEC 62443-3-3/SR 3.1, RE1)
39	Input validation	The CBS shall validate the syntax, length and content of any input data via untrusted networks that is used as process control input or input that directly impacts the action of the CBS. (IEC 62443-3-3/SR 3.5)
40	Session integrity	The CBS shall protect the integrity of sessions. Invalid session IDs shall be rejected. (IEC 62443-3-3/SR 3.8)
41	Invalidation of session IDs after session termination	The system shall invalidate session IDs upon user logout or other session termination (including browser sessions). (IEC 62443-3-3/SR 3.8, RE1)

Section 5

Works Assessment

5.1 Works Assessment

5.1.1 A survey of the manufacturer's works will be carried out by IRS Surveyor to review the manufacturing & testing facilities and process control to ensure consistency in product quality.

5.1.2 The survey will cover assessment of the capability, experience and organization structure of the manufacturer, qualification and experience of the production and QA/ QC personnel, manufacturing facilities, quality control operations, identification and traceability, record keeping and storage facilities etc.

5.1.3 Extent of survey may be limited for manufacturers in possession of valid quality management system certificate.

Section 6

Certification

6.1 Performance Tests

6.1.1 The performance tests are to be conducted as per agreed performance test protocol and will be witnessed by IRS surveyor. Refer Section 4 for tests to be witnessed.

6.1.2 Any deviation from the agreed performance test protocol is to be referred to H.O for the concurrence.

6.2 Issuance of Certificate

6.2.1 Type Approval Certificate will be issued after successful witnessing of testing at manufacturer's works. Approval Certificate will be issued with validity for 5 years.

6.3 Withdrawal of Certificate

6.3.1 The type approval certificate will be invalid if :

a) There are substantial modifications in the design, in the manufacturing or control processes or in the characteristics of the components/ materials unless approved in advance by IRS.
b) Safety or any other feature of the components is found to be unsatisfactory in service.

6.4 Intermediate Audit

6.4.1 IRS will carry out an intermediate audit of the manufacturing works during the five year period. The intervals between initial, intermediate audits is not to be more than 30 months.

6.5. Certificate Renewal

6.5.1 A renewal of type approval certificates will be granted upon:

a) Submission of request for renewal

b) Submission of modified documents or new documents with substantial modifications replacing former documents compared to the previous submission(s) for TA.

c) A declaration that no substantial modifications have been applied/ undertaken since the last TA was issued.

End of Classification Note