OCORA

Open CCS On-board Reference Architecture

Cybersecurity testing strategy

Document ID: OCORA-TWS09-050

Version: 1.00

Date: 07.12.2022

Management Summary

This document aims to define the test strategy from a cybersecurity perspective. It addresses the testing objectives. It proposes an overview of the test to perform across the system lifecycle. It lists the different type of assessment. It identifies resource and characteristic of tests facilities. Finally, it proposes a brief list of specific tests relevant in the OCORA context. This document was reviewed jointly by TWS09 Testing and TWS06 cybersecurity

Revision history

Version	Change Description	Initial	Date of change
1.00	▪ Official version for OCORA Release R3	MT	07/12/2022

Table of contents

References

Reader’s note: please be aware that the numbers in square brackets, e.g. [1], as per the list of referenced documents below, is used throughout this document to indicate the references to external documents. Wherever a reference to a TSI-CCS SUBSET is used, the SUBSET is referenced directly (e.g. SUBSET-026). OCORA always reference to the latest available official version of the SUBSET, unless indicated differently.

[1] OCORA-BWS01-010 – Release Notes

[2] OCORA-BWS01-020 – Glossary

[3] OCORA-BWS01-030 – Question and Answers

[4] OCORA-BWS01-040 – Feedback Form

[5] OCORA-BWS03-010 – Introduction to OCORA

[6] OCORA-BWS03-020 – Guiding Principles

[7] OCORA-BWS04-010 – Problem Statements

[8] OCORA-BWS05-010 – Road Map

[9] OCORA-TWS01-030 – System Architecture

[10] OCORA-TWS01-035 – CCS On-Board (CCS-OB) – Architecture

[11] OCORA-TWS06-030 – (Cyber-) Security – Concept

[12] OCORA-TWS09-010 – Testing – Strategy

[13] TS 50701 - Railway applications – Cybersecurity

[14] IEC 62443 - Industrial communication networks - Network and system security

1 Introduction

1.1 Purpose of the document

The purpose of this document is to define the cybersecurity testing strategy in the context of the OCORA project.

This document is addressed to experts in the CCS domain and to any other person, interested in the OCORA concepts for on-board CCS. The reader is invited to provide feedback to the OCORA collaboration and can, therefore, engage in shaping OCORA. Feedback to this document and to any other OCORA documentation can be given by using the feedback form [4].

If you are a railway undertaking, you may find useful information to compile tenders for OCORA compliant CCS building blocks, for tendering complete on-board CCS system, or also for on-board CCS replacements for functional upgrades or for life-cycle reasons.

If you are an organization interested in developing on-board CCS building blocks according to the OCORA standard, information provided in this document can be used as input for your development.

1.2 Applicability of the document

The document is currently considered informative but may become a standard at a later stage for OCORA compliant on-board CCS solutions. Subsequent releases of this document will be developed based on a modular and iterative approach, evolving within the progress of the OCORA collaboration.

1.3 Context of the document

This document is published as part of an OCORA Release, together with the documents listed in the release notes [1]. Before reading this document, it is recommended to read the Release Notes [1]. If you are interested in the context and the motivation that drives OCORA we recommend reading the Introduction to OCORA [5], the Guiding Principles [6], the Problem Statements [7], and the Road Map [8].The reader should also be aware of the Glossary [2] and the Question and Answers [3].

2 Cybersecurity objectives

Cybersecurity testing aims to give confidence that the system under test reaches the requested level of security performance.

The requested level of security is provided through the risk assessment process which conducts to identify the requirement and additional protection that the system shall implement. The testing process aims to verify that the system implements these requirements and provide confidence that the system can face the identified risk.

Cybersecurity testing is a cross domain which applies on all components of a system for which requirements or protection are required (Security level SL ≥1)

Due to system complexity, tests are only a sample of all situations that the system can face. The coverage of tests shall also consider the difference between testable and non-testable requirement and the clear distinction between functional proof and penetration testing as a practical method to measure the resilience against cyber attacks

The effort and the complexity of the tests have to be estimated and defined accordingly to the level of security that is assessed and the level of confidence to be achieved.

As there is no formal method to demonstrate compliance, the tester is not subject to an obligation of results but more to an obligation of means. The results of the tests are valid at the time they are executed according to the level of threat and exposure of the system. But this must be challenged throughout the lifecycle of the system.

The duration of penetration testing should be prioritized on the level of exposition for subsystem to an attack and proportionally aligned with the resilience needs in front of an attack / with the security level target.

3 Cybersecurity standard

The standard TS 50701 defines the activities relative to cybersecurity assurance and system acceptance for operation (§9)

The output of the testing activities feeds into the cybersecurity case (§9.2)

The TS 50701 is inherited from the IEC 62443. The 62443-4-1 defines the security verification and validation tests for products. Especially the types of tests are:

- Functional test
- Performance test
- Limit test, constraint, wrong forged or unexpected input

4 Cybersecurity SuC scope

The “System under Consideration” scope is defined on the system architecture [1] and [10]. It is composed of the CCS On board, the Shared Cybersecurity services, the Security Gateway, Train to Ground communication (FRMCS included)

Following principles defined in TS 50701, the security concept [11] defines the zones and conduits by gathering component-based criteria. The coherence of security level is one of these criteria. Zones are connected to each other through conduits.

The following zones are defined:

- CCS (red)
- Train adapter (orange)
- JRU (light blue)
- MNT (dark blue)
- CSS and SecGW (purple)
- Communication (green)

Furthermore, OCORA defines the concept of building block in [1]. A building block is a sourceable unit of the CCS on-board system (hardware and/or software). Each building block can be provided by different suppliers.

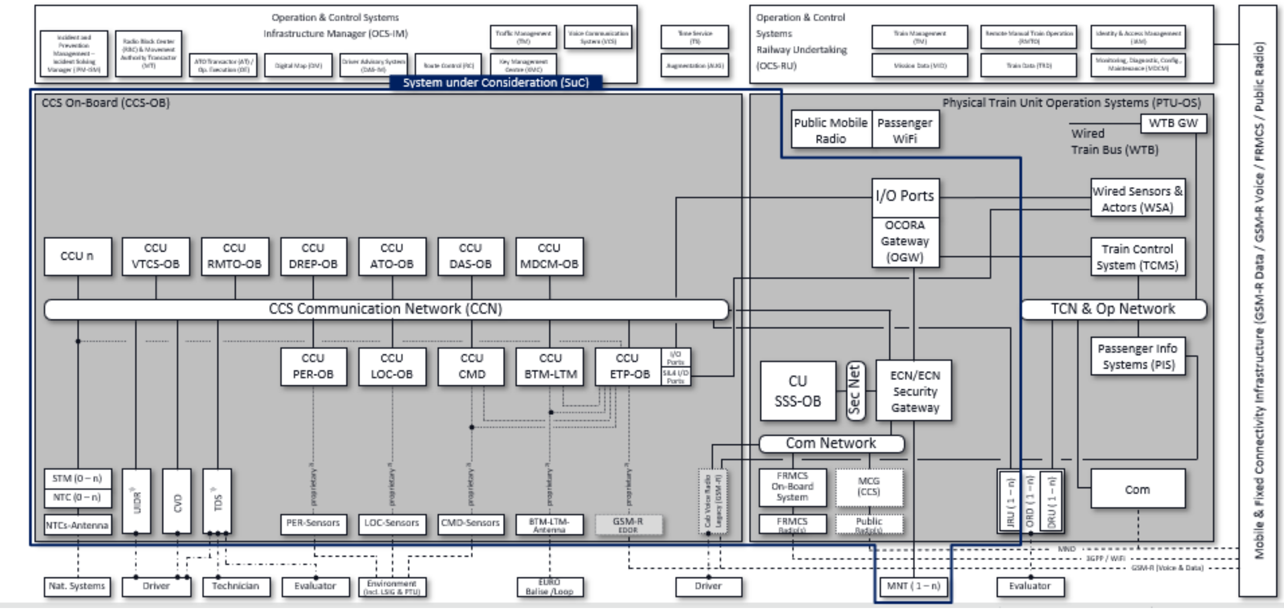
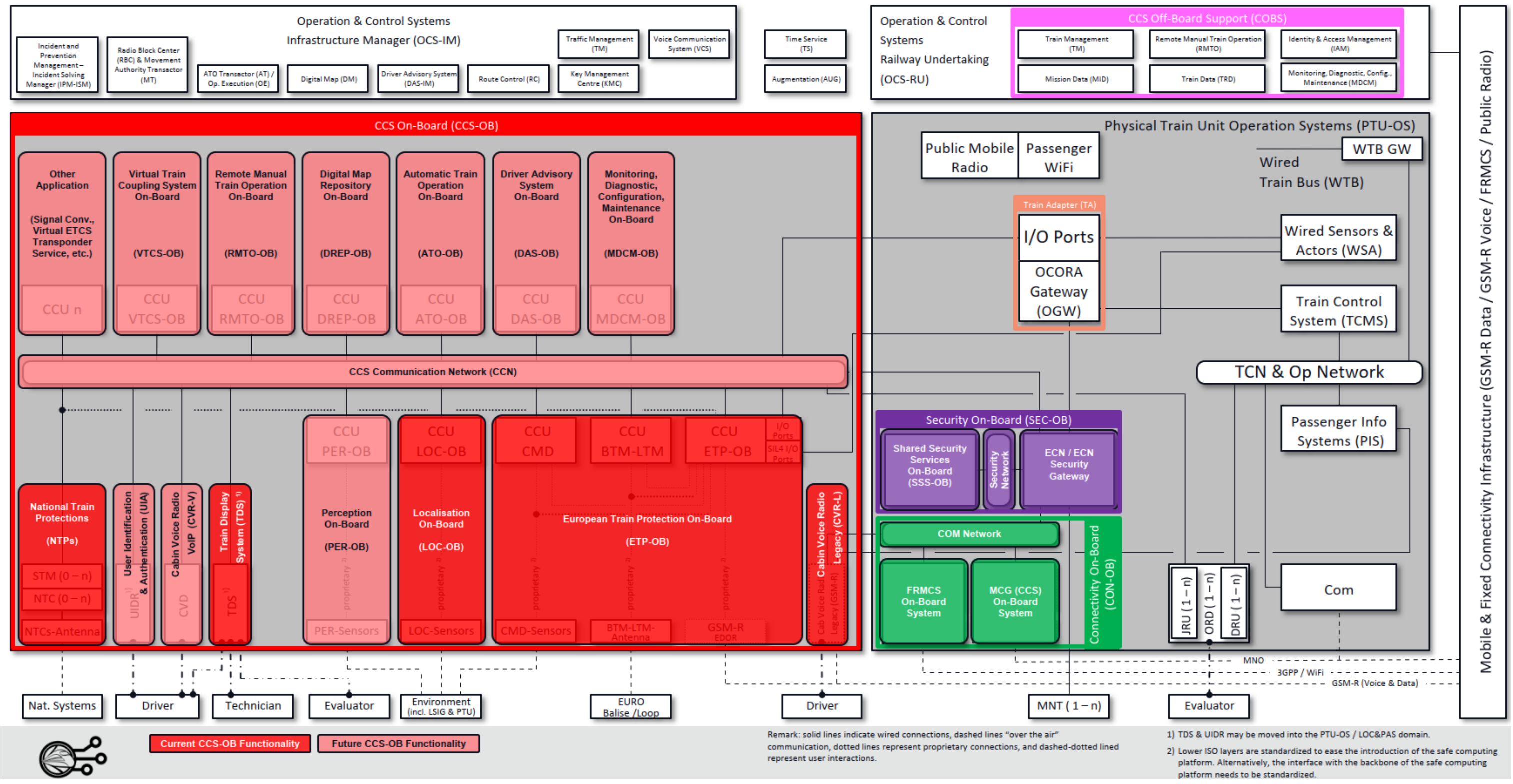

Operation & Control Systems
Infrastructure Manager (OCS-IM)
Incident and Prevention Management – Incident Solving Manager (PM-ISM)
Radio Block Center (RBC) & Movement Authority Transactor (MT)
ATO Transactor (AT) / Op. Execution (OE)
Digital Map (DM)
Driver Advisory System (DAS-IM)
Route Control (RC)
Traffic Management (TM)
Voice Communication System (VCS)
Key Management Centre (KMC)
Time Service (TS)
Augmentation (AUG)
Operation & Control Systems Railway Undertaking (OCS-RU)
Train Management (TM)
Remote Manual Train Operation (RMTO)
Identity & Access Management (IAM)
Mission Data (MD)
Train Data (TD)
Monitoring, Diagnostic, Config., Maintenance (MDCM)
System under Consideration (SuC)
CCS On-Board (CCS-OB)
Physical Train Unit Operation Systems (PTU-OS)
Public Mobile Radio
Passenger WiFi
WTB GW
Wired Train Bus (WTB)
I/O Ports
OCORA Gateway (OGW)
Wired Sensors & Actors (WSA)
Train Control System (TCMS)
CCU n
CCU VTCS-OB
CCU RMTO-OB
CCU DREP-OB
CCU ATO-OB
CCU DAS-OB
CCU MDCM-OB
CCS Communication Network (CCN)
TCN & Op Network
CCU PER-OB
CCU LOC-OB
CCU CMD
CCU BTM-LTM
CCU ETP-OB
I/O Ports
SIL4 I/O Ports
CU SSS-OB
Sec Net
ECN/ECN Security Gateway
Passenger Info Systems (PIS)
Com Network
STM (0 – n)
NTC (0 – n)
NTCs-Antenna
UIDR
CVD
TDS
proprietary
PER-Sensors
LOC-Sensors
CMD-Sensors
BTM-LTM-Antenna
GSM-R EDOR
Cab Voice Radio Legacy (GSM-R)
FRMCS On-Board System
FRMCS Radio(s)
MCG (CCS)
Public Radio(s)
JRU (1 – n)
ORD (1 – n)
DRU (1 – n)
Com
MND
3GPP / WiFi
GSM-R (Voice & Data)
Nat. Systems
Driver
Technician
Evaluator
Environment (incl. LSIG & PTU)
EURO Balise /Loop
Driver
MNT (1 – n)
Evaluator
Mobile & Fixed Connectivity Infrastructure (GSM-R Data / GSM-R Voice / FRMCS / Public Radio)

Figure 1: System under Consideration and Zoning - Physical Architecture - Transition View


Operation & Control Systems
Infrastructure Manager (OCS-IM)
Incident and Prevention Management – Incident Solving Manager (IPM-ISM)
Radio Block Center (RBC) & Movement Authority Transactor (MT)
ATO Transactor (AT) / Op. Execution (OE)
Digital Map (DM)
Driver Advisory System (DAS-IM)
Route Control (RC)
Traffic Management (TM)
Voice Communication System (VCS)
Key Management Centre (KMC)
Time Service (TS)
Augmentation (AUG)
Operation & Control Systems Railway Undertaking (OCS-RU)
CCS Off-Board Support (COBS)
Train Management (TM)
Remote Manual Train Operation (RMTO)
Identity & Access Management (IAM)
Mission Data (MID)
Train Data (TRD)
Monitoring, Diagnostic, Config., Maintenance (MDCM)
CCS On-Board (CCS-OB)
Other Application
(Signal Conv., Virtual ETCS Transponder Service, etc.)
CCU n
Virtual Train Coupling System On-Board
(VTCS-OB)
CCU VTCS-OB
Remote Manual Train Operation On-Board
(RMTO-OB)
CCU RMTO-OB
Digital Map Repository On-Board
(DREP-OB)
CCU DREP-OB
Automatic Train Operation On-Board
(ATO-OB)
CCU ATO-OB
Driver Advisory System On-Board
(DAS-OB)
CCU DAS-OB
Monitoring, Diagnostic, Configuration, Maintenance On-Board
(MDCM-OB)
CCU MDCM-OB
CCS Communication Network (CCN)
National Train Protections
(NTPs)
STM (0 – n)
NTC (0 – n)
NTCs-Antenna
User Identification & Authentication (UIA)
UIDR 1)
Cabin Voice Radio VoIP (CVR-V)
CVD
Train Display System (TDS) 1)
TDS 1)
CCU PER-OB
Perception On-Board
(PER-OB)
proprietary 2)
PER-Sensors
CCU LOC-OB
Localisation On-Board
(LOC-OB)
LOC-Sensors
CCU CMD
CCU BTM-LTM
CCU ETP-OB
I/O Ports
SIL4 I/O Ports
European Train Protection On-Board
(ETP-OB)
CMD-Sensors
BTM-LTM-Antenna
GSM-R EDOR
Cabin Voice Radio Legacy (CVR-L)
Cab Voice Radio Legacy (GSM-R)
Physical Train Unit Operation Systems (PTU-OS)
Public Mobile Radio
Passenger WiFi
WTB GW
Wired Train Bus (WTB)
Train Adapter (TA)
I/O Ports
OCORA Gateway (OGW)
Wired Sensors & Actors (WSA)
Train Control System (TCMS)
TCN & Op Network
Passenger Info Systems (PIS)
Security On-Board (SEC-OB)
Shared Security Services On-Board (SSS-OB)
Security Network
ECN / ECN Security Gateway
COM Network
FRMCS On-Board System
MCG (CCS) On-Board System
Connectivity On-Board (CON-OB)
JRU (1 – n)
ORD (1 – n)
DRU (1 – n)
Com
MNO
3GPP / WiFi
GSM-R (Voice & Data)
Mobile & Fixed Connectivity Infrastructure (GSM-R Data / GSM-R Voice / FRMCS / Public Radio)
Nat. Systems
Driver
Technician
Evaluator
Environment (incl. LSIG & PTU)
EURO Balise /Loop
Driver
MNT (1 – n)
Evaluator
Current CCS-OB Functionality
Future CCS-OB Functionality

Remark: solid lines indicate wired connections, dashed lines "over the air" communication, dotted lines represent proprietary connections, and dashed-dotted lined represent user interactions.

1) TDS & UIDR may be moved into the PTU-OS / LOC&PAS domain.

2) Lower ISO layers are standardized to ease the introduction of the safe computing platform. Alternatively, the interface with the backbone of the safe computing platform needs to be standardized.

Figure 2: System under Consideration – Logical Architecture – Building Block View

5 Cybersecurity test scope

The test perimeter includes tests on system and subsystem according to their security capability. It includes also compensating countermeasures in the integration phases which are identified during risk analysis in order to reach the required level of security.

6 Link with RAMS and usability

The perimeter of the test includes verification of security requirement but also usability of the system and is also linked to functional and safety of the system.

In fact, cybersecurity introduces some constraints in the system environment that can conduct more complex operations, especially for human interaction. Tests shall verify that the security measures have been implemented in a way the overall system is not hindered in an unexpected or not specified manner.

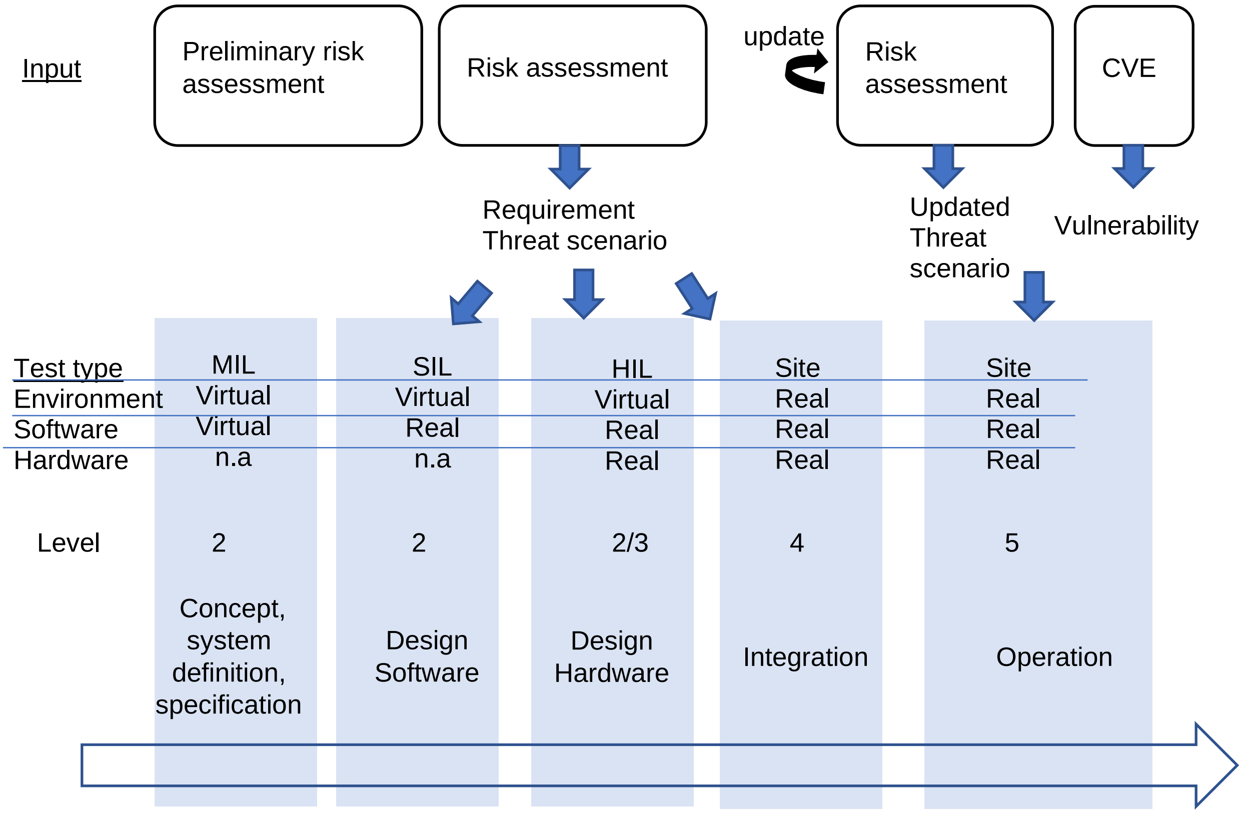
Regarding responsibility, the verification of the absence of deterioration of safety performance by security mechanism will be in the perimeter of functional RAMS tests, especially safety tests.

7 Test lifecycle

7.1 During conception

Test activities can be conducted at each stage of the development.

- During the concept phase, system definition and specification phases, threat and system can be modelled so that test can be conducted at an early stage. This is model-in-the-loop approach (MIL). The system is modelled based on specification. Simulation can be performed based on operational scenarios. The input for modelling the scenario comes from risk analysis which provide security requirements (system capabilities) and threat model and scenario for modelling the environment. The modelling of environment of the system under test and the scenario are reused through all the cycle of conception as a reference. The behaviour of the system shall be the same from specification until deployment.
- During software design, specific software tests can be conducted. The developed software is embedded in a digital test bench where the environment is simulated. This is Software-in-the-loop approach (SIL).
  Tests are performed according to software requirements. Especially, common cybersecurity design flaws are evaluated such as broken access control, injection, misconfiguration, cryptographic failures, insecure design (buffer overflow etc.).
- During hardware design, hardware with deployed software can be tested. This is Hardware-in-the-loop approach (HIL). A physical test bench integrates the system, simulates the interface, and records the output of the system in order to verify its behaviour. Specific physical tests can be carried out e.g. auxiliary channel attack.
- During integration of components in the train and during operational exploitation, on-site test shall be performed.



Test type	MIL	SIL	HIL	Site	Site
Environment	Virtual	Virtual	Virtual	Real	Real
Software	Virtual	Real	Real	Real	Real
Hardware	n.a	n.a	Real	Real	Real
Level	2	2	2/3	4	5
	Concept, system definition, specification	Design Software	Design Hardware	Integration	Operation

Virtual: a digital representation of the system is implemented in order to perform early tests without waiting for production of the finalized software.

Real: release version of software or hardware.

Level: System decomposition according to testing strategy document [12]

- 2: building block
- 3: CCS-OB
- 4: vehicle
- 5: system (vehicle and trackside)

7.2 During operation

The cybersecurity test strategy shall consider:

- The lifecycle of the technology
- The lifecycle of the product
- The lifecycle of the train project where the CSS-OB system will be integrated
- The context of using the SuC, in particular the evolution of exposures, of threats or of attack technics

Tests shall be adapted to the phase of conception and be performed during the life of the system to ensure maintenance in operational secure condition. In fact, the level of protection shall follow the evolution of the threat and the exposure.

The test strategy can be based on time by defining recurrent test phases or based on event (e.g., when vulnerability appears, when regulation rules evolve). The frequency of a test has to be defined proportionally to the level of threat and exposure and the nature of the different components that compose the system.

The publication of the vulnerability (CVE) is the responsibility of the supplier, whereas the update of the risk assessment is the responsibility of the railway undertaking (regarding CCS-OB scope).

§10.3.2 of TS 50701 relating to patch management identifies tests to be carry out through the patch process.

8 Test accountability

The accountability of the test shall be defined for each stakeholder. It’s defined in the testing strategy document [12]and there is no specificity according to cybersecurity.

According to the type of test certain level of independence shall be ensured (EN 62443-4-1 §9.6).

9 Test consistency

Different kind of tests can be conducted (in accordance with (TS 50701 §9.1):

- Verification: tests are conducted in order to verify that component or system requirement are taken into account (focused on process) during all the design and implementation phases.
  Verification activities could also be performed after the handover between integrator and operator throughout the lifecycle.
- Validation: the system is evaluated according to its final use with a specific project configuration in its operational context (focus on performance).
  The responsibility can be shared between suppliers and operator
  - During specification of system requirements by the supplier
  - During system validation by the system integrator
- System acceptance: Final synthesis before handover of the system to the asset owner (operator). The asset owner delivered the acceptance based on technical requirement conformity and respect of contract clauses.
- Certification: Control and/or tests made in order to certify that a component / a system is compliant with a normative document and/or a certification scheme preliminary defined for it. This kind of certification may be delivered by an independent laboratory / assessor depending on the certification scheme. Very few certification schemes are available at this moment (common criteria according to ISO/IEC 154048 for e.g.), but it has to be considered for the future. They cover generic processes and do not take into account specificity of high level of security for railway. In mid/long term, a certification scheme can be considered in order to increase / standardize the proof of level of performance assessed by an independent entity.

The test plan is based on the following inputs:

- Security requirement at the component, building block and at the system level (regarding Cybersecurity Requirements): specific tests have to be defined in order to verify each requirement defined in the system specification.

- Threat scenario (regarding risk analysis assessment): The system is tested in its operational environment, and it is subjected to sequences of attacks following scenarios deemed plausible in order to verify its robustness.

1.	Reconnaissance
2.	Weaponization
3.	Delivery
4.	Exploitation
5.	Installation
6.	Command and control
7.	Actions on objective

Table 1: Pattern of attack sequence for cybersecurity test operational scenario

10 System assessment

The following activities shall be conducted for assessing the SuC:

- Architecture review: choice, implementation of hardware and software component are assessed
- Configuration review:
- Source code review: whole or part of the code and compilation condition is analysed. Poor coding practices and logical fault are searched. Static analysis can also be performed by specialized software that can detect coding errors according to predefined rules
- Penetration testing: tests are performed in real condition in order to discover vulnerabilities
- Vulnerability testing: based on a known list of Common Vulnerabilities and Exposures (CVE)
- Threat mitigation: test of robustness of the defence in depth layer principles
- Physical access review: control that physical access are robust enough regarding exposure
- Organizational review: control that exported organizational constraints are correctly fulfilled and/or implemented into organization or maintenance documentation

11 Penetration Testing

Test based on the knowledge of the system:

Black box testing	Tests are performed on the attack surface, especially on the interfaces. Tests are performed only by identifying external access to the system and attempt made to enter into the system. The activities can be decomposed in several tasks: 1- Recognition: sniffing the information exchanged by the system, port scanning, vulnerability scanning 2- Exploitation: code injection, emission of special forged packet, denial of service, brute force password attack This test implies that we have a partial knowledge of the system and its interface. This kind of test is frequently needed for COTS products that we don't have access to the specification or the code.
White box testing	The tests are based on the complete knowledge of the system. The aim is to verify that the system correctly implements the requirements. Tests are performed also inside the system. The intrinsic performances will be tested, in particular the hardening (vulnerability scan, hardening of memory for password and cryptographic, right and access profiles for example).
Grey box testing	It's a mix of black box and white box testing approaches stated above. Tests on external interfaces are performed and internal behaviour is monitored simultaneously. Internal mechanism is not precisely known e.g., we do not have access to the source code.

Table 2: type of test according to the knowledge of the system

The test practices shall be evaluated regarding the test strategy and derived from the risk analysis. Especially, the coverage level of security risk, the coverage level of security requirements, the number of threat scenario tested.

12 Test facilities

The test means includes all the material needed to perform tests including hardware and software.

12.1 Software

Software tool is a specialized application or library which allow to perform e.g., :

- sniffer and analyser: Wireshark
- vulnerability identifier: Nessus, Metasploit, OpenVAS, Lynis
- port scanner: Nmap
- brute force: hydra
- static code analysis: SAST (static application security testing) / DAST (dynamic application security testing)

Framework software tool provides a list of tools to perform pentesting test:

- KALI: distribution of Linux which integrates several security tools
- PARROT (https://www.parrotsec.org/)

12.2 Hardware

The level of hardware resource is different depending on the tasks and the phases of development:

Task	Equipment
Test on code	Computer with IDE for executing the code and security tool chain
Hardware in the loop	A test bench emulated the environment of the system. It allows to interface to the external interface of the system. the test equipment can be shared between functional and security test Test are performed on: - generic version of the system (with generic configuration) - specific version of the system (project specific configuration). Testing is reduced to functions linked to this specific configuration.
Site test	Laptop with security toolchain in order to be able to connect to different parts of the train directly on equipment or on the network.

12.3 Protective measures

By preference, cybersecurity tools shall be installed on a computer separated from the operational network of the company with suitable identification and usage control.

It shall also be ensured that tests performed on the “system under consideration” shall not present risk on a safety perspective and shall not unintentionally damage the system itself. That’s why, for acceptance, test on laboratory shall be preferred and the site test on train shall be limited to the minimum. The risk of damage and its consequence and the recommissioning capacity shall be assessed when designing the tests.

During lifecycle, as tests on train are difficult, test on laboratory shall be performed with simulated environment in order to ensure compliance of the system on track. This is a relevant use case for digital twin where the system in laboratory duplicates the system in operation.

Verification of lack of degradation on the system and to the connected system shall be done after the test.

13 Test actors

Different actors are involved in the assessment of the cybersecurity of the system

Role	Skills	Task
Code reviewer	Code hardening Secure coding practices	• Static review of code (detection of backdoor or malicious code) • dynamic test on code (buffer overflow)
Penetration tester	Test design Use of security toolchain Testbed definition	• Design test according to requirement and operational scenario • Install, configure and use security toolchain • Perform tests • Analyse test result
Cybersecurity architect	Security architecture	• Review of architecture and configuration

14 Specific test

According to the specificity of the OCORA CCS-OB reference architecture, high level test principles can be identified

Topic	Description	Test
Control Command Network	The CCN allows exchange of information through the CCS and the TCMS system. Logical and/or physical segregation allows the separation of heterogenous safety. Different types of information are exchanged with potential need of high level of integrity, confidentiality, availability.	• Review of switch file configuration that has to be conform to flow matrix • VLAN hopping • Bypass of firewall rule, dataflow restriction tentative • Malformation of packet • Fuzzing • Sniffing • Log review • Denial of Service • Log protection and correlation
Cryptographic material	Cryptographic materials are stored on board insuring integrity and authenticity of the exchange.	• Secret encryption theft
Maintenance access	Maintenance access allow diagnostic, upload of configuration or software file. Embedded web server provides an interface to ease the maintenance task	• Password • Web server vulnerability • Rules and rights: Privilege escalation, URL manipulation • SQL injection • Log registration
Computing platform / HMI	The processing unit achieves the computation of the system. It can be based on operating system (e.g., Linux). It can also deploy several virtual machines to implement software with logical segregation.	• Vulnerability scan • Port scan • Virtual machine escape

15 Key performance indicator

The efficiency of the testing activities has to be measured through KPI. The KPI should define a global objective and measurement shall be done through the test process

KPI	Description	Detail
Test coverage	Coverage regarding - The operational attack scenario: - The requirement: test covers the applicable requirements according to the level of security: Functions, capabilities, interfaces	ratio of scenario covered by a test: 100% ratio of requirement covered by a test: 100% ratio of test by requirement: 1 min, maximum duration of robustness test (force password): 12h
Test results	Ratio between passed/ not passed tests	

16 Additional subject

Cybersecurity verification applies to the system itself but also to the design process itself. In fact, flaw can be introduced during the design process in order to exploit it later. The process itself shall be evaluated. For example:

- Integrated Development Environment (IDE): use for generating code. It can be hijacked to introduce back door.
- Supply chain: the traceability and integrity of the product (hardware and/or software) shall be ensured especially during the phase of exchange between the supplier and the end-user (exchange of data or software shall be done with encrypted file container, transport of equipment shall be sealed)

That's why each supplier shall make verification about equipment, software or tool they use and provide secure means of transmission of their products.

This subject is more related to organisational aspect, especially relation between supplier and asset owner. It is not link to the technical approach of OCORA. So, it shall not be taken into account by testing workstream.