Rail Security Expert Group

Procurement Guideline

23E176
1A
03.04.2024

Modification history

Version	Date	Modification / Description	Editor
0A	30.10.2023	Final draft after internal review	Christof Jungo, Roger Metz, Richard Poschinger, Nicolas Poyet, Max Schubert, Juhana Yrjölä
1A	03.04.2024	Final version after external review	Christof Jungo, Roger Metz, Richard Poschinger, Nicolas Poyet, Max Schubert, Juhana Yrjölä

Table of Contents

1 Introduction 5
1.1 Scope 5
1.2 References 5
1.3 Abbreviations 6
1.4 Authors 6
1.5 Applicability and Document Status 7
1.6 Definition of Requirement Types 7
2 Legal aspects 8
2.1 Rationale 8
2.2 Requirements 8
3 Audit 9
3.1 Rationale 9
3.2 Requirements 9
4 Lifecycle description 10
5 Procurement Styles 12
6 Implementation, Manufacture, FAT, Development 13
7 Transport 13
7.1 Rationale 13
7.2 Requirements 14
8 Integration 14
8.1 Rationale 14
8.2 Requirements 15
9 Validation 15
9.1 Rationale 15
9.2 Requirements 15
10 SAT and Commissioning 16
10.1 Rationale 16
10.2 Requirements 16
11 Vulnerability and Patch Management 17
11.1 Rationale 17
11.2 Requirements 17
12 Business Continuity Management 19
12.1 Rationale 19
12.2 Requirements 19
13 Decommissioning 21
13.1 Rationale 21
13.2 Requirements 21

Table of Figures

Figure 1: Lifecycle Process.....11

1 Introduction

1.1 Scope

1.1.1.1 The document is designed for (but not limited to) the CCS+ scope defined by the EU RAIL System Pillar.

1.1.1.2 The purpose of this document is to define a guideline for the tender process to ensure similar approach, requirements, and solutions in Europe. These requirements may be used in every tender process or contract to allow similarity in service and quality.

1.1.1.3 This document does not cover physical access management for external personnel.

1.1.1.4 This document does not cover aspects like e.g., warranty or service lifetime.

1.2 References

1.2.1.1 Subsets and EUG publication are referenced directly with their corresponding ID.

1.2.1.2 At the moment, of finalisation of this document the IEC 63452 was not published and still under review and modification. Thus, an alignment was not possible. The alignment for consistency will be performed in a future version of the document after IEC 63452 is published.

1.2.1.3 Other referenced documents:

[1] “RFC 2119,” 1997. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2119.

[2] „NIS2,“ [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555.

[3] „Cyber Resilience Act,“ [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act.

[4] „Cyber Security Act,“ [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881.

[5] „EN 50126-1:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)“.

[6] IEC 62443-4-1:2018 Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.

[7] „IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers“.

[8] „IEC 62443-3-3:2019 Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels“.

[9] „ISO IEC 27036-3;2023 Cybersecurity - Supplier Part 3 - Guidelines for hardware, software, and services supply chain security“.

[10] „Good Practices for Supply Chain Cybersecurity,“ [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity.

[11] „ISO 22301:2019 Security and resilience - Business continuity“.

1.3 Abbreviations

BCM ..... *Business Continuity Management*
BCP ..... *Business Continuity Plan*
BIA ..... *Business Impact Analysis*
EFTA ..... *European Free Trade Association*
SAT ..... *Site Acceptance Test*

ERTMS Abbreviations are listed in SUBSET-023

1.4 Authors

1.4.1.1 The Rail Security Expert Group (RSEG) consists of security experts of the following groups:

- ERTMS Security Expert Group (ESCG) – Part of the EEIG ERTMS Users Group
- EULYNX Security Cluster – Part of the EULYNX Initiative

1.4.1.2 The following members of the Rail Security Expert Group were involved in creating this document.

- ERTMS User Group (EUG)
  - Max Schubert
  - Richard Poschinger
  - Roger Metz
- SBB
  - Christof Jungo
- SNCF
  - Nicolas Poyet
- Fintraffic
  - Juhana Yrjölä

1.5 Applicability and Document Status

1.5.1.1 To ensure the usability for tender documents, this document is using classifications and requirement key words. This classification does not result in any binding requirements for members of the EUG or other involved parties. The documents will be updated in the future to be adapted to a changed threat landscape, updated standards, and newly developed security solutions.

1.6 Definition of Requirement Types

1.6.1.1 This document uses key words indicating requirement levels according to RFC 2119 [1]. Each clause in this document is classified as follows:

M	Mandatory	function must be implemented as specified
R	Recommendation	function must be implemented as specified, but there may exist valid reasons in particular circumstances to ignore a particular requirement, but the full implications must be understood and carefully weighed and documented before choosing a different course.
O	Optional	not mandatory, must be as specified if implemented (not applied in the document)
I	Informative	included for clarification purposes only

Texts without a tag do not constitute a requirement.

2 Legal aspects

2.1 Rationale

2.1.1.1 The following EU legislations apply regarding cyber security: **(I)**

- NIS 2 directive [2]
- Cyber Resilience Act [3]
- Cyber Security Act [4]

2.1.1.2 In this specific context, business related security aspects such as GDPR are not treated. **(I)**

2.1.1.3 Definition: On-Premises cloud services means that the cloud is under full control, owned and operated by either the supplier or the railway and it is located at a facility that is owned either by the supplier or the railway. **(I)**

2.2 Requirements

2.2.1.1 The supplier shall declare that all its infrastructure (technical or organizational) that are used to provide the requested services are located in the EU and EFTA countries. This especially includes but is not limited to: **(M)**

- Data centre, e.g., for cloud solutions
- Asset Management
- Configuration and Software Management
- Spare part warehouse

2.2.1.2 If cloud services for safety relevant or related systems are required, the supplier shall only use on-premises cloud services for this purpose. **(M)**

2.2.1.3 If cloud services for safety relevant or related test systems are required, the supplier should use on-premises cloud services for this purpose. **(R)**

2.2.1.4 If a cloud service for safety relevant or related test systems is located at a third-party location, the supplier shall ensure that confidentiality of all data and information in rest and motion is ensured. **(M)**

2.2.1.5 If a cloud service for safety relevant or related test systems is located at a third-party location and the test results are used for homologation, the supplier shall ensure that integrity of all data and information in rest and motion is ensured. **(M)**

2.2.1.6 The supplier shall include the clauses of these requirements in its subcontracting and co-contracting agreements (current and future) to ensure their effective implementation. **(M)**

2.2.1.7 The supplier shall be able to demonstrate compliance to the requirements of this documents throughout the lifetime of the services he delivers. **(M)**

2.2.1.8 The supplier shall notably perform regularly assessments and provide the results of these assessments both at the request of the railway operator and regularly in the form of an up-to-date dashboard. **(M)**

3 Audit

3.1 Rationale

3.1.1.1 Audits proof the compliance to requirements. These requirements are coming from legal aspects, norms and standards as well as contractual requirements. **(I)**

3.1.1.2 The cost of security checks (e.g. "vulnerability scan", "computer intrusion test") is borne by the customer. However, the cost incurred by the participation of the supplier's staff in the controls remains at the supplier's expense. **(I)**

3.2 Requirements

3.2.1.1 The supplier should do self-assessments and provide evidence to the customer to proof the compliance. In addition, by good reason, the customer may ask for the right to audit. This request should be accepted by the supplier to proof the compliance independently. **(R)**

3.2.1.2 The supplier shall allow the customer to perform security checks (e.g. "vulnerability scan", "computer intrusion test") on the supplier's system. **(M)**

3.2.1.3 The supplier shall specify the notice period for such security checks. **(M)**

4 Lifecycle description

4.1.1.1 Figure 1 shows the lifecycle used in this document. The figure is split into three different responsibilities: **(I)**

- National Safety Authority (green)
- Supplier (red)
- Customer (blue)

Solid lines with arrows show dependencies between the different steps according to the CENELEC EN50126 [5] process.

Dashed lines highlight that aspects of these processes need to be part of a requirement document either for the customer or the supplier.

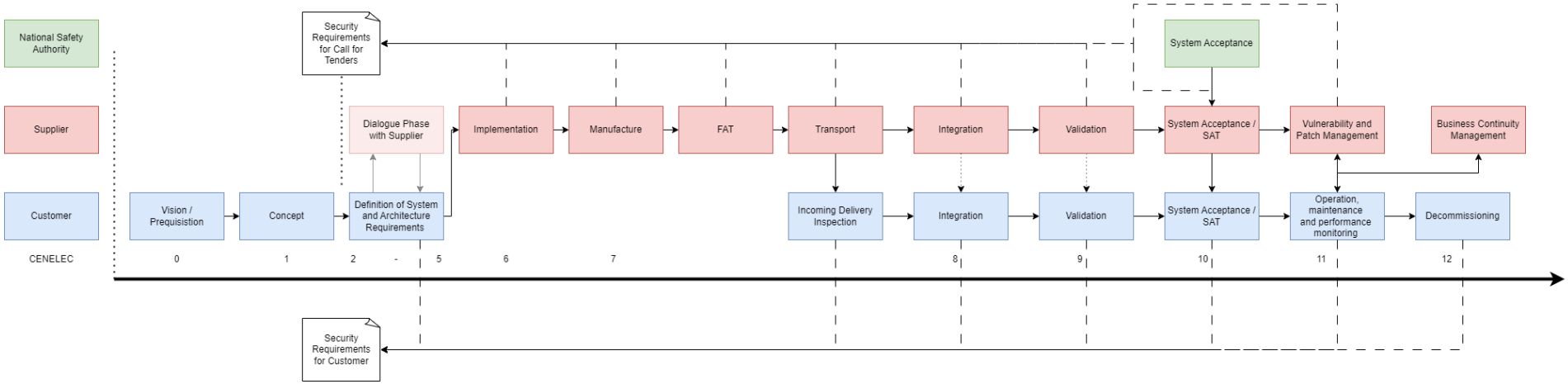

Figure 1: Lifecycle Process

5 Procurement Styles

5.1 Rationale

5.1.1.1 The tender processes for railways are bound to European procurement regulations, which require compliance with the principles of transparency, non-discrimination, equal treatment, and proportionality. **(I)**

5.1.1.2 To allow the railways to get an overview over the supplier capabilities on the market, a dialogue with the potential suppliers might be required. To be compliant with European law the following rules and steps are taken into consideration: **(I)**

1. Define the system under procurement with all relevant requirement specifications, e.g., the EULYNX Security Specification Baseline 4 Release 2.
2. Define a reasonable set of questions to the potential suppliers that allow to get an insight to the available solutions and capabilities on the market.
3. Publish a request for information (benchmarking) for the defined system to publish the plan to go for tender for the defined system together with the prepared question combined with the invitation for a dialogue phase.
4. Accomplish the dialogue phase with each applicant. The answers to the questions can stay confidential.
5. Adopt, correct, specify in more detail the requirements of the system based on the gained insights and experience.
6. Go for tendering phase.

5.1.1.3 The railway can exclude suppliers which do not fulfil the moral codex by requiring the compliance with the following requirements (this list is not complete): **(I)**

- No violation of the UN embargo and European or national sanctions regulations
- Delivery of spy equipment to countries or organisations that do not comply with human rights.

5.2 Requirements

5.2.1.1 If the supplier is currently not able to comply with the security requirements, one or the combination of multiple of the following measures shall apply: **(M)**

1. The supplier presents a migration plan towards fulfilment with time and full cost overview including a time limit.
2. The supplier presents mitigating measures that reach the same level of security protection. This might include own- or third-party solutions.

6 Implementation, Manufacture, FAT, Development

6.1 Requirements

6.1.1.1 The supplier of products shall declare compliance with IEC 62443-4-1 [6] for the development of the offered products. **(M)**

6.1.1.2 The supplier should document and provide evidence of the maturity level (according to the IEC 62443-4-1) he has reached. **(R)**

6.1.1.3 The supplier shall declare to include the compliance with IEC 62443-4-1 [6] and IEC 62443-2-4 [7] in its subcontracting and co-contracting agreements. **(M)**

6.1.1.4 The supplier shall provide proof regarding the compliance to standards by certification from an accredited certification body. **(M)**

6.1.1.5 The supplier shall declare to be compliant to the technical security requirements mentioned in the tender. **(M)**

6.1.1.6 The supplier shall demonstrate that the tools and services made available to the customer comply with the rules of secure development as requested in the tender. **(M)**

6.1.1.7 The supplier shall protect its development environment from malicious attacks and potential supply chain attacks. **(M)**

7 Transport

7.1 Rationale

7.1.1.1 Transport means the physical transport (delivery) from the supplier to the customer. **(I)**

7.1.1.2 Security measures during the transportation phase are required to ensure that the cybersecurity of the component/system is maintained for the period of shipping until start of operation. **(I)**

7.1.1.3 In the time the component or system has left the trusted environment of the supplier/manufacturer, it is in an unsecure environment. At the same time all security functions, that work in operation, as security logging, secure boot, etc. are not active as the system is not in operation. In this period, it would be possible, in general, to modify or manipulate the component/system. To either avoid or detect such malicious modifications, measures of supply chain security are recommended. **(I)**

7.1.1.4 Knowledge about the current threat landscape, tampering trials and attacks is crucial to evaluate the current criticality and threat landscape. **(I)**

7.1.1.5 For the software and configuration, it is assumed that they are downloaded after commissioning at its installation destination. **(I)**

7.1.1.6 The following requirements are based on IEC 62443 [8], IEC 27036-3 [9] and best practices from ENISA [10]. **(I)**

7.2 Requirements

7.2.1.1 The supplier shall protect the system/component from tampering during the delivery phase with suitable measures. **(M)**

7.2.1.2 The supplier shall integrate an electronic tamper detection mechanism which detects physical access to all components. **(M)**

7.2.1.3 The supplier shall notify the customer of any tamper detection on a component or system that was delivered to the customer. **(M)**

7.2.1.4 The supplier shall notify each customer of a specific component or system of any tamper detection on that component or system that was delivered to any other customer. **(M)**

7.2.1.5 The supplier shall notify each customer of a specific component or system of any theft of that component or system that was delivered to any other customer. **(M)**

7.2.1.6 The supplier shall provide secure proof of change history to the customer to allow him to transparently prove authorization and verification before download and implementation. **(M)**

7.2.1.7 The supplier shall allow independent continually compliance check of the success of the protections within the agreement. **(M)**

7.2.1.8 The supplier shall check and provide evidence of code inspection of sub-supplier's code that is integrated in the component/system. **(M)**

7.2.1.9 The supplier shall ensure that subcontractors are aware of and comply with the requirements of Chapter 7.2 when participating in the supply of goods or services to be procured. **(M)**

7.2.1.10 The supplier shall provide information about the transportation path for traceability to the customer. **(M)**

8 Integration

8.1 Rationale

8.1.1.1 The process of integration differs a lot depending on the split of responsibilities between the operator, supplier, service provider and integrator. In Europe, the customer has currently multiple different set-ups which have the whole set-up from turn-key project to taking the integration role themselves and providing detailed input for requirements documents, test cased, homologation and test accomplishment. **(I)**

8.1.1.2 The whole process of the integration runs via multiple phases in the V-model [5]. The integration starts with the corresponding requirements at the system's interfaces and goes on with the testing in the test lab where the systems are technically integrated for the first time. After successful testing the systems are installed at site and the site integration testing is performed. This is the last step of the integration process. **(I)**

8.1.1.3 Technical specifications may be detailed but usually additional knowledge is needed to successfully perform testing and integration. The supplier provides this information. **(I)**

8.2 Requirements

8.2.1.1 All information which are provided shall be free for use to fulfil the integration task. Even if it is “secret” knowledge it must made available to perform the task. If that’s not fulfilled, the supplier or the supplier’s solution shall not be accepted. Appropriate non-disclosure agreements between the parties are assumed. **(M)**

8.2.1.2 Every party that is part of the integration task should provide all technical specifications needed to successfully accomplish that task. **(R)**

8.2.1.3 The supplier shall provide relevant specification for an integration task. **(M)**

8.2.1.4 The supplier shall provide relevant information, e.g., descriptive documents, for an integration task. **(M)**

8.2.1.5 The supplier shall provide additional know-how from experts, if needed, for an integration task. **(M)**

8.2.1.6 The supplier of integration services shall declare compliance with IEC 62443-2-4 [7] for the offered services during life cycle as a service supplier. **(M)**

8.2.1.7 The supplier should document and provide evidence of the maturity level (according to the IEC 62443-2-4) he has reached. **(R)**

9 Validation

9.1 Rationale

9.1.1.1 Validation has two main parts. The final validation is the document-based validation. A pre-condition is the validation testing to proof the planned behaviour. For the document-based validation the standard process in railways can be applied. For testing, the validation can be split in two parts again: **(I)**

- Functional Testing – Testing of the planned behaviour
- Penetration Testing – Testing the system to find possible vulnerabilities and check its resilience against attacks.

9.1.1.2 Ideally, a complete system set-up is available in the test lab or in connected test labs. In practice, it is taken into consideration that a full system set-up might be difficult due to the complexity of the system. As a minimum goal for the functional testing, every connection is tested at least separately. **(I)**

9.1.1.3 The pre-condition for functional testing is a test case specification. **(I)**

9.1.1.4 The pre-condition for penetration testing is a test lab that allows easy access to the connections. **(I)**

9.2 Requirements

9.2.1.1 The functional tests should be performed in a test lab. **(R)**

9.2.1.2 The supplier shall provide real equipment for testing of security features and penetration testing in a test laboratory. **(M)**

9.2.1.3 For penetration testing the Penetration Testing Guideline should be used (23E245) **(R)**

9.2.1.4 The supplier shall provide all available documentation relevant for testing of security features and penetration testing. This shall be, but is not limited to: **(M)**

- Test methodology
- Inventory list
- Tool list
- Test tool list
- Configuration documentation
- Role list

10 SAT and Commissioning

10.1 Rationale

10.1.1.1 The site acceptance and commissioning process is structured in four main steps: **(I)**

1. Setting the system into a functional working mode - Establishment of the function.
2. Perform Site Acceptance Test (SAT).
3. Perform the final checks from the Approver.
4. Set the system into formal operation.

10.1.1.2 In many cases the site test is the first time when real end-to-end test can be performed as all systems that are interacting are working together. This includes the successful integration of services like SIEM, PKI, TIME the safety systems themselves and services for maintenance and diagnostics. **(I)**

10.1.1.3 The supplier has the responsibility for the system until the successful handover is documented. **(I)**

10.1.1.4 If the site acceptance test had open points (unsuccessful tests) the customer has the right to reject the handover (shift of responsibility) partly or complete. **(I)**

10.2 Requirements

10.2.1.1 The supplier shall support the site acceptance test with relevant knowledge support to allow quick resolve of any upcoming conflicts. **(M)**

10.2.1.2 The supplier shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during SAT. This shall cover all security functions required by the security requirements specifications referenced by this document. **(M)**

10.2.1.3 The supplier shall provide the capability to employ automated mechanisms to support management of security verification during SAT. This shall cover all security functions required by the security requirements specifications referenced by this document. **(M)**

10.2.1.4 The supplier shall support digital documentation of all tests to support documented handover, including open points lists. **(M)**

11 Vulnerability and Patch Management

11.1 Rationale

11.1.1.1 The vulnerability and patch management process from a customer view starts after the responsibility of the system has been transferred from the supplier to the customer. **(I)**

- Supplier continuously checks for vulnerabilities of provided system.
- Supplier identifies vulnerability affecting the system.
- Supplier checks impact of vulnerability and if an impact on safety is possible.
- Supplier assesses:
  - Temporary mitigating measures
  - Patch strategy to fix the security issue
- Supplier informs customer about the mitigation and patch strategy.
- Customer defines implementation and schedule of temporary mitigating measures
- Supplier and customer test the mitigating measure.
- Patch rollout to fix the security issue
- Supplier performs necessary tests for the patch
- Supplier provides patch and installation details
- Customer implements mitigation and patch rollout

11.1.1.2 The usual process for putting a system in operation for a customer (homologation) is also relevant for the patch rollout procedures but is not completely covered in the process described above. **(I)**

11.1.1.3 The supplier is required to offer security patches over the expected lifetime of the product. Additional details regarding continuous service and maintenance can be added to the tender. **(I)**

11.2 Requirements

11.2.1.1 The supplier shall agree on systematic repeatable vulnerability response processes with the customer. **(M)**

11.2.1.2 The supplier shall provide insights to the customer on how the vulnerability detection is implemented. **(M)**

11.2.1.3 The supplier shall provide a system without any known vulnerabilities before SAT. **(M)**

11.2.1.4 The supplier shall provide spare parts without any known vulnerabilities before shipping to the customer. **(M)**

11.2.1.5 The supplier shall provide information about the impact on safety of the vulnerability. **(M)**

11.2.1.6 The supplier shall provide CVE reference, if applicable. **(M)**

11.2.1.7 The supplier shall provide CVSS v.4 score to the customer regarding the vulnerability (independent if it is published or not). **(M)**

11.2.1.8 The supplier shall provide a patch strategy to fix security issues. **(M)**

11.2.1.9 The supplier shall provide a patch strategy which contains a realistic implementation schedule of a patch, and temporary mitigating measures that needs to be agreed on with the customer. **(M)**

11.2.1.10 The supplier shall test every patch before its deployment at the customer's. **(M)**

11.2.1.11 The supplier shall provide the patch in time according to the schedule in the patch strategy. **(M)**

11.2.1.12 The supplier shall provide required installation details about the patch. **(M)**

11.2.1.13 The supplier shall provide the patches with the complete set of security test documentation. **(M)**

11.2.1.14 The supplier shall provide the customer with the ability to ensure that patch has been successfully installed and cyber security threat has been mitigated. **(M)**

12 Business Continuity Management

12.1 Rationale

12.1.1.1 The Business Continuity Management (BCM) guarantees the availability of the system. The process is designed and maintained by the customer and covers aspects beyond the security scope. **(I)**

12.1.1.2 The BCM can be defined based on ISO 22301 [11]. **(I)**

12.1.1.3 Prerequisite for the BCM process is a Business Impact Analysis (BIA) provided by the responsible department. **(I)**

12.1.1.4 Procurement process takes the Business Continuity Plan (BCP) and BIA into account when procuring new systems and capabilities to ensure proper levels of business continuity. **(I)**

12.1.1.5 The security-related part of the BCM process consists of the following aspects: **(I)**

- Full BCM for
  - Shared Security Services
  - Decentralized security-related components (e.g. hardware firewalls, application level gateways, IDS/IPS)
  - Provide Recovery Plan
- For other business critical services (OT)
  covered by amongst other RAMS
  (for example: Maximal Tolerable Downtime, Maximum Allowable Data Loss...)
  - Maintain list of essential services required to guarantee railway operation
    (including mappings of services to component
    and mappings of impacts of security functionalities to services)
  - Provide security knowledge and service for the OT critical services
  - Support recovery plan for the OT critical services
- Definition of overall process for recovery including a business continuity management team (security incident management team in security language) which is built following a strict process if an according event occurs.
- Integration of CSIRT of the organisation/customer according to NIS 2 directive

12.2 Requirements

12.2.1.1 The BIA should consider the criticality of processes for railway operation. **(R)**

12.2.1.2 The supplier shall provide a hotline to address security incidents with an availability (e.g., 24/7) defined by the customer in the BCM process. **(M)**

12.2.1.3 The supplier shall provide a contact to relevant security and OT experts within a timespan (e.g., 2 hours) defined by the customer in the BCM process after initial support request. **(M)**

12.2.1.4 The supplier shall provide an on-site security and OT expert within a timespan (e.g., 8 hours) defined by the customer in the BCM process after initial support request. **(M)**

12.2.1.5 The supplier shall confirm and prove in a suitable manner that the supplier has a BCM himself to guarantee the agreed support remote and on-site in case of a BCM case of the customer. **(M)**

12.2.1.6 The supplier shall provide spare parts after request according to the service level agreement within a timespan (e.g., 24 hours) defined by the customer in the BCM process. **(M)**

12.2.1.7 The supplier shall support the design and definition of the BCM process with technical and procedural knowledge for the provided before delivery and installation. **(M)**

12.2.1.8 The supplier shall provide information about the availability of backups. **(M)**

12.2.1.9 The supplier shall provide technical and procedural knowledge to support the writing of playbooks and handbooks for reaction and recovery after security incidents. **(M)**

12.2.1.10 The supplier shall support BCM simulation and training. **(M)**

12.2.1.11 The supplier shall review, test, and update its BCM process on a regular basis, defined by the customer, at least every third year. The results of these tests and exercises shall be formalized and presented to the customer. **(M)**

13 Decommissioning

13.1 Rationale

13.1.1.1 The decommissioning of a component starts triggered by the customer if **(I)**

- the component is broken and taken out of operation for repair
- the component is finally decommissioned because e.g.,
  - it is replaced
  - the system is going out of operation

13.1.1.2 The following process is implemented: **(I)**

- Customer decides to decommission a component
- Customer informs affected parties about decommissioning
  - for planned decommissioning according to a defined notice period
- Component is put out of operation
- Components access rights removed, certificates are revoked, and network access is revoked
- Component is marked as decommissioned in the asset management
- Component is physically disconnected
- If logs are not centrally stored, these need to be extracted and saved if needed according to legal requirements
- Component memory is purged
- Component is
  - sent to repair (and afterwards used as spare part or put in operation)
  - Or disposed
- The application of this process is documented (report) and verified.

13.2 Requirements

13.2.1.1 The supplier shall provide manuals for purging of memory. **(M)**

13.2.1.2 The supplier shall provide the customer with the ability to verify the successful execution of the purging process. **(M)**