# ANNEXURE-R

# KAVACH Cloud and

# Cyber Security Requirements

1. **Scope:**

   This document defines a common, minimum set of security measures and risk management etc. to be considered to design a system /subsystem for more stringent security levels to address the threats during cyber attack along with storage requirements.

2. This specification requires reference to the following documents –

| | | |
|---|---|---|
| 1 | EN 50126 | Railway Applications- Specifications and demonstration of Reliability, Availability, Maintainability & Safety. |
| 2 | IEC 62443 | Security for industrial automation and contrtol systems |
| 3 | ISO 27017 | Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services |
| 4 | EN-50701 | Railway applications – CyberSecurity |

| | | |
|---|---|---|
| 5 | EN-50716 | |
| 6 | CSM-RA | Common safety method for risk evaluation and assessment |

3. **Abbreviations:**

| **Abbreviation** | **Full Form/ Description** |
|---|---|
| **AES** | Advanced encryption standard |
| ATP | Automatic Train Protection System |
| CERT-In | Indian Computer Emergency Response Team |
| CRS | Cyber security Requirement Specification |
| CTC | Centralized Traffic Control |
| CIKMS | Centrlized Intelligent Kavach Management System |
| **DC** | Data Center |
| **DC** | **Data Confidentiality** |
| **DoS** | Denial of service |
| **DR** | Disaster Recovery |
| **DRA** | Detailed Risk Assessment |
| ETCS | European train control system |
| FRACAS | Failure Reporting and Corrective Action System |
| **IAC** | Identification and authentication control |
| **IACS** | Industrial Automation Control System |
| **ICERT** | Indian Computer Emergency Response Team |
| ICMS | Information Security Management System |
| **ID** | Identifier |
| ISA | Independent Safety Assessor |
| KMS | Key Management System |
| LPOCIP | Loco Pilot operation cum indication panel |
| NMS | Network monitoring system |
| PIMS | Privacy Information Management System |
| **PKI** | Public key infrastructure |
| **PQC** | Post Quantum Cryptography |

| Abbreviation | Full Form/ Description |
|---|---|
| PSK | Pre-Shared Keys |
| RA | Resource availability |
| **RDF** | Restricted data flow |
| RFID | Radio frequency identification |
| RIU | Remote Interface Units |
| **SI** | System integrity |
| **SIM** | Subscriber Identity Module |
| **SL** | Security level |
| **SL-A** | Achieved security level |
| **SL-C** | Capability security level |
| **SL-T** | Target security level |
| **SR** | System requirement |
| **SSL** | Secure Sockets Layer |
| **SUC** | System Under Consideration |
| TRE | Timely response to events |
| TSR | Temporary speed restrictions |
| **UC** | Use control |
| **VAPT** | Vulnerability Assessment and Penetration Testing |
| **V&V** | Verification and Validation |

4. **Definition:**

4.1 **Attack:** Assault on a system that derives from an intelligent threat.

4.2 **Active Attack:** attempts to alter system resources or affect their operation;

4.3 **Passive Attack:** attempts to learn or make use of information from the system but does not affect the system.

4.4 **Inside Attack:** is an attack initiated by an entity inside the security perimeter (an "insider"),

4.5 **Outside Attack**: initiated from outside the perimeter, by an unauthorized or illegitimate user of the system(including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists and hostile governments

4.6 **Threat:** circumstance or event with the potential to adversely affect operations (including mission,functions, image or reputation), assets,

control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service.

4.7 **Authentication:** provision of assurance that a claimed characteristic of an identity is correct.

4.8 **Authenticator:** means used to confirm the identity of a user (human, software process or device).

4.9 **Authenticity**: property that an entity is what it claims to be

4.10 **Identifier:** symbol, unique within its security domain, that identifies, indicates or names an entity which makes an assertion or claim of identity

4.11 **Identify**: assertion of an identity

4.12 **Session:**semi-permanent, stateful and interactive information interchange between two or more communicating devices

4.13 **Session ID**: identifier used to indicate a specific session

4.14 **Impact**: evaluated consequence of a particular event

4.15 **Security Level** : measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

4.16 **Countermeasure:** action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

5. **Procedure:**

5.1 The following fundamental requirements to be considered while development/design of product:

i. Identification and authentication control (IAC),
ii. Use control (UC),
iii. System integrity (SI),
iv. Data confidentiality (DC),
v. Restricted data flow (RDF),
vi. Timely response to events (TRE),
vii. Resource availability (RA).

5.2 System shall be designed in such a way to meet the following requirements:

i. Identify, asses and understand to perform the risk assessment and to mitigate risk of cybersecurity threats.There shall be provision of comprehensive Information Security Management System(ICMS) and Privacy Information Management System(PIMS) involved implementing security (as well as data protection and privacy) control in order to mitigate and prevent emerging threats affecting security of land transport services and systems(including their data).

ii. Detect of cyber security threats

iii. Protect against cyber security threats

iv. Respond to cybersecurity incidents

v. Procedure to secure system design in accordance to 50701 and 50716: The product life cycle shall be in accordance with V-cycle representation in EN-50126. The following phase wise activities shall be adhered:

5.2.1 **Concept Phase**:

i. Review of the degree of security achieved up to now.

ii. Analysis of project's security implication and context (including generic threats)

iii. Alignment with Indian Railways cyber security goals.

iv. Consideration of security life cycle aspects (patch management, monitoring etc.,)

5.2.2 **System Definition and Operational Context Phase**:

i. Review of logical and physical network plans.

ii. *Initial Risk Assessment for the SuC shall be carried out as shown in the Table-01

**Table-01: Initial Risk Assessment of Assets**

| Asset | Impact (A to E)# A- Major interruption E- no influence | Likelihood (1 to 5)## 1 being low and 5 being high | Risk (Extreme/ High/ Significant// Medium/ Low) | Acceptable (Yes/No) |
|---|---|---|---|---|
| | | | | |
| | | | | |



# These are assessed based on availability, safety integrity, confidentiality and business integrity.

# # Likelihood=Exposure+Vulnerability-1. Exposure is rated from 1 to 3 where 1- Highly restricted; 2- restricted; 3- Easy; for physical/logical access. Vulnerability is rated from 1 to 3 where 1- high; 2- average; 3- unskilled; hacker can attack the SuC.

iii. *Partitioning of the SuC into zones and conduits

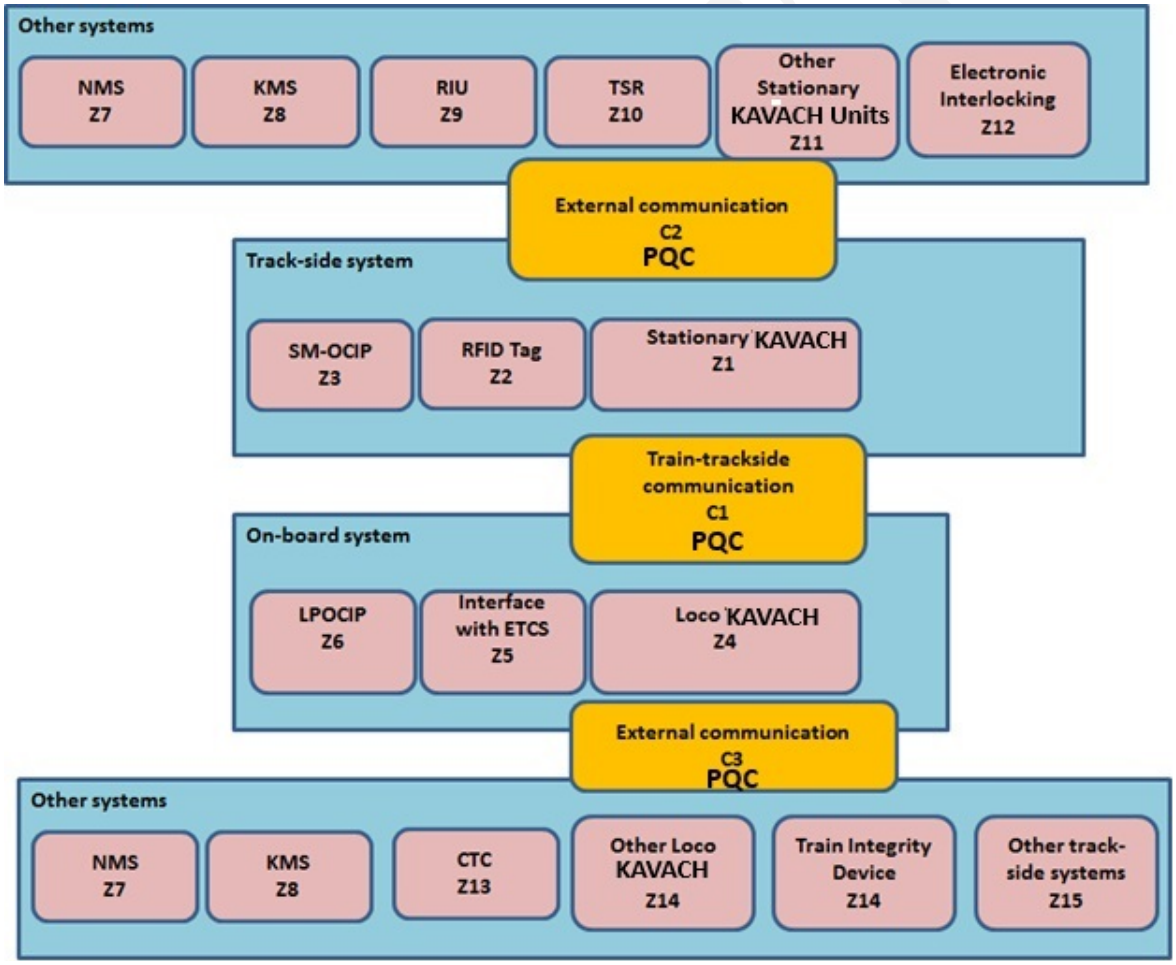
iv. *Documentation of components, interfaces and characteristics for each zone and conduit in risk analysis and evaluation phase.

v. *This activity and the corresponding synchronization point may also be conducted in DRA.

5.2.3 **Risk Analysis and Evaluation Phase:**

i. Detailed Risk Assessment (DRA): Derive Security Level Targets, physical and organizational countermeasures or assumptions for zones and conduits.

ii. The tentatives of zones and conduits for Indian Railway ATP system is shown in the figure below:




iii. The process needs to take into account also legacy solutions and shall allow a non-disruptive move to IEC 62443/EN 50701/EN

50716. Zone/conduit requirements are to be consolidated.

**Table-02:Classification in Zones and Conduits**

| N Zone/Conduit | Type Zone/Conduit | Including (List of assets) | Risk (Extreme/ High/ Significant// Medium/ Low) | Acceptable (Yes/No) |
|---|---|---|---|---|
| Z1 | Zone | | | |
| Z2 | Zone | | | |
| C1 | Conduit | | | |
| C2 | Conduit | | | |

iv. Consider business continuity aspects (including incidence response and recovery) for the SuC.

5.2.4 **Specification of system requirements:**

i. SuC- specific refinement of normative requirements.

ii. Definition of organizational and physical requirements.

iii. Definition of security-related application conditions.

5.2.5 **Determination of Security Level (SL):**

i. Security Level shall be viewed as a qualitative means of risk reduction. A risk matrix with appropriate acceptance criteria shall be developed.

ii. Based on detailed risk assessment (DRA), the technical (SL-T) , physical and organizational countermeasures or assumptions for zones and conduits to be arrived at considering business continuity aspects (including incidence response and recovery) for the SuC.

iii. A list of the threats that could affect the assets contained within the zone or conduit shall be developed.

iv. Identify the vulnerabilities. The zone or conduit shall be analysed in order to identify and document the known vulnerabilities associated with the assets contained within the zone or conduit

including the access points.

v. For each threat at least the following information as shown in the table shall be documented in the threat log.

| Threat name | Threat Source (internal/ external) | Capability or skills ot motivation of threat source | Possible threat scenarios and actions | Potentially affected assets (Z1..Zm, C1….Cn) | Vulnerabilities of the SuC (if known) |
|---|---|---|---|---|---|
| Ex: T.Physical attacks | | | | | |
| T.Unintentional Damage | | | | | |
| | | | | | |

5.2.6 Determine consequence and impact. Each threat scenario shall be evaluated to determine the consequence and the impact should the threat

be realized. Consequences should be documented in terms of the worst-case impact on risk areas.

5.2.7 Determine unmitigated likelihood. Each threat shall be evaluated to determine the unmitigated likelihood. This is the likelihood that the threat will materialize.

5.2.8 The unmitigated cyber security risk for each threat shall be determined by combining the impact measure and the unmitigated likelihood measure determined above.

5.2.9 Determine SL-T. SLs have been broken down into three different types: target, achieved and capability. These types, while they all are related, have to do with different aspects of the security lifecycle.

i. Target SLs (SL-T) are the desired level of security for a particular system. This is to be determined after performing the risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.

ii. Achieved SLs (SL-A) are the actual level of security for a particular system. These are to be measured after the system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the target SLs.

iii. Capability SLs (SL-C) are the security levels that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the target SLs natively without additional compensating countermeasures when properly configured and integrated.

iv. The developing firm shall assess the cyber security risk and determine the SL-T for each defined zone and conduit based on IEC 62443 3-2 and IEC 62443 3-3. However, a sample overview is given in the following table:

v. SL-T shall be established for each security zone or conduit.

**Annexure-R**

| | **Violation** | **Means** | **Resources** | **Skills** | **Motivation** |
|---|---|---|---|---|---|
| **SL 0** | | | | | |
| **SL 1** | Causal or coincidental | | | | |
| **SL 2** | Intentional | Simple | Low | Generic | Low |
| **SL 3** | | Sophisticated | Moderate | Specific | Moderate |
| **SL 4** | | | Extended | | High |

5.2.10 Compare unmitigated risk with tolerable risk.

5.2.11 Existing countermeasures in the SUC shall be identified and evaluated to determine the effectiveness of the countermeasures to reduce the likelihood or impact.

5.2.12 The likelihood and impact shall be re-evaluated considering the countermeasures and their effectiveness.

5.2.13 The residual risk for each threat identified above, shall be determined by combining the mitigated likelihood measure and mitigated impact values.

5.2.14 The residual risk determined for each threat identified shall be compared to the organization's tolerable risk. If the residual risk exceeds the tolerable risk, the organization shall determine if the residual risk will be accepted, transferred or mitigated.

5.2.15 Additional cyber security countermeasures such as technical, administrative or procedural controls shall be identified to mitigate the risks where the residual risk exceeds the organization's tolerable risk.

## 5.3 Selection of counter measures:

5.3.1 System definition and operational context:

5.3.2 System design and operation shall be defined as follows:

5.3.3 System under consideration boundaries shall be defined.

5.3.4 Partitioning of the SuC into zones and conduits

5.3.5 The PQC encryptor shall be used to establish a secure connection between multiple sites over the public/captive network, as illustrated in the deployment scenario. The encryptor works as the gateway for each of the sites. The sites may comprise of servers, individual PCs, laptops or even cluster of subnets. As per the configuration, quantum resistant connection is authenticated either using Pre-Shared Keys (PSKs) or quantum–safe digital certificates. A single PQC encryptor shall be capable of establishing quantum-secure connections with multiple PQC

encryptors located at different geographical sites.

5.3.6 Generate true 2 sets of random keys with key size of 16 bytes based on Advanced Encryption Method (RFC 3826 or better) to generate 2 keys, each. Keys shall be delivered as described in clause 4 of System Requirement Specifications of KAVACH Specifications. The key generating system shall generate One Time Password to at least four SIMs (configurable) for each of the Kavach entities and shall be working in DC-DR mode at geo redundant different enterprise locations. The SMS service shall also be part of development. The development shall not necessitate any change in KAVACH working.

5.3.7 The solution provider shall identify two meity-listed robust data centers of different enterprises for hosting Kavach cloud data in DC-DR mode. The Kavach cloud data requirements shall include: Key generation system, Post quantum encrypting servers, Failure Reporting and Corrective Action System, Centralized KAVACH Intelligent Monitoring system, Version control software, Kavach executive and application data hosting servers, Kavach training and video material, Chatbots etc.

5.3.8 The software developed shall be deposited in escrow account and indian railways shall be the owner of it.

## 5.4 Cloud Storage Requirements

5.4.1 Production Environments:

| **Description** | **Purpose** | **OS Version** | **Qty** | **RAM (GB)** | **Cores** | **Storage** |
|---|---|---|---|---|---|---|
| Application Server | FRACAS | LINUX | 3 | 128 | 8 | 700 GB |
| Database Server | FRACAS | LINUX | 2 | 256 | 8 | 4 TB |
| Mobile Server instance | FRACAS | LINUX | 1 | 128 | 8 | 700 GB |
| SAN Storage | FRACAS | LINUX | 1 | 128 | 8 | 15 TB |
| Application Server | KMS | LINUX | 2 | 256 | 8 | 4 TB |
| Database Server | KMS | LINUX | 1 | 128 | 8 | 1 TB |
| Application Server | CIKMS | LINUX | 1 | 256 | 8 | 15 TB |

| **Description** | **Purpose** | **OS Version** | **Qty** | **RAM (GB)** | **Cores** | **Storage** |
|---|---|---|---|---|---|---|
| Database Server | CIKMS | LINUX | 1 | 128 | 8 | 15 TB |
| Application Server | Chatbot | LINUX | 1 | 128 | 8 | 15 TB |
| Database Server | Chatbot | LINUX | 1 | 128 | 8 | 15 TB |

5.4.2 DR Environment:

| **Description** | **Purpose** | **OS Version** | **Qty** | **RAM (GB)** | **Cores** | **Storage** |
|---|---|---|---|---|---|---|
| Application Server | FRACAS | LINUX | 3 | 128 | 8 | 700 GB |
| Database Server | FRACAS | LINUX | 2 | 256 | 8 | 4 TB |
| | KMS | | | | | |
| | CIKMS | | | | | |
| | Chatbot | | | | | |

5.4.3 Test Environment:

| **Description** | **Purpose** | **OS Version** | **Qty** | **RAM (GB)** | **Cores** | **Storage** |
|---|---|---|---|---|---|---|
| Application Server | FRACAS | LINUX | 3 | 32 | 4 | 700 GB |
| Database Server | FRACAS | LINUX | 1 | 32 | 4 | 1 TB |
| Mobile Server instance | FRACAS | LINUX | 1 | 128 | 8 | 700 GB |
| Database Server | KMS | LINUX | 1 | 32 | 4 | 700 GB |
| Application Server | KMS | LINUX | 1 | 32 | 4 | 700 GB |

| **Description** | **Purpose** | **OS Version** | **Qty** | **RAM (GB)** | **Cores** | **Storage** |
|---|---|---|---|---|---|---|
| Application Server | CIKMS | LINUX | 1 | 32 | 4 | 700 GB |
| Database Server | CIKMS | LINUX | 1 | 32 | 4 | 1 TB |
| Application Server | Chatbot | LINUX | 1 | 32 | 4 | 700 GB |
| Database Server | Chatbot | LINUX | 1 | 32 | 4 | 1 TB |
| Mobile Server instance | Chatbot | Linux/ Android/ IoS | 1 | 128 | 8 | 700 GB |

5.4.4 Development Environment:

| **Description** | **Purpose** | **OS Version** | **Qty** | **RAM (GB)** | **Cores** | **Storage** |
|---|---|---|---|---|---|---|
| Application Server | FRACAS | LINUX | 3 | 32 | 4 | 700 GB |
| Database Server | FRACAS | LINUX | 1 | 32 | 4 | 1 TB |
| Mobile Server instance | FRACAS | LINUX | 1 | 32 | 4 | 700 GB |
| Application Server | KMS | LINUX | 3 | 32 | 4 | 700 GB |
| Database Server | KMS | LINUX | 1 | 32 | 4 | 1 TB |
| Application Server | CIKMS | LINUX | 3 | 32 | 4 | 700 GB |
| Database Server | CIKMS | LINUX | 1 | 32 | 4 | 1 TB |
| Application Server | Chatbot | IOS/Android | 1 | 32 | 4 | 700 GB |
| Database Server | Chatbot | IOS/Android | 1 | 32 | 4 | 1 TB |

| Description | Purpose | OS Version | Qty | RAM (GB) | Cores | Storage |
|---|---|---|---|---|---|---|
| Mobile Server instance | Chatbot | IOS/Android | 1 | 32 | 4 | 700 GB |

## 5.5 Data Center Requirements

5.5.1 The data centers shall have Cert-IN approval (MEITY) and shall be owned by government or public sector.

5.5.2 The data centers hosting the cloud shall be secured with VAPT, hack-proof measures, and SSL certifications.

5.5.3 The data center/ disaster recovery center shall be cerified for preferably Tier IV Data Center (Fault Tolerant) and shall at least be minimum Tier III (Concurrently Maintainable)

5.5.4 The Data Centres(DCs) & Disaster Recovery(DR) sites are to be located in seismic zone II.

5.5.5 The location of disaster recovery site shall at least be based on the following criteria:

a) Minimum influence by natural disasters - Cyclones, Earthquakes and Floods.

b) Minimum influence by man made disasters - Fire, terrorist strike, labour strikes.

c) Distance from the primary site - As far as possible so that catastrophe does not strike at both the sites.

5.5.6 Roles and responsibilities with reasonable allocation shall be defined for DC and DR.

5.5.7 Quarterly periodic reviews and audit, quarterly trainings and half-yearly mock drill of the employees for resuming the operations from the DR site should be done.

5.5.8 Back up:

a) 3 – Keep 3 copies of any important file: 1 primary and 2 backups.

b) 2 – Keep the files on 2 diferent media types to protect against different types of hazards.

c) 1 – Store 1 copy offsite (e.g., offline at remote location)

d) The department shall maintain Backup register that contains complete records of the backup copies such as Site location, Device type, Name, Backup type, frequency, Backup location, date etc to be given.

5.5.9 Continuous monitoring: The comprehensive log collection and immutable storage platform (e.g. syslog server) should be established. The log management platform shall be used to identify the incident, incident response, post incident analysis, threat hunting and forensics. The log shall be sumitted to NCIIPC every quarterly. The real time monitoring and analysis of the logs should be done. The DC & DR shall be configured with at least two synchronized time sources. The time synchronization must be done using Network Time Protocol Server of National Informatics Center (NIC) or National Physical Laboratory (NPL).

5.5.10 No remote access to be provided to Stationary KAVACH entities and KAVACH OEMs should get their systems tested for VAPT and get it certified. Any incident occurring should be reported to the Zonal Railway Officer for further action. The prospective bidder shall submit template for this service including the penalties and payment structure.

5.6 **Typical Overview of Cyber Security Case: The followings shall be taken care off while conducting test cases.**

5.6.1 System under Consideration definition (Includes Zones and Conduits)

5.6.2 **Threat and risks assessment.**

i. Assumption
ii. List of threat intelligences sources
iii. List of threat Scenarios
iv. List of sufficiently mitigated risks (with explanation)
v. Cyber security Requirement Specification (CRS) (could be a set of references to other documents).

5.6.3 **Assumptions**

i. Cybersecurity needs (including safety-related high level objectives
ii. Cybersecurity requirements
iii. List of open risks (with explanation)
iv. Cybersecurity management (Could be a set of references to other

documents)

v. Cybersecurity policy

vi. Cybersecurity plan

vii. Cybersecurity process

viii. Vulnerability assessment and management

ix. Cybersecurity fulfillment (could be a set of references to other documents

5.6.4 Implementation of cybersecurity measures – evidences of fulfillment of CRS

5.6.5 Evidence of application of cybersecurity process

5.6.6 **Verification & validation results**

i. Testing of security measures (e.g. V&V, Penetration testing)

ii. Traceability to cybersecurity requirements.

5.6.7 Related cyber security cases (from included components or subsystems, if any.

5.6.8 Security-related application condition (could be a set of references to other documents)

i. Installation

ii. Maintenance

iii. Operation

5.7 **Conclusion**

i. Cybersecurity claim

ii. Residual risks status

5.8 **Security cases to meet the mitigation of threat shall adopt mechanism as below:**

i. Unique and authentication

ii. Multi Factor authentication for untrusted network

iii. Multi Factor authentication for all network

iv. Identification and authentication of software processes and devices

5.9 Safety Case shall refer to the cyber security report. ISA shall allow

update of Cybersecurity cases without change of safety cases.

5.10 Risks for Cybersecurity assessment shall be done in concept phase, System Definition phase, Risk Analysis phase and Counter Measures shall be planned in System Requirements phase.