|  |  |
| --- | --- |
| ATO over ETCS  GoA 3/4 | |
| **Operational Principles** | |
| REF  : |  |
| ISSUE  : | 0.0.3 draftA |
| DATE : | 15/12/2017 |

|  |  |  |
| --- | --- | --- |
| **Company** | **Technical Approval** | **Management approval** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Modification History

| Issue Number Date | Section Number | Modification / Description | Author |
| --- | --- | --- | --- |
| 0.0.1  17/10/2017 | All | New document |  |
| 0.0.2  15/12/2017 | 3 | Several actors removed because of wider system scope. | RT |
| 0.0.3  15/12/17 | 6 | Non functional requirement have been added | BBF |
|  |  |  |  |
|  |  |  |  |

# Table of Contents

[1. Modification History 2](#_Toc501123067)

[2. Table of Contents 4](#_Toc501123068)

[3. Introduction 5](#_Toc501123069)

[1.1 Scope of the document 5](#_Toc501123070)

[1.2 Reference and applicable document 5](#_Toc501123071)

[1.3 Abbreviations and definitions 5](#_Toc501123072)

[2 Operational Needs and Missions 5](#_Toc501123073)

[2.2 Manage railway operation efficiently 5](#_Toc501123074)

[2.3 Quality of Service 5](#_Toc501123075)

[2.4 Flexibility of railway operation 5](#_Toc501123076)

[2.5 Safety 5](#_Toc501123077)

[2.6 Security 6](#_Toc501123078)

[2.7 Efficient use of energy and resources 6](#_Toc501123079)

[2.8 Lifecycle costs 6](#_Toc501123080)

[3 Roles and responsibilities (Actors definition) 7](#_Toc501123081)

[3.1 Train Equipment without ATO Control 7](#_Toc501123082)

[3.2 IM Control Centre staff 8](#_Toc501123083)

[3.3 RU Control Centre staff 9](#_Toc501123084)

[3.4 Physical Railway Environment 10](#_Toc501123086)

[3.5 Passenger 11](#_Toc501123087)

[3.6 Freight (Goods) 11](#_Toc501123088)

[3.7 Train Attendant 13](#_Toc501123091)

[3.8 Power Supply 15](#_Toc501123094)

[3.9 Driver 15](#_Toc501123095)

[3.10 Maintainer IM/RU 16](#_Toc501123096)

[3.11 Configuration Management 16](#_Toc501123097)

[3.12 Maintenance Management 17](#_Toc501123098)

[4 System Inputs and Outputs (interface with actors) 18](#_Toc501123099)

[5 Operational Environment (Ops environment and contexts) 19](#_Toc501123100)

[5.1 Automatic Railway Operation – Super system Context 19](#_Toc501123101)

[5.2 ATO – GoA 4 20](#_Toc501123102)

[5.3 ATO – GoA 3 21](#_Toc501123103)

[5.4 ATO – GoA 2 22](#_Toc501123104)

[5.5 ATO – GoA 1 23](#_Toc501123105)

[5.6 ATO – Maintenance and Configuration Maintenance 23](#_Toc501123106)

[6 Non functional specification 25](#_Toc501123107)

[4. Overview 26](#_Toc501123108)

# Introduction

## Scope of the document

## Reference and applicable document

## Abbreviations and definitions

# Operational Needs and Missions

##### This section captures the high-level needs and mission for railway operation in GoA3 and GoA4.

## Manage railway operation efficiently

* Operate trains according to requirements listed in sections 2-7
* Manage train running numbers
* Monitor train movement (at control area entry, during movement, at control area exit)
* Monitor train status (assigned running number, position, speed, actual status, status history, alarms, warnings)
* Manage operational and technical incidents and degraded situations
* Use the same reference time within the entire system
* Manage maintenance
* Manage staff

## Quality of Service

* Prevent, detect and quickly solve deviations from planned time table
* Prevent, detect and quickly solve conflicts on infrastructure elements
* Achieve required RAM performance (application specific)
* Achieve required passenger comfort (minimum dwell times, jerk limitation, …)
* Avoid damage to freight
* Avoid

## Flexibility of railway operation

* Flexibility to customer demand (cancel trains, start new trains, adjust train consist, …)
* Provide trackside remote commands to override automatic functions (start, stop, change direction, …)
* Flexible use of infrastructure (Insert or remove train journeys; Change in speed limits, …)
* Flexible shunting operations
* Mixed operation in different Grades of Automation
* Interoperability between track sub-systems and on-board sub-systems (different suppliers, different RU, different IM)
* Interoperability between adjacent track sub-systems (seamless cross-border traffic, different track areas or different IM)

## Safety

* Safe train separation (movement authority, danger point, …)
* Safe speed supervision (maximum speed, dynamic braking profile, rollback, …)
* Safe standstill supervision (passenger exchange, stabling, driver entry / exit; …)
* Safe passenger exchange (door release, door opening / closing, …)
* Safe joining and splitting
* Safe loading and unloading of goods
* Safety of staff
* Safety at level crossings
* Safety of the environment (including dangerous goods)
* Safe management of intrusion
* Safe management of obstacles
* Safety management of degraded situations
* Safe train operation in accordance to the rolling stock limitations (avoid damage to the coupling while accelerating, …)

## Security

* IT security
* Physical security

## Efficient use of energy and resources

* Efficient energy management of railway operation
* Energy efficient movement of trains and vehicles
* Efficient management of trackside power limitations
* Efficient use of transport capacity (minimum headway, minimum crossing time)
* Efficient railway operation by reducing process time (e.g. doors management, turning trains, splitting and coupling trains, start and end of missions)
* Efficient use of rolling stock
* Efficient use of staff (rescue staff, service staff, central operators, stabling staff, maintenance staff, …) including reduction of operational staff (train and trackside)

## Lifecycle costs

* Modular, expandable, extendable, upgradable over the products life cycle
* System scalability (amount of trains, extend track fitment, …)
* Technological upgradability (including innovation, independent innovation cycle)
* Interchangeability (according to open FFFIS for vendor independency)
* Backwards and forwards compatibility between different system versions
* HW platform independency (HW independent application SW)
* Cost-efficient maintenance and component replacement
* Cost-savings (e.g. avoid building new track infrastructure)
* Life-extension of railway assets (reduction of wear and tear on wheels, tracks, etc.)

# Roles and responsibilities (Actors definition)

## Train Equipment without ATO Control

### Role

##### Train Equipment without ATO Control represents train equipment without ATO control, but with diagnostic supervision by the SysATO (Train- and Trackside).

### Responsibilities

##### Train Equipment without ATO Control provides the following exemplary functionality:

* HVAC
* Toilette
* Reading lights
* Coffee machine
* Interior comfort equipment

### Requirements

##### None

### Actor-Actor-Communication

##### Train Equipment Without ATO Control is also in communication with:

* Diagnostic System

## IM Control Centre staff

### Role

#### This actor supports scheduling the flow of trains through the railway network.

### Responsibilities

#### Optimise traffic flow

#### Request route setting

#### Manage communication with infrastructure Maintenance Management

#### Considers IM related information from Environment Conditions Monitoring System(s)

#### Considers information related to dangerous goods (ranking)

#### Manage communication with adjacent trackside Control Center

#### Considers infrastructure assets data.

#### Authorisation/command of awakeness, coupling, uncoupling, etc…

#### Continously calculate and provide the exact required operationnal running data for trains

#### Process real time information on train positions and train speeds

#### Schedule trains according to the current scheduling strategy (e.g. travel time optimisation or optimisation of energy consumption)

#### Change scheduling strategy automatically or by user action

#### Provide user interface and reporting

#### Provide emergency management

### Requirements/Constraints:

#### None

### Actor-Actor-Communication

#### The actor is also in communication with:

##### RU Control Centre staff

##### Maintainer IM/RU

##### Power Supply

##### Physical Railway Environment

## RU Control Centre staff

### Role

#### This actor supports scheduling the flow of trains through the railway network.

### Responsibilities

#### Manage communication with train Maintenance Management

#### Considers RU related information from Environment Conditions Monitoring System(s)

#### Request of awakeness, coupling, uncoupling, etc…

#### Define required service level (flexibility in time schedule)

#### Provide user interface and reporting

#### Provide emergency management

### Requirements/Constraints:

#### None

### Actor-Actor-Communication

#### The actor is also in communication with:

##### IM Control Centre staff

##### Maintainer IM/RU

##### Power Supply

##### Physical Railway Environment

## Physical Railway Environment

### Role

##### Physical Railway Environment represents the physical environment an ATO controlled train passes through. This comprises at least the kinematic gauge along the running track of the train.

##### This actor is passive, i.e. cannot send information or perform tasks.

### Responsibilities

##### Physical Railway Environment provides the following exemplary properties:

* Degraded situations in the railway system external to ATO
* Objects on or near the right of way e.g. road users at level crossings, trespassers, animals, vegetation
* Obstacles within the kinematic gauge
* Environmental influences like snow, rain, fog
* Aerodynamic effects

### Requirements/Constraints

##### None

### Actor-Actor-Communication

##### Physical Railway Environment is also in communication with:

* Control Center

## Passenger

### Role

##### Passenger represents a passenger traveling on an ATO controlled train.

### Responsibilities

##### None

### Requirements/Constraints:

##### Passenger requires:

* Safe travel according to the relevant individual safety targets
* Safe boarding and alighting according to the relevant individual safety target
* Adherence to comfort criteria during travel like temperature, humidity, oxygen content, acceleration, jerks and vibrations.

### Actor-Actor-Communication

##### Passenger is also in communication with:

* Control Centre

## Freight (Goods)

### Role

##### Freight (Goods) represents freight transported on an ATO controlled train.

### Responsibilities

##### Freight (Goods) provides the following exemplary functionality:

##### Detection and reporting of unsafe conditions like spilling of dangerous materials or fire hazard (if e.g. intelligent Freight (Goods) is able to report this condition itself)

##### Detection of violation of environmental conditions (if e.g. intelligent Freight (Goods) is able to report this condition itself)

### Requirements/Constraints:

##### Freight (Goods) requires:

* Safe transport
* Safe loading and unloading
* Detection and reporting of unsafe conditions like spilling of dangerous materials or fire hazard (if Freight (Goods) cannot detect this itself)
* Detection of violation of environmental conditions (if Freight (Goods) cannot detect this itself)

### Actor-Actor-Communication

##### Freight (Goods) is also in communication with:

* (tbd)

## Train Attendant

### Role

##### Train Attendant represents a person performing a given set of operational tasks.

### Responsibilities

##### Train Attendant provides the following exemplary functionality:

* Provide service to Passengers also degraded situation
* Monitoring the state of the train
* Reporting problems to the Control Center
* Cancelling the door release for departing stations
* Recovery after disturbances

### Requirements/Constraints:

##### None

### Actor-Actor-Communication

##### Train Attendant is also in communication with:

* Control Center
* Diagnostic System
* Passenger
* Wayside Signals

## Power Supply

### Role

##### Power Supply represents the components providing electrical power to SysATO (Train- and Trackside).

### Responsibilities

##### Power Supply provides the following exemplary functionality:

* Supply power for operation of SysATO (Train- andTrackside)

### Requirements/Constraints:

##### None

### Actor-Actor-Communication

##### Power Supply is also in communication with:

* Control Center

## Driver

### Role

Driver represents the person controlling the Train in GoA 2 and

GoA 1.

### Responsibilities

⦁ Safe, optimized and punctual controlling of the train

according to the time schedule

⦁ Stoping and starting of the train in stations, open track

and yards

⦁ Shunting of the train in stations and yards

⦁ Ensure harmonized and safe operation for the

Passenger and Freight (Goods)

### Requirements/Constraints

None

### Actor-Actor Communication

Driver is also in communication with the:

⦁ Control Center

⦁ Wayside Signals

⦁ ATP

⦁ Passenger

⦁ Train Equipment Without ATO Control

⦁ ATO Controlled Local Train Equipment

⦁ Diagnostic System

## Maintainer IM/RU

### Role

##### Maintainer IM/RU represents the maintenance personnel of the infrastructure manager or railway undertaking that ensures a safe state, failure free functioning, reliability and availability of SysATO (Train- and Trackside) during the active life cycle.

##### Maintainer IM/RU can be refined into roles Maintenance Management and Configuration Management. See description of these actors and diagram System ATO - Refinement Actor

##### Maintainer IM [SysATO BDD 2].

### Responsibilities

##### Maintainer IM/RU provides the following exemplary functionality:

* Update software
* Ensure preventive maintenance
* Replace or repair hardware
* Prepare and update of configuration data (e.g. extension, application, bug-fix, patching, .....)
* Update remote and local configurations (e.g. extending of the ATO area, ...)

### Requirements/Constraints:

##### None

### Actor-Actor-Communication

##### Maintainer IM/RU is also in communication with:

* Control Center
* Diagnostic System

## Configuration Management

### Role

Configuration Management is a refinement of actor Maintainer

IM/RU, representing tasks of personell responsible for

configuring SysATO (Train- and Trackside).

### Responsibilities

##### Configuration Management provides the following exemplary functionality:

* Prepare and update of configuration data (e.g. extension, application, bug-fix, patching, .....)
* Update remote and local configurations (e.g. extending of the ATO area, ...)

### Requirements/Constraints:

##### None

## Maintenance Management

### Role

##### Maintenance Management is a refinement of actor Maintainer IM/RU, representing tasks of personnel responsible for maintaining SysATO (Train- and Trackside).

### Responsibilities

##### Maintenance Management provides the following exemplary functionality:

* Update software
* Ensure preventive maintenance
* Replace or repair hardware

### Requirements/Constraints:

##### None

# System Inputs and Outputs (interface with actors)

# Operational Environment (Ops environment and contexts)

## Automatic Railway Operation – Super system Context



## ATO – GoA 4



## ATO – GoA 3



## ATO – GoA 2



## ATO – GoA 1



## ATO – Maintenance and Configuration Maintenance



# Non functional specification

## Conformance to the Standards

##### TSI L&P

##### <https://www.prorail.nl/siteassets/homepage/samenwerken/vervoerders/documenten/netverklaring-2022-initiele-versie-versie-1.0-d.d.-11-december-2020.pdf>

## Risk to environment

##### The following regulation is applicable in The Netherland:

<https://www.rijksoverheid.nl/documenten/kamerstukken/2017/06/15/aanbieding-verslag-basisnet-2016>

## Reliability, Availability and Maintainability

##### For trackside we could avoid to define figure because, it is clearly application specific.

##### For on-board, we have to define figures for availability.

##### These figures for on-board will be similar to the ones used for other embedded systems like ETCS-OB.

## Safety

### Introduction:

##### The Risk Acceptance Criteria according the CSM RA based on EU Railway Safety Directive applies.

##### Side to side with the models (Semi Formal Mode (SFM) and Fully Formal Model (FFM)), should lay a set of static safety properties on the model. The higher level properties will be provided

##### by the document provided after safety analysis, that we will consider here as a preliminary hazard analysis, because it provides us the higher level feared events.

##### These feared events will be refined during a Sub System Hazard Analysis (SSHA) into events of the abstraction level of the sub system, which will be collected in the Hazard Log. For all hazardous events named in the Hazard Log a risk analysis will be performed.

##### Based on the analyses suitable risk control activities a determined and collected in the Hazard Log. All hazards and their control activities are then refined into safety requirements/ properties.

##### The lower level Safety Properties/Feared Events shall address variables, state and interfaces used in the formal model.

##### As much as possible, formal proof would then be used to prove that the ATO Model never enters a Feared State, as long as the other systems (RBC, obstacle detection, communication layer) fulfil their own safety properties (axiom describing the environment). The exact process shall be described in the Safety Plan.

### Non-functional requirement related to safety

##### A Safety Case Concept and Safety Plan shall be issued describing the safety activities for all the steps from the SRS to the SFM, the FFM and the source code, according to CENELEC EN~50126, EN~50128 and EN~50129.

##### All the output documents required by the EN~50126, EN~50128 and EN~50129 for each step of the lifecycle shall be described, or their lack shall be justified.

##### The safety activities shall at least be applied on a sample of the ETCS on-board functionalities and the respective safety requirements to demonstrate the suitability of the safety plan.

##### The safety activities shall aim at a THR compatible with the safety hazard analysis

##### The safety analysis shall consider as higher level Feared Events the events named in the safety hazard analysis in respect to the scope of the subsystem.

##### Those Feared Events shall be refined to SRS and Model levels, then to the model level, and allocated to the functions to determine hazardous events.

##### The refinement shall only be done for a sample part of the system.

##### The model-level safety requirements shall be written in the same degree of formality as the corresponding model or higher.

##### It shall be verified that the SFM, FFM and source code complies with all respective safety requirements either by a real-time constraint. This real-time constraint is not guaranteed in the model itself, but can be expressed in the model using the RTM/API.

##### if a safety requirement/property can not be proven, testing covering all reasonable possible events shall be used.

##### The software safety activities will comply to the requirements of CENELEC 50128.

##### The model safety activities will be adapted from the requirements of CENELEC 50128.

## IT Security

##### For the whole system, security is in the scope of WP8 of X2Rail-1.

##### We just have to make sure that they will consider ATO needs.

##### A priori, there will be no ATO requirement relating to security.

##### But, WP8 could define some exported constraints on ATO architecture and/or interfaces.

##### If there is no specific requirement coming from WP8, we should add this chapter.

##### But, today, it be remain open (to be defined)

##### When mature, we would have to organise joint meeting with WP8 representatives.

##### By definition IT security requirement should cover all the Use Cases (including maintenance and configuration activities)

##### Obsolescence requirement

##### For OB HW, we have to consider the figures applicable for Rolling Stock (typically 30-40 year).

##### For TS HW, similar figures should be considered if we use the same business model as today; That is to say delivering some trackside server belonging to the customer.

##### For OB SW upgrade, to ATO system shall permit regular update to be done remotely without immobilizing the train.

##### TS SW should be easily upgradable.

##### EN-62402 (dependability) defines obsolescence requirement and process to manage obsolescence.

## Interoperability

##### Rolling stock must be able to run on all ATO fitted lines in Europe, in the highest GoA modes that is supported by both ATO-OB and ATO-TS.

##### We shall refer to the Operation Requirement v1.9

## Requirement on System and architecture

##### The description of the architecture shall be semi-formal.

##### On functional level fully formal methods will be used

##### This architecture shall provide the functions and the data streams between them.

##### All parts of the architecture should be modelled.

##### The SRS shall provide the interfaces between the considered subsystem and its environment.

##### When the boundary of the formalized subsystem corresponds to a FIS or FFFIS, the SRS shall try to comply to it even when it is not mandatory.

##### The SRS shall allocate the requirements of the SRS to the functions and their I/O

##### The SSRS shall be compliant or shall allow compliance to the mandatory requirements from the other subsets of the TSI.

##### Traceability between the SRS and the formal Model shall be provided.

##### All interpretations, additions, refinement, omissions and design choices during the allocation have to be documented in one log and justified.

##### All interpretations, additions, refinement, omissions and design choices during the allocation have to be documented in one log and justified.

##### The requirements allocated to other subsystems e.g. ETCS shall be tracked.

##### In case of divergence between an identified national behaviour and the SRS behaviour, it shall be discussed and decided whether or not the national behaviours are required in the formal model.

##### If this is the case, it shall be traced explicitly.

##### if this is the case, If it is the case, it shall be possible by configuration to enforce pure compliance to the SRS

##### The formal model shall identify the Vital and Non Vital functions, requirements, and data streams.

## Interchangeability

##### The ATO system shall be modular with FFFIS interfaces.

##### The interchangeable building blocks are defined in the Logical Architecture

##### The application SW and HW (incl. Operating system) shall be interchangeable. This leads to requirements to the Runtime Model/API

##### The framework needs to provide a list of properties and functions. If we take the parallel of the Java environment, some of these properties/functions will be provided by the properties, and some of them will be provided by the API.

##### If we consider for example ``allocation of memory'', in Java usually it is just provided by the creation of an object (thus in the ``Runtime model''). In C it is given by the malloc function, which is part of the API (of course, we will find eventually that it leads to the runtime model too, but in the user point of view, it is definitely part of the API).

##### What is considered is that at requirement level, it is not useful to know which property will come from API and which will come from the runtime model. It is only interesting to provide the properties themselves.

##### In order to avoid ambiguities, we will define the following.

##### The RTM/API model shall provide an abstraction layer of the hardware architecture.

##### The RTM/API shall abstract memory management

##### The RTM/API shall abstract the execution of states machine

##### The RTM/API shall allow communication and concurrence (if requested by the model formalism)

##### The RTM/API shall allow read/write to a persistent data store

##### The RTM/API shall allow to state real time constraints

##### The RTM/API shall provide emulation for a real time clock

##### The RTM/API shall make possible to refine the software into final code able to run on hardware complying the EN 50129 standard for the requested SIL

##### The RTM/API shall allow discriminating Vital processing, data and I/O from Non Vital processing, data and I/O

##### The RTM/API shall provide a way of communication between Vital processes and Non Vital processes.

##### The purpose of these requirements is to be able to discriminate the safety part from the non safety part. It should be made possible to have it run on a proprietary architecture with both

##### software on the same computer (with for example 2oo3, or coded monoprocessor) or on two different computers. One way of doing this, for example is to have some critical state machines with their data on one side, and the non critical part on the other side, with API channels to make them communicate.

##### The RTM/API shall allow fault injection.

##### The RTM/API shall allow logging and tracing

##### The RTM/API shall provide a way of reading configuration data e.g. constants

##### The RTM/API shall provide an abstraction layer of the communication and interfaces with other components.

##### Even if the FIS or FFFIS requires a specific protocol (\emph{e.g.} Profibus), this protocol will not be implemented in the high level model. It will be considered that low level communication issues are taken into account (= emulated) by the RTM/API.

## Diagnostics and data analytics

##### For the train diagnostic, we have a Use Case for that.

##### But, at least we have to define the required output (or post condition) from this UC in order to be able to manage properly other ATO UC as degrade mode management.

##### Today, diagnostic and onboard activities are performed by the driver or the train attendant.

##### For non-functional requirement related to Diagnostics, we have to refer to IEC 62541.

##### Additionally, the OPC protocol should be used for all the diagnostic features.

## Requirements to the Model

##### Refer to EuLynX Modelling standard Baseline 1 (or baseline 2).

## Requirements to the Verification and Validation

##### The already provided requirements require a safety plan compliant to the CENELEC EN~50126, 50128 and 50129.

##### This pulls a number of requirements on V\&V, including Verification and Validation plans. On the topic of compliance to EN~50128.

##### As the CENELEC standards are not clear enough and have ambiguities, the following requirement have been added.

##### The verification plan shall provide a method to demonstrate the requirements covering all the development artefacts.

##### The verification plan shall state all verification activities required for each of these development artefacts.

##### A Validation Plan shall be issued and complied with.

##### The validation plan shall provide a method to validate all functional and safety requirements over all development artefacts.

##### The validation plan shall state all validation activities required for each of these development artefacts

##### The test plan shall comply with the mandatory documents to be specified. It will possibly be difficult to model all the tests in the course of the project, but the test plan should at least be complete.

##### Each design artefact needs a reference artefact which it implements e.g. code to detailed model.

##### The implementation between them relation shall be specified in detail.

##### E.g. for state machine and a higher level state machine mapping of interfaces, states and transition is required. This includes additional invariants, input assumptions and further restrictions. This information is the basis for verification activities.

##### The design of the artefacts shall be made such to allow verifiability as far as possible.

##### The findings from the verification shall be traced, and will be adequately addressed (taken into consideration, or postponed or discarded with a justification.

## Requirements to language and Formalism

##### Refer to EuLynX Modelling standard Baseline 1.

## Requirements to the Toolchain

##### Refer to EuLynX Modelling standard Baseline 1

##### Because CENELEC standards are not clear enough and have a lot of ambiguities the following requirement have been added to the standard.

##### Each tool in the tool chain shall be classified among T1, T2 and T3 depending on its usage in the process

##### The tool chain shall conform to EN~50128 requirements, for the corresponding SIL and tool class.

##### For T2 and T3 tools, the choice of tools shall be justified, and the justification shall include how the tool's failures are covered, avoided or taken into account (ref. to EN 50128 6.7.4.2).

##### All T2 and T3 tools must be provided with their user manuals.

##### For all T3 tool, the proof of correctness or the measure taken to guarantee the correctness

##### of the output w.r.t. their specification and the inputs shall be provided. E.g. for data transformation, for software transformation (translation, compilation).

## Requirements to the Testing

##### The SFM shall be simulable in debug mode (step-by-step), allowing inspection of states, variables and I/O.

##### The environment shall be emulated by high level construction of the inputs. ``High level'' means that it will not be necessary to define bitwise the inputs at each cycle. On the contrary, some automation will be available to define the behaviour of the inputs.

##### The environment shall be emulated by construction of the inputs compliant to SRS, if safety critical.

##### The tool chain shall allow time-based test cases

##### The tool chain shall allow to write, execute and store test cases and use cases for the SFM.

##### Version management will allow to map test cases version to the SFM, the FFM and source code versions

##### The tool chain shall allow to generate test cases for the SFM, the FFM and source code from test model

##### The test model is independent from the tested model. The test model can be either a model of the environment, or a model of the same subsystem that is being tested, but in both cases this test model must be completely independent from the tested model.

##### The tool chain shall allow to write, execute and store test sequences combining multiple test cases for the SFM, the FFM and source code.

**Requirements to the Lab Demonstrator**

* A Lab demonstrator is required to validate and review the Formal Users requirement.
* A demonstrator software will be built from the Fully Formal Model.
* The demonstrator may not be vital.
* The demonstrator shall be able to run in real time.
* The demonstrator shall comply to the standardized interfaces in order to be able to interface with other subsystems.
* The demonstrator shall run on a COTS platform
* The demonstrator shall be able to run on different target platforms.

**Requirement to RAMS**

* Refer to COMMISSION REGULATION (EU) 2016/919
* Refer to EN 50126

**Requirements to the Performance, Portability, Environment Conditions, Interchangeability, Interoperability, Life-Cycle, Assumptions and Costs.**

* EUG Document: ATO over ETCS Operational Requirements version 1.9 GoA 4 only

## NF requirement recovered from the GoA2 Ops requirement

##### The following requirements have been extracted from the Ops requirement to be inserted in the NF requirement:

## Interoperability in a given grade of automation

##### The ATO on-board function and the ATO trackside function shall be interoperable.

##### The ATO on-board can be equipped for any GoA or combination of GoAs. Implementing a GoA shall not mandate implementing lower GoAs.

## Interoperability with different grades of automation

##### It shall always be possible to operate in the highest Grade of Automation supported by both the ATO trackside and the ATO on-board.

## Interchangeability

##### Those ATO constituents that are designed with the same open FFFIS specifications shall be interchangeable.

## Configurability

##### The ATO over ETCS system shall be configurable to enable line extensions, modifications of track layout and trackside or rolling stock performance changes.

##### Note:

This non-functional requirement permits to remove any UC and Operation Context dedicated to the system configuration

## Backward compatibility

##### The ATO on-board and the ATO trackside shall operate the highest system version supported by both. Backward compatibility shall be possible by allowing the ATO on-board and the ATO trackside to support several system versions.

##### The previous requirements will be inserted in the list to be imported in the Operation Principles documents (see actions below).

# Overview