Horizon 2020
European Union Funding
for Research & Innovation

X2Rail-5

Project Title:	Completion of activities for Adaptable Communication, Moving Block, Fail Safe Train Localisation (including satellite), Zero on site Testing, Formal Methods and Cyber Security
Starting date:	01/12/2020
Duration in months:	30
Call (part) identifier:	S2R-CFM-IP2-01-2020
Grant agreement no:	101014520

Deliverable D10.4

Verification Report

Due date of deliverable	Month M28
Actual submission date	June 13, 2023
Organization name of lead contractor for this deliverable	TRV
Dissemination level	PU
Revision	2.1

Deliverable template version: 01 (21/04/2020)

Authors & Version Management

Author(s)	**Trafikverket** Arne Borälv
	Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR) Daniel Schwencke
	Alstom (ALS) Fernando Mejia
Reviewer(s)	**Thales (THA)** Dominik Hansen

Version Management

Version Number	Modification Date	Description / Modification
1.0	June 4, 2023	
1.1	June 7, 2023	Included 6.3.
1.1.1	June 7, 2023	Editorial, minor edits.
1.1.2	June 8, 2023	Review by THA and DLR (partially addressed).
1.1.3	June 8, 2023	Minor editorial.
2.0	June 12, 2023	Updated Chapter 7, removed comments and change markers.
2.1	June 13, 2023	Updated Chapter 7 based on review comments.

1 Executive Summary

This document is Deliverable **D10.4 Verification Report**, describing results related to Tasks 10.4, 10.5, 10.6, and 10.7 of WP10 within the X2Rail-5 project. This document builds upon other deliverables by WP10 in X2Rail-5 (D10.1 Requirement Analysis, D10.3 Configuration Data, D10.6 Formal Methods Demonstrator). The main input for these tasks was the Moving Block Specification (Deliverable D4.1, X2Rail-5), defining an ETCS L3 trackside system with moving block ("L3 trackside"). This document describes safety requirements for L3 trackside, in terms of a fault tree-based approach applied at the system of systems (SoS) level, evaluation and refinement of safety hazards for L3 trackside, and results from Formal Methods (FMs) application for V&V of requirements.

The Moving Block Specification (its Part 6, Safety Analysis) specifies the principal ETCS Level 3 hazards identified (beyond existing hazards for ETCS Level 2). These hazards were used for improving the moving block specification, by including mitigation measures in its system requirements. Ideally, safety requirements for L3 trackside should be based on all safety hazards at the System of Systems level, apportioning the safety hazards that apply to L3 trackside (as a subsystem). Traceability from each safety hazard to safety requirements would enable validation of completeness of safety requirements (based on completeness of the safety hazards). This document describes how this approach can be applied to L3 trackside using fault trees.

The moving block specification does not systematically distinguish which requirements are to be considered safety requirements. WP10's requirement analysis identified several issues that complicate to determine clearly defined safety requirements for L3 trackside. One issue is that the moving block specification is a partial requirement specification in many respects. Another issue is that the central Track Status Area (TSA) concept is not sufficiently clear to. Despite this, this document describes two FMs application approaches, based on the ontology and properties described in D10.1 Requirement Analysis, to detail requirements in the moving block specification, to validate their consistency and to prove representative safety properties (if making additional assumptions).

Safety requirements for L3 trackside implementations should, if fulfilled, ensure that all relevant safety hazards are mitigated. In principle, this should be possible to achieve by:

1. Using a systematic approach to determine the safety hazards at the system of systems level, and apportion the relevant hazards to the L3 trackside subsystem, and
2. Defining safety requirements that are configurable for the different types of L3 trackside systems, and other static configuration data.

The 2nd step above requires clarifying and augmenting the ontology concepts and requirements for L3 trackside in the moving block specification, to enable validation that the safety requirements indeed mitigate all hazards (using V&V based on FMs).

2 Table of Contents

3 Abbreviations and Acronyms

Abbreviation / Acronyms	Description
AB	Authority Base
AP	Authority Path
AoC	Area of Control
EoA	End of Authorization
ETCS	European Train Control System
FM	Formal Methods
FMB	Full Moving Block
FVB	Fixed Virtual Block
HW	Hardware
JT	Joined Train
L2, L3	Level 2, Level 3 (ETCS)
LEU	Lineside Electronic Unit (ETCS)
LX	Level Crossing
MA	Movement Authority (ETCS)
OBU	On-Board Unit (ETCS)
OS	On Sight (ETCS mode)
RBC	Radio Block Center (ETCS)
RP	Reserved Path
RV	Reversing (ETCS mode)
SoS	System of Systems
SR	Staff Responsible (ETCS mode)
SW	Software
TD	Technology Demonstrator (Shift2Rail)
TD 2.3	Technology Demonstrator: Moving Block
TD 2.7	Technology Demonstrator: Formal methods and standardisation for smart signalling systems
TL	Train Location
TLP	Train Location Path
TMS	Traffic Management System
TSA	Track Status Area
TTBJ	Train To Be Joined
V&V	Validation and Verification
WP	Work Package
WP10	Work Package *Formal Methods for Functional Railway System Architecture*, X2Rail-5

4 Background

This document is Deliverable **D10.4 Verification Report**, describing results related to Tasks 10.4, 10.5, 10.6, and 10.7 of WP10 within the X2Rail-5 project. The main input for these tasks was the Moving Block Specification [2], defining an ETCS L3 trackside system with moving block ("L3 trackside").

4.1 Moving Block Specification

The main input for the tasks relevant to this document is the Moving Block Specification, created by Shift2Rail TD2.3. The plan was to use the version created by the X2Rail-3 project [3]. However, during requirement analysis, it became clear that work-in-progress additions and updates within the X2Rail-5 project needed to be considered and/or adopted. Ultimately, tasks shifted to use work-in-progress versions created within the X2Rail-5 project, to consider the most mature version of the requirements, despite the associated drawbacks:

- Several assumptions WP10 had made previously were invalidated[1].
- The final version [2] was issued late in the schedule of X2Rail-5 (in 2023).

The moving block specification is divided into six parts, defining assumptions, requirements, and rules (grouped further into subcategories, such as requirements for train location, etc.). Table 1 gives an overview of its different parts.

TD2.3 has defined operational use cases as part of its work to define requirements in the Moving Block Specification. However, these use cases could not be made available as input for WP10 (and so WP10 could not use or benefit from these).

Part	**Description**
Part 1 – Introduction	Introduction
Part 2 – System Definition	Assumptions (relating to work in other TDs in Shift2Rail)
Part 3 – System Specification	Requirements for L3 Trackside (beyond those for L2)
Part 4 – Operational Rules	Operational rules for L3 Trackside (beyond those for L2)
Part 5 – Engineering Rules	Engineering rules for L3 Trackside (beyond those for L2)
Part 6 – Safety analysis	Safety hazards for L3 System (beyond those for L2)

Table 1 The different parts of the moving block specification

4.1.1 Safety Analysis with Formal Methods

This document builds upon other deliverables by WP10 in X2Rail-5 (see Figure 1): D10.1 Requirement Analysis, D10.3 Configuration Data, D10.6 Formal Methods Demonstrator.

Figure 1 illustrates the scope of the safety analysis based on the use of formal methods in this deliverable D10.4, in relation to the generic process steps for FMs application (see [7] Section 7.2). The scope includes results obtained in V&V using FMs and relevant learning and output

[1] A technical note that assumed the Moving Block Specification from X2Rail-3 as basis was created during the requirement analysis task. This was not a total waste of effort however, since is also related to gain an understanding of ETCS L2 (which the Moving Block Specification depends on).

produced as a result. Figure 1 also illustrates the scope of other deliverables (D10.1, D10.3, D10.6), related to the earlier steps of the generic FMs application process.

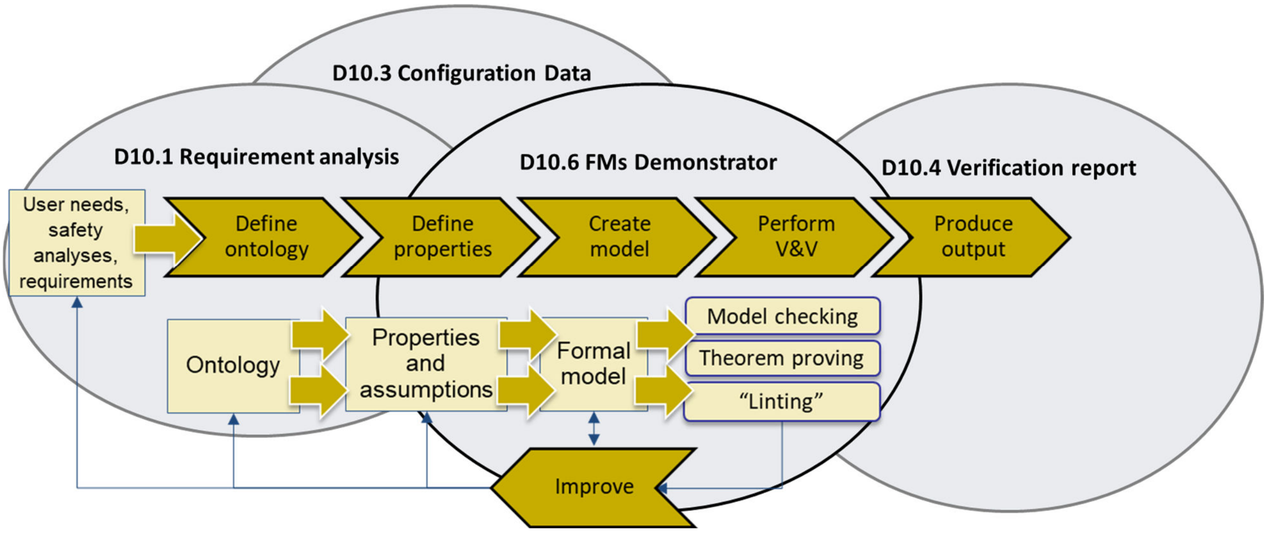

Figure 1 Scope of FMs-based safety analysis in this deliverable (versus D10.1, D10.3, D10.6)

4.2 Outline

The chapters of this document are organised as follows:

- Chapter 5 describes a fault-tree based approach to define safety hazards and safety requirements.
- Chapter 6 describes safety requirements from the FMs application approaches applied to the case study of L3 trackside with moving block.
- Chapter 7 gives a summary and conclusions of this deliverable.
- Chapter 8 gives the references.

5 Safety Analysis with Fault Trees

This chapter presents an approach based on fault trees to derive safety requirements on the L3 trackside system specified by [2].

5.1 Motivation

The focus of the WP10 work on the moving block system of systems (SoS) is the analysis of the L3 trackside system requirements specified in [2] using FMs. Chapter 6 reports on two V&V approaches that have been performed within WP10. They basically make the textual requirements more precise to (a) investigate their consistency and (b) prove that desirable system properties follow from the requirements and some added assumptions. However, for the latter activity, they face several challenges:

1. Identification of the "desirable system properties".
2. Identification of the requirements necessary to prove those properties.
3. Identification of concepts that form a useful basis for expressing requirements, properties to be proved and the proofs themselves.
4. Identification of additional assumptions necessary to prove those properties.

These challenges can be approached bottom-up, i.e., starting from the requirements specification, or top-down, i.e., starting from goals on the SoS level (see Figure 2). Both approaches are relevant, as the proofs need to apply to systems that are built according to the given requirements, and as the proven system properties need to be such that all SoS goals are reached.

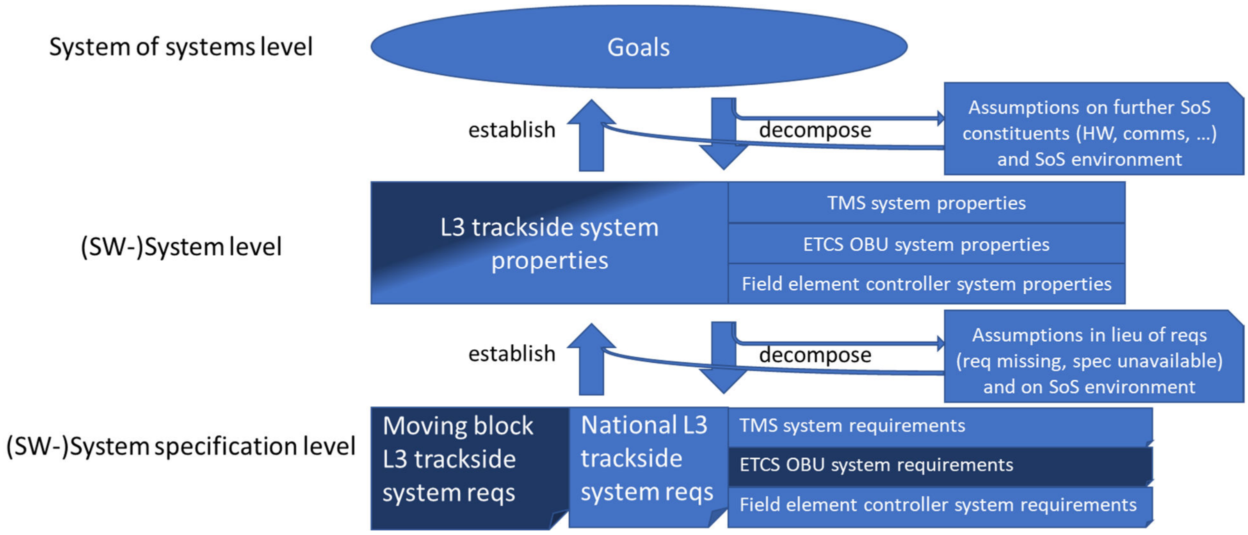
System of systems level
Goals
establish
decompose
Assumptions on further SoS constituents (HW, comms, …) and SoS environment
(SW-)System level
L3 trackside system properties
TMS system properties
ETCS OBU system properties
Field element controller system properties
establish
decompose
Assumptions in lieu of reqs (req missing, spec unavailable) and on SoS environment
(SW-)System specification level
Moving block L3 trackside system reqs
National L3 trackside system reqs
TMS system requirements
ETCS OBU system requirements
Field element controller system requirements

Figure 2 Levels involved in V&V of the moving block SoS and bottom-up vs. top-down analysis approaches. Items in dark blue have been available as input material to WP10. Any item may contain safety- and non-safety-relevant parts (e.g., safety goals, safety reqs). Abbreviations: comms = communications, req(s) = requirement(s), spec = specification.

To complement the FM V&V approaches and to connect their proven system properties systematically to SoS goals, it was decided to concentrate on safety goals that the moving block requirements contribute to, as goals of utmost importance, and to utilize fault trees without quantification as a top-down approach which enables to reason about completeness of proven system properties and requirements with respect to those goals. This chosen approach provides several opportunities which meet the above-mentioned challenges:

- Systematic identification of L3 trackside safety properties that should be proven by the FM tracks.
- Subsequently, identification/classification of safety requirements in the moving block specification.
- Sketching proofs of safety goals, including necessary assumption on other systems and actors.
- Isolating concepts that are useful from a safety perspective and comparing with concepts used in the FM tracks.

Regarding the classification of requirements in the moving block specification, those are so far not systematically distinguished in safety and non-safety requirements. A hazard analysis based on expert judgement of moving block scenarios/use cases has been conducted (Part 6 of [2]), including risk estimations, but aiming at improving the specification by including mitigation measures rather than being a complete analysis towards system realization.

5.2 Analysis Approach

This section gives a quick overview of the steps involved in the analysis. Details and results regarding each step are provided in the following Section 5.3. Input material included:

- The moving block specification [2].
- The ETCS systems requirements specification [8].
- The list of “starting point hazards” from [11].

Furthermore, the analysis was inspired by the tree-based decomposition techniques fault tree analysis [9] and Why-Because-Analysis [10]. The starting point was the general goal of safety for the SoS. The following steps were performed:

1. Prepare for the analysis by extracting relevant concepts from the input specifications and set the analysis scope by making general assumptions.
2. Identify safety goals that the L3 trackside system contributes to.
3. Turn the safety goals into top-level faults (by negation) and decompose them (by using simplified fault trees) into “leaf faults” that can be attributed either to L3 trackside or not to L3 trackside. If deemed necessary, introduce further specific assumptions to simplify the analysis.
4. Turn the leaf faults related to L3 trackside into safety properties for L3 trackside (by negation).
5. Filter out safety properties not related to the moving block specification.
6. As an auxiliary step for the following steps, identify additional basic safety properties for the L3 trackside system.
7. Identify safety requirements among the requirements of the moving block specification by finding the ones relevant for the L3 trackside safety properties.
8. Perform a gap analysis of the moving block specification by checking sufficiency of the safety requirements w.r.t. establishing the safety properties.

The last two to four steps use the moving block specification as their starting point and thus may be viewed as a bottom-up analysis complementing the previous top-down analysis ("connecting to the moving block specification").

The main outputs of the analysis are:

- Within the scope/assumptions made, a complete set of implementation-independent high-level safety properties for the L3 trackside system (output of step 4, see Section 5.3.4),
- A classification of a subset of the moving block requirements as safety requirements (step 7, Section 5.3.5.3) and
- A list of possible gaps of the moving block specification regarding safety (step 8, Section 5.3.5.4).

5.3 Analysis Steps and their Results

5.3.1 Set Analysis Scope and Prepare Analysis

As the analysis proceeds from the SoS level to the L3 trackside system level, it was first of all important to have a basic SoS purpose and architecture at hand which provides information about the systems and users involved, their interfaces and responsibilities (for a brief overview of the L3 trackside system, see Section 5 in deliverable D10.1 [4]). This provided the basic vocabulary/ontology for the analysis, like "area of control", "train", "TMS", or "dispatcher". As the SoS builds on ETCS L2, in particular regarding the interface of the L3 trackside system to trains, the ontology is further enriched by concepts from [8] like "mode" (of operation) or "movement authority". In the end, the analysis even focuses on the part of the L3 trackside system specified in the moving block specification [2], so the scope of this specification (described in Part 2 of [2]) and its relevant concepts like "track status area" and "reserved area" (Part 3 of [2]) needed to be understood.

A major scope-setting decision was to concentrate on safety properties already mentioned in Section 5.1. Besides delimiting the set of properties and thus the analysis effort, this had several further advantages:

- Relevance: The importance of safe rail operation and the contribution of a centralised trackside system to safety is undoubted, so the results of a proper analysis can be expected to be meaningful.
- Existing knowledge: Rail signalling safety and safety analysis methods are generally well-understood, so a rather complete analysis within the safety scope seems possible.
- Binary nature: Usually, a safe and an unsafe state can be clearly distinguished without discussing quantitative metrics, which enables purely qualitative analysis.
- Homogeneity: Safety properties join a common scheme (being the negation of a fault), so the same analysis method can be applied to all of them (here: a qualitative simplified fault tree analysis).

Security was not in the focus of the analysis, even if some faults identified may be (also) caused by security issues.

It was decided to start the analysis from high-level SoS faults. This was motivated by the following considerations:

- The analysis does not include any – possibly wrong – a priori assumptions on the type of signaling system. This may be considered important because a new moving block system may ensure safety in part by different principles than traditional systems.
- It is easier to conclude completeness w.r.t. overall safety of the SoS.
- The number of faults to analyse is relatively small, and so is the number of fault trees.

Finally, some generic assumptions were made to limit the scope of analysis further:

(A1) All systems involved have been installed / configured correctly.

(A2) Communication between all systems involved is free of error.

(A3) Any train or vehicle entering the area of control (except active shunting areas) needs to be made known in advance either to L3 trackside or to the dispatcher (which must react according to safe procedures, e.g., by entering train or vehicle information into the L3 trackside system). This includes entering the area of control from an adjacent area of control or from a shunting area, deactivation of a temporary shunting area, performing joining or splitting operations, and starting up operation of the area of control.

(A4) Any train or vehicle movement in the area of control is either authorized by L3 trackside or happens under responsibility of the train driver (in this case procedures to synchronize with the dispatcher need to be in order, or the movement happens within an active shunting area). In particular, trains or vehicles are secured against rollaway movements, and train drivers or any third parties will not move trains deliberately.

(A5) Should train integrity be lost, the lost vehicle(s) will immediately start to brake to standstill, so that they will never exceed the permitted maximum speed or any movement authorization provided by L3 trackside to their train or hit the rear of the train that lost them.

5.3.2 Identify Safety Goals

Starting from the general goal “The SoS shall be safe”, this was refined into a set of safety goals, subject to the following conditions:

- Only safety goals to which the L3 trackside system contributes are included. (Rationale: this is the system of interest in WP10.)
- Within the scope of the first condition, the set of safety goals is complete. (Rationale: disregarding single safety goals may lead to an unsafe SoS.)
- There are no redundant goals in the set. (Rationale: to avoid unnecessary duplicated analysis effort.)

Four safety goals were identified:

1. No derailment of train
2. No collision of train with railway vehicle
3. No collision of train with road user at level crossing
4. No collision of train with other obstacle known to L3 trackside

It is relatively straightforward to come up with examples for each goal that prove the relevance of the L3 trackside system for that goal. E.g., the system commands the points, and if it commands a position change while a train passes the point, this can result in a derailment. It is also straightforward to see that none of the goals is redundant by checking for each goal that does not imply any of the others. Whereas it is generally hard to be complete, there exist collections of safety goals or – the other way round – safety hazards for the railway system which can be assumed complete. Such a collection, the list of “starting point hazards” from the ROSA project [11], was consulted to check against. In fact, for each starting point hazard it was concluded that it either affects one of the safety goals above (and thus is subsumed in its analysis) or the L3 trackside system is not responsible for its prevention.

5.3.3 Decompose Top-level Faults

Each of the safety goals identified in the previous step was negated to obtain a top-level fault that was subsequently decomposed using a simplified fault tree. The tree for the top-level fault “(ETCS-controlled) Train derails (in area of control of L3 trackside system)” is shown in Figure 3. Further assumptions were added to the generic ones (cf. Section 5.3.1) to simplify the decomposition of the specific top-level faults; for example, for the derailment fault, the following two assumptions were formulated:

(A6) The train and the track it is running on are generally constructed (e.g. material and geometry of track and wheelsets, axle load) to allow safe operation.

(A7) For the specific train, track, and operational situation (e.g., strong cross winds) there is a defined permitted maximum train speed that allows safe operation.

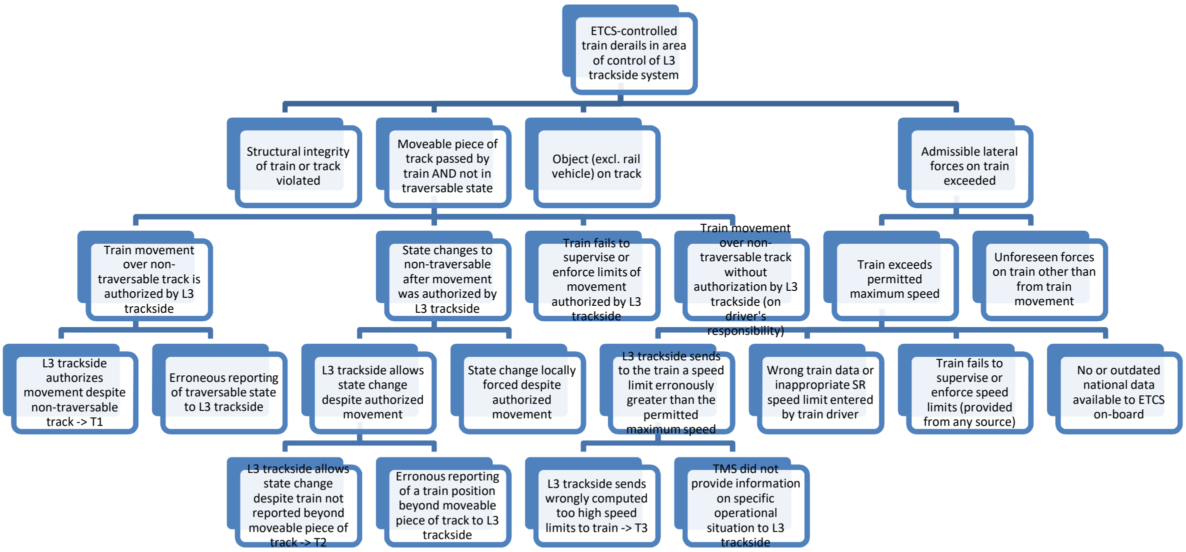
ETCS-controlled train derails in area of control of L3 trackside system
Structural integrity of train or track violated
Moveable piece of track passed by train AND not in traversable state
Object (excl. rail vehicle) on track
Admissible lateral forces on train exceeded
Train movement over non-traversable track is authorized by L3 trackside
State changes to non-traversable after movement was authorized by L3 trackside
Train fails to supervise or enforce limits of movement authorized by L3 trackside
Train movement over non-traversable track without authorization by L3 trackside (on driver's responsibility)
Train exceeds permitted maximum speed
Unforeseen forces on train other than from train movement
L3 trackside authorizes movement despite non-traversable track -> T1
Erroneous reporting of traversable state to L3 trackside
L3 trackside allows state change despite authorized movement
State change locally forced despite authorized movement
L3 trackside sends to the train a speed limit erronously greater than the permitted maximum speed
Wrong train data or inappropriate SR speed limit entered by train driver
Train fails to supervise or enforce speed limits (provided from any source)
No or outdated national data available to ETCS on-board
L3 trackside allows state change despite train not reported beyond moveable piece of track -> T2
Erronous reporting of a train position beyond moveable piece of track to L3 trackside
L3 trackside sends wrongly computed too high speed limits to train -> T3
TMS did not provide information on specific operational situation to L3 trackside

Figure 3 Fault tree for top-level hazard “train derails”

The decomposition of a node into a set of child nodes was repeatedly performed according to the following rules, starting with top-level fault node, and resulting in the fault tree:

- If a fault can be attributed to either the L3 trackside system or not the L3 trackside system, its node is not further decomposed.
- Otherwise, it is decomposed by giving a set of child nodes labelled with faults such that:
  - Each child node fault is a possible cause of the parent node fault.
  - None of the child node faults is redundant (i.e., a special case of another one).
  - Together, and under the generic and specific assumptions, the child node faults cover all conceivable causes for the parent node fault.

Example

The top-level fault node in Figure 3 (“train derails”) was further decomposed because derailments may be caused e.g. by wrong speed or distance limits sent by L3 trackside, but may also be caused e.g. by some object on the track, without any L3 trackside fault being involved.

For systematic decomposition of the derailment fault, derailment is by definition a situation where wheels are no longer guided by the rails. If caused by trackside, this means that the geometry of a piece of track is or becomes non-appropriate when passed by the train, which may be due to geometry change foreseen by system design (“moveable piece of track not in traversable state”) or not (“structural integrity of track violated”). If caused by trainside, any change in wheel geometry relative to track that leads to derailment is not foreseen by system design (“structural integrity of train violated”, e.g., broken axle). If geometry of both trackside and trainside is ok there still may be forces that lift wheels from the rails (forces drawing away the rails under the wheels are considered negligible). Such forces may originate from touching physical objects (“object on track”, where collisions with rail vehicles are excluded because they are another top-level fault that is handled separately) or from elsewhere (“admissible lateral forces exceeded”, where upwards vertical forces other than from touching physical objects are considered negligible).

The “complete decomposition” approach taken here, which repeatedly divides the fault into a set of complementary sub faults, implies the desired non-redundancy and (practical) completeness properties (provided that the exclusions made are in fact practically negligible). Furthermore, the relevance property can be established by giving examples of the sub faults.

Furthermore, for the fault tree to be comprehensible, the number of child nodes had to be sufficiently small (in our case, no more than four child nodes were used), and the faults had to be formulated with care (where necessary, terms were explicitly defined). Another simplification compared to usual fault trees is that no explicit logical gates were used; the decomposition of a parent node into child nodes can be regarded as an implicit OR gate, and no AND gates were needed.

In practise, provided that the decompositions are chosen to isolate L3 trackside faults, the above procedure terminates after a limited number of decomposition steps, delivering a set of leaf nodes whose faults can be either attributed to the L3 trackside system or not to the L3 trackside system. For the derailment top-level fault, it can be seen in Figure 3 that eight decomposition steps were done; the three leaf nodes with L3 trackside faults were added a label “-> Tn”, 1≤n≤3. According to the above decomposition rules, the identified L3 trackside faults are correct (i.e., relevant) and complete w.r.t. the top-level fault.

5.3.4 Establish Safety Properties for L3 Trackside

By negation of the L3 trackside faults identified through the decomposition of the top-level faults, one obtains safety properties for the L3 trackside. For example, for the derailment top-level fault, reusing the labels of the leaf nodes from Figure 3, the following safety properties were obtained:

(T1) L3 trackside shall never authorize a train movement[2] over a moveable piece of track[3] if it has not been reported traversable to L3 trackside.

(T2) L3 trackside shall never allow change of a moveable piece of track[3] to a non-traversable state if it authorized a train movement[2] over that piece of track and the train has not yet reported beyond that piece of track.

(T3) L3 trackside shall never compute speed limits to be sent to a train wrongly too high.

Further safety properties obtained from decomposition of the other top-level faults were:

(T4) L3 trackside shall never authorize a train movement[2] over a piece of track that is known to be occupied or to be used by a vehicle unless in OS mode, SR mode or for joining.

(T5) L3 trackside shall never authorize a vehicle movement[2] into a forbidden area[4].

(T6) L3 trackside shall never authorize a train movement[2] without having established forbidden areas[4] at (a) each track branching from the authorized track and (b) each track that has an overlapping clearance gauge with the authorized track, such that the forbidden areas prevent vehicles from flank and touching collisions with the authorized train when not entered, even when the train exceeds the structure gauge.

(T7) L3 trackside shall never remove a forbidden area[4] if it authorized a train movement[2] that is protected by that forbidden area at some branch or track with overlapping clearance gauge and the train has not yet reported beyond the branch or track with overlapping clearance gauge.

(T8) L3 trackside shall never authorize a too far vehicle movement[2] towards a forbidden area[4] for a vehicle that exceeds the clearance gauge.

(T9) L3 trackside shall never wrongly remove or change its information about a vehicle and its position.

(T10) L3 trackside shall never authorize a train movement[2] over an LX which has not reported protected status to it and does not report its status to a LEU without having included sufficient restrictions[5] to pass the LX safely.

(T11) L3 trackside shall never command/agree to opening of a level crossing over which it authorized a train movement[2] and the train has not yet passed the level crossing.

[2] Authorisation of a train movement by L3 trackside may be done by sending an MA (possibly with OS profile), an SR authorization or a reversing distance to the train. It does not matter who triggered the authorisation (automatic route setting via TMS, dispatcher via TMS, train or train driver through request).

[3] The only moveable piece of track known to be managed by L3 trackside is a point. A point is considered traversable for a train approaching it precisely if it is locked in an end position and, in case of a train passing the point trailing, the end position corresponds to the point's leg the train will travel.

[4] A forbidden area is a (connected) track area where no railway vehicle is supposed to be.

[5] Such restrictions may be given by speed restrictions, an obligation to stop before the level crossing, or the obligation for the driver to secure the LX or ensure that it is free of obstacles. Technically they may be part of an MA (packet 15), speed profile (packet 27), level crossing information (packet 88), the authorized mode (SR mode implies driver responsibilities and mode speed limit V_NVSTFF, reversing speed limit V_REVERSE in packet 139) or national rules or additional national/local information. It may also be the case that e.g., reversing over an unprotected LX is not considered sufficiently safe at all so that (T10) effectively forbids it.

(T12) L3 trackside shall never compute track condition “sound horn” to be sent to a train wrongly or miss to include them in an MA for approaching/passing a passive level crossing, unless only driver information via trackside signs is foreseen.

(T13) L3 trackside shall apply a safety reaction immediately if an obstacle on a piece of track where it authorized a train movement[2] becomes known.

(T14) L3 trackside shall never authorize a train movement[2] without having included sufficient restrictions to pass any obstacle on the authorized piece of track that has been reported to L3 trackside and has not yet been reported no longer present.

From the correctness and completeness of the safety goals w.r.t. the railway system (see Section 5.3.2), the correctness and completeness of the L3 trackside faults w.r.t. the top-level faults related to the safety goals (see Section 5.3.3), and the correct and complete separation into L3 trackside and non L3 trackside portions, it follows by transitivity that the set of safety properties obtained for L3 trackside is correct and complete. Of course, this is relative to assumptions made along the way and subject to the assumption that the methodology has been applied correctly in each step and its inputs (in particular the ROSA starting point hazards) can be trusted and are applicable to a moving block railway SoS.

5.3.5 Connect to Moving Block Specification

Having identified a correct and complete set of safety properties for a L3 trackside system relative to some assumptions (see Section 5.3.4) enables analysis of the moving block specification [2] w.r.t. safety: it becomes possible to identify safety requirements and rules among all the requirements and rules, to reason why they are indeed safety relevant and to identify potential safety gaps in the specification. Regarding the generic and specific assumptions made (see Sections 5.3.1 and 5.3.3), those were checked to be consistent with the moving block specification. For parts of them this was explicitly the case (e.g., generic assumption A4 above is partly covered by the operational rules OPE-Generic-6[6]/9 from Part 4 of [2], for the other parts at least no contradiction with the specification could be identified.

5.3.5.1 Filter out Safety Properties not related to the Moving Block Specification

However, as the moving block specification only partially specifies the L3 trackside system, it needs to ensure the safety properties only together with national specifications of interlocking functions and operational procedures, and with the ETCS specification [8]. Thus, in a first step, safety properties that only relate to those additional specifications were identified and removed from the scope of further analysis. This concerned safety properties T3, T5-T8 and T10-T12, because computing/sending speed restrictions, providing protection against flank/touching

[6] Some safety relevant requirements and operational rules from the moving block specification allow for exceptions for degraded situations so that the usual safety properties are violated. Consequently, safety needs to be ensured differently than in nominal situations. This can often be done by excluding them from the main safety analysis (as was done here) and to defer them to a separate safety analysis (not done here). This separate analysis may prove, e.g., by referring to operational procedures, a somewhat weaker but still sufficient safety property for the degraded situation and that returning to the nominal situation will reestablish the usual safety property.

collisions incl. consideration of trains/vehicles that exceed the clearance gauge, and providing level crossing safety are functions that are not specified by the moving block specification.

5.3.5.2 Establish Additional Basic Safety Properties for L3 Trackside

For the analysis of the remaining six safety properties, it turned out to be easier to formulate a few additional basic safety properties that the analysis can refer to, to avoid redundancy. To do so, in a first step basic principles of the L3 moving block SoS that contribute to establishing the safety properties were identified:

- At any time (except for initialisation) and for its whole area of control, L3 trackside maintains areas where trains or sets of railway vehicles may potentially be (track status areas associated with trains or train lengths, and reserved areas).
- Any movement of a train within the area of control of a L3 trackside system needs to
    - either be directly authorised by the L3 trackside system (movement authority, SR authorisation, reversing distance and speed),
    - or be indirectly authorised by the L3 trackside system (by sending route related information to an adjacent L3 trackside system or RBC)
    - or be authorised by the dispatcher (SR movement of non-communicating trains),
    - or take place within a permanent or active temporary shunting area (SH movement).

The L3 trackside contributions to realise those principles are:

(T0a) correctly updating (creating, removing, extending, reducing) the areas where trains or sets of railway vehicles may potentially be upon receipt of new information from adjacent L3 trackside/RBC systems or through dispatcher inputs, and

(T0b) ensuring that any authorisations sent directly or indirectly to a train are within the maintained area where this train may potentially be.

Similarly, it is a SoS principle that L3 trackside may – as far as information is provided to it – maintain areas where obstacles may potentially be (unknown track status areas). The L3 trackside contribution to realise this principle is:

(T0c) correctly updating (creating, removing, extending, reducing) the areas where obstacles may potentially be upon receipt of new information from adjacent L3 trackside/RBC systems or through dispatcher inputs.

5.3.5.3 Identify Safety Requirement in the Moving Block Specification

Requirements from the moving block specification contributing to the L3 trackside safety properties – and thus being safety requirements – could be identified as follows:

- For T0a: REQ-TrackStatus-6, REQ-TrackStatus-22 (area creation for trains entering the area of control), REQ-TrackStatus-4/5 (area creation/extension for trains performing SoM), REQ-TrainLoc-7 together with REQ-TrackStatus-7 (area maintenance upon reception of position report), REQ-Reserved-10 (area reduction/removal).
- For T0b: REQ-MA-2, REQ-HO-1, REQ-MovSR-1, REQ-MovSR-3 and REQ-Rev-3. Furthermore, the sentence “only allow shunting in predefined areas” from the introduction of Chapter 3.20
- For T0c: REQ-TrackStatus-22/23/24 (unknown track status area creation/extension).

- For T1: the sentence “All the necessary protections need to be in place before a Reserved Status Area is created or extended, e.g., points in flanks or overlap must be in the requested position, as for locked routes in a Level 2 system.” from the introduction of Chapter 3.3. Note that also T0b and T0a are required to establish T1.
- For T2: REQ-PTS-1, REQ-PTS-2. Note that also T0b and T0a are required to establish T2.
- For T4[7]: REQ-MA-3, REQ-MA-7/8, REQ-Reserved-2/3, REQ-Reserved-6/7. Note that also T0b and T0a are required to establish T4.
- For T9: This follows from T0a.
- For T13: REQ-TrackStatus-26. Note that also T0c is required to establish T13.
- For T14: REQ-MA-3. Note that also T0c is required to establish T14.

5.3.5.4 Perform Gap Analysis of Moving Block Specification

- For T0a:
  - A requirement seems missing to ensure that when unknowns with reason “created at initialisation” are removed according to REQ-TrackInit-4, all trains are inside some other track status or reserved areas.
  - There are lots of situations where areas may be removed/reduced (e.g. REQ-TrainLoc-8/9 together with REQ-TrackStatus-7, REQ-TrackStatus-14/15, REQ-PTS-4, REQ-TrackStatus-18-20, REQ-Reserved-8/9, REQ-EoM-1/3, REQ-SH-5), but except for REQ-Reserved-10 there is no explicit exclusion of unsafe removals/reductions of areas.
- For T0b:
  - For reversing, the requirement is slightly weaker than required by T0b as an area where the train may reverse is only created if the train changes to RV and thus actually uses the “authorisation to reverse” that has been received earlier. However, this possible violation of T0b, usually for a very short period of time, is justified due to a conflicting safety goal, namely, to enable train drivers to start reversing immediately and independent of the L3 trackside system in case of emergency.
  - For shunting, there are no explicit requirements that ensure T0b. Such requirements could be that an SH authorisation is only sent to trains completely located inside an active shunting area, and that supervision of the border of the shunting area is either done by sending a list of balises for shunting or by a safety reaction upon border violation detected by TTD.
- For T0c:
  - A requirement seems missing to ensure that when unknowns with reason “created at initialisation” are removed according to REQ-TrackInit-4, all obstacles known to L3 trackside are inside some other unknown track status area.
  - There are situations where unknown track status areas may be removed/reduced (e.g., REQ-TrackStatus-24), but there is no explicit exclusion of unsafe removals/reductions of areas.

[7] Note that because T4 holds symmetrically for the vehicle that occupies or uses the piece of track, it should be impossible that after authorisation of the train a piece of track over which the authorisation has been granted becomes occupied or used by a train. In case such a situation occurs erroneously nevertheless, REQ-TrackStatus-26 will take care.

- For T1: There are no explicit requirements that ensure T1.
- For T2:
    - REQ-PTS-03[6] undermines REQ-PTS-01 by adding an exception so that T2 is no longer ensured for SR and RV movements. At least REQ-PTS-03 requires that "other safety conditions are met", so that the reader is made aware of the need to design such conditions carefully.
    - The moving block spec does not imply T2 for moveable pieces of track other than points.
- For T4: For the case that the authorisation refers to reverse movements, a requirement is missing which ensures that reversing area information is only provided to a train if the area where the train may reverse is free of other trains.
- For T9: See gap analysis for T0a.
- For T13: A similar requirement like REQ-TrackStatus-26 to prevent reversing trains (where the Reserved Area has changed to an Unknown Track Status Area according to REQ-Rev-2 and REQ-Rev-3) from collisions with obstacles seems missing, or it should at least be stated that this is intentionally not included.
- For T14: A requirement to prevent reversing trains from collisions with obstacles seems missing, or it should at least be stated that this is intentionally not included.

6 FMs-based Analyses

The general goal of using FMs for "System Inception" is to help achieve system requirements that are clear with respect to how they satisfy user needs and shall be implemented and verified (independent of whether FMs are used or not for those purposes). This aims to facilitate that multiple stakeholders understand and implement requirements in the same way, and to ensure desired system properties (e.g., interoperability, safety, reliability, standards compliance).

This chapter describes results from two different FMs application approaches, one object-based approach and one based on refinement; their ontology and properties are described in deliverable D10.1 [4] and the formal model creation and V&V is described in deliverable D10.6 [6].

6.1 Introduction

As identified in WP10's requirement analysis (see [4] Section 6.3), the moving block specification [2] provides a partial specification in several respects[8]:

- It is a bit vague on standard principles that shall apply.
- It does not describe a mechanism for protecting a train that may reverse.
- It lacks requirements (or assumptions) for interlocking functionality.
- It does not specify any means to prevent any authorization into a section of track, e.g., if there is maintenance or construction ongoing (a user's need).
- It does not specify any assumptions for when the initialisation procedure completes. This should be considered a "safe state", to enable to reason that actions of L3 trackside maintain a safe state.
- It does not describe operational scenarios, to help determine proper system behaviour.

Since the moving block specification [2] does not systematically distinguish which requirements are to be considered safety requirements, the two FMs application tracks defined their own safety requirements. Neither of the FMs application tracks modelled the Track Status Area (TSA) concept in the moving block specification [2], because the assessment was that the TSA concept is not sufficiently clear to be straight-forward to formalize (clarification of this concept is needed).

6.2 Object-Based Approach

In this track, the formal model used for verification and validation (V&V) was based on an ontology in which each concept is an object type. Generic properties representing assumptions and properties to verify were expressed in terms of object types (see [4] Section 7.2), as invariants and transition requirements. The formal model was created by instantiating the generic properties using example system configurations (specific track layouts). This track used the Prover iLock tool suite, and formal analyses were based on a model checker for the language HLL.

[8] Presumably due to dependency on non-harmonised principles and requirements.

The V&V that was carried out was focused on the following primary validation goals:

1. Validate that ontology concepts and associated properties are consistent (without contradiction).
2. Validate that properties one expects to follow from assumptions made indeed can be proved.
3. Validate dynamic behaviour permitted by assumptions made.

The above goals could be achieved, but results are partial and experimental, e.g., since V&V was limited to specific system configurations, and many scope-reducing assumptions were made:

- A nominal mode assumption made was that trains only move within authorities granted.
- Validation goal 2 did not attempt generic proof of properties independent of system configuration (due to work bandwidth reasons).
- Validation goal 3 was used for debugging purposes (in lieu of having an executable model that can be tested/simulated) but not systematically, to validate all kinds of behaviour.

Ideally, it should be obvious that important safety requirements, such as that trains will not collide (front-to-front, front-to-rear, sideswipe) follow from standard principles and requirements. In this ontology, the Train Location Path concept represents where a train is, and the nominal mode assumption is that a train only moves within an Authority Path granted to it. The next section 6.2.1 recapitulates the standard principles for Authority Paths (from [4] Section 7.2), and Section 6.2.2 outlines possible assumptions to ensure the following two general safety requirements:

- R1: Authority paths for different trains shall not overlap.
- R2: Occupied train location paths for different trains shall not overlap.

6.2.1 Standard Principles

The standard principles for Authority Paths are based on generalising how Movement Authorities are constrained by Reserved Paths in the moving block specification. The idea of these standard principles is to treat any Authority Path the same way:

- An **Authority Base (AB)** path is the basis for an authority path (as a principle).
- An **Authority Path (AP)** is a prefix path of an AB path (as a principle).
- AB paths shall not intersect (as a principle).
- A train is associated with at most one AB path at a time (as a principle).
- An AB path must be created before an AP path within the AB path is created (as a principle).

To remove an AB path requires that the train has no AP within the AB path, or that the AB and AP paths are removed at the same time. To remove an AP for a train requires that L3 trackside knows the train will have removed the corresponding authority in the onboard system.

The restrictions for authority paths are described in Table 2. Table rows with indices 1 and 2 are the preferred authorities, used when possible. SR distance is represented by two types of authority paths (SR_DIST1 and SR_DIST2), corresponding to that SR distance can be issued in two types of AB paths. The Forbidden Authority Base path is special in the sense that no Authority Path within is allowed. Figure 4 provides a graphical illustration of the authority paths.

Index	Authority Base (type)	Authority Path (type)	Authority Path restriction
1	Reserved Path (RP)	Movement Authority (MA)	Prefix path of RP
2	Reserved Path (RP)	SR distance (SR_DIST1)	Prefix path of RP
3	AB_SR	SR distance (SR_DIST2)	Prefix path of AB_SR
4	AB_RV	RV distance (RV_DIST)	Prefix path of AB_RV
5	Forbidden (FORB)	<intentionally empty>	<intentionally empty>

Table 2 Authority paths within AB paths

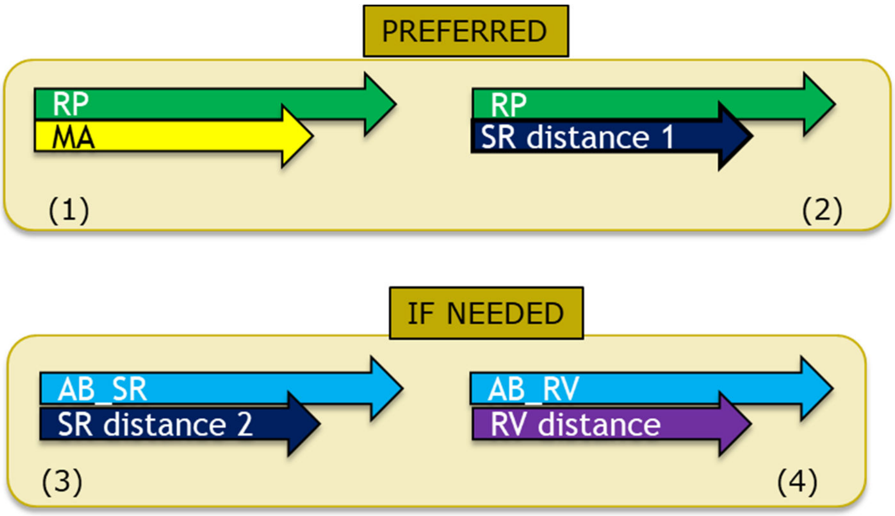

Figure 4 Authority paths within AB paths (illustration)

The train location path (TLP) concept merges two concepts in the moving block specification: train location, and the (Unknown or Occupied) Track Status Area (TSA) that a train is associated with[9]. It has a Status attribute that can be either Unknown or Occupied, to correspond to when the TSA that a train is associated must be Unknown or Occupied (according to the moving block specification). A TLP also has a TL attribute (for train location), set to False when a train is considered to not have a train location, such as when the ETCS session timer expires. The TLP path's extent can modify, aiming to correspond to how the TSA that a train is associated with shall modify its extent (according to the moving block specification).

To create an Authority Base path for a train requires that the train has a Train Location Path (TLP). An AB path is adjacent to either the rear or front of the train's TLP (see Figure 5):

- Rear of RP and AB_SR paths are adjacent with front of the TLP (they are in the same direction).
- Rear of AB_RV is adjacent with the rear of the TLP (they are in opposite direction).

[9] Cf. REQ-TrackStatus-7: When the L3 Trackside has updated the Train Location for a train, then the Track Status Area associated with this train shall be updated accordingly.

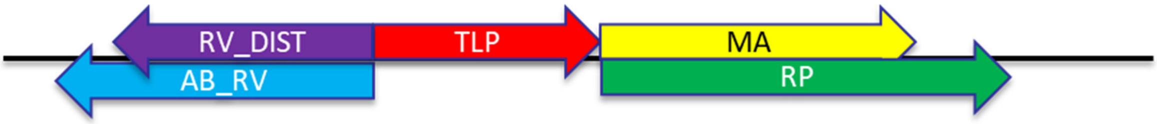

Figure 5 Adjacency of TLP and AB paths

A TLP can begin outside the Area of Control and end at its border, corresponding to an incoming handover path (e.g., a statically defined path). If the train enters the Area of Control, this corresponds to a "normal" train movement based on a train position report (see Figure 6).

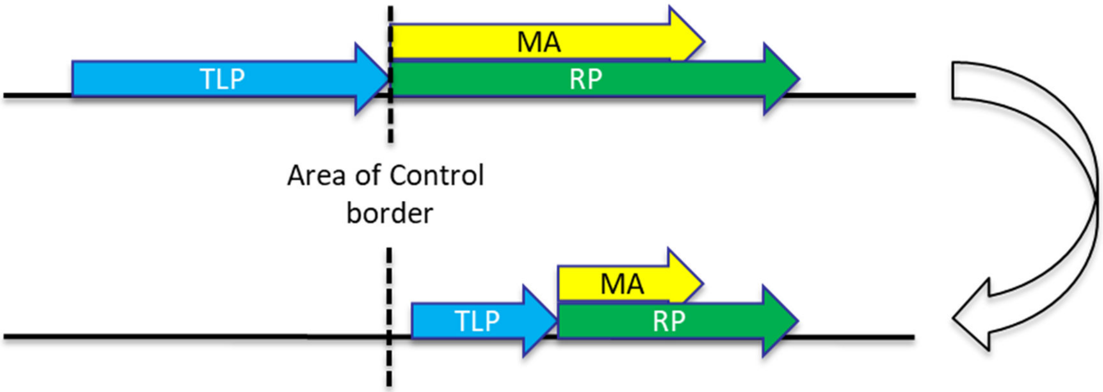

Figure 6 Entering Area of Control in Handover

Join and split operations are assumed to be compartmentalised to only take place within dedicated paths[10] for split and join (created by the TMS), to enable to distinguish when loss of train integrity is expected, and when a RP is allowed to overlap an Occupied TLP[11]. Figure 7 illustrates a join path; when this is created, its Train to be Joined (TTBJ) is at standstill and its TLP is entirely within the join path, and the join path does not overlap any AB path or TLP not associated with either the TTBJ or the Joining Train (JT).

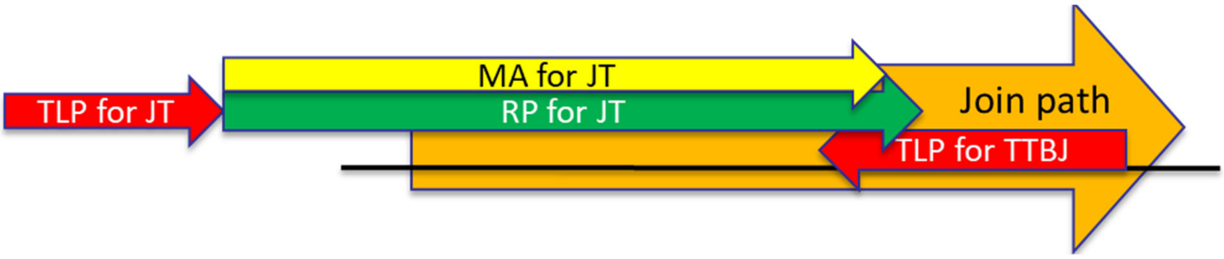

Figure 7 Path for joining (JT: joining Train, TTBJ: Train to be Joined)

[10] The direction of a join or split path is not significant.

[11] Join and split operations are expected to result in reported loss of train integrity. For joining, a Reserved Path (RP) shall be allowed to overlap an Occupied TLP, to enable the joining train to move close enough.

6.2.2 Assumptions for Safety

These safety requirements were identified as relevant properties to be ensured by L3 trackside:

- R1: Authority paths for different trains shall not overlap.
- R2: Occupied train location paths for different trains shall not overlap.

This section outlines assumptions needed for the above safety requirements, in addition to standard principles (see Section 6.1.1.):

- Properties assumed to hold when the initialisation procedure completes.
- Properties assumed to hold for all state transitions after completing the initialisation procedure.

Before the initialisation procedure for L3 trackside has completed, trains that are physically present in the Area of Control may not yet be known to L3 trackside. As a simplification, the states before completion of the initialisation procedure of L3 trackside are excluded from scope.

The following assumptions are made about the state when the initialisation procedure completes:

1. Each train that is physically present in the Area of Control is located within a train location path whose length is at least as long as the train.
2. Train location paths are disjoint (not overlapping).
3. Authority Base paths are disjoint (not overlapping).
4. If a fouling path (associated with a point or a track crossing) intersect a train location path, an Authority Base path, or a path for split or join, then the associated point or track crossing shall be locked, and no other conflicting fouling path intersects any of those types of paths.
5. A forbidden path does not overlap a train location path, or a path for split or join.
6. A path for split or join does not overlap another path for split or join.

After the initialisation procedure has completed, the above assumptions are maintained by any state change of L3 trackside (in its reaction to new input events). Additionally, train location paths are only created and removed because of:

7. Train entering the Area of Control within an Authority Base path from the Area of Control border.
8. Train leaving the Area or Control based on confirmation that it left the Area of Control using a Train Position Report or a TMS command (if need be).
9. Train confirmed to have joined with another train (within a path for joining).
10. Train confirmed to have split from another train (within a path for splitting).

The only authorisations that can be granted to a train to enter a train location path associated with another train is using On Sight (OS) or Staff Responsible (SR) mode, in which case L3 Trackside delegates safety responsibility to the train driver (and/or the dispatcher and/or other staff). If the train location path is Occupied, a train can only be authorised to enter it if it is the Joining Train and the train location path is entirely within a path for joining.

6.2.3 V&V

The FMs-based V&V that was carried out was lightweight in the sense that it was focused on validating the ontology and associated properties, using example system configurations:

1. Validate that ontology concepts and associated properties are consistent (without contradiction).
2. Validate that properties one expects to follow from assumptions made indeed can be proved.
3. Validate dynamic behaviour permitted by assumptions made.

For the first and second goal, example system configurations were used as basis for proving properties of interest, such as the lemmas based on transitive closure of next/previous relations for directed segments (see [4] Section 7.2.3.5) and safety requirements R1 and R2 (see Section 6.2.2).

For the last goal above, formal verification of falsifiable properties was used for debugging purposes, in lieu of having an executable model that can be tested/simulated. These properties were defined as a sequence of events that should not be reachable, so that a counter example to a property (obtained using formal verification) demonstrates the sequence of events. Such properties were used to validate behaviour allowed by the assumptions (see Figure 8), and to identify mistakes (e.g., a sequence of events may be impossible due to an erroneous assumption). This was however not done systematically, to validate all kinds of behaviour.

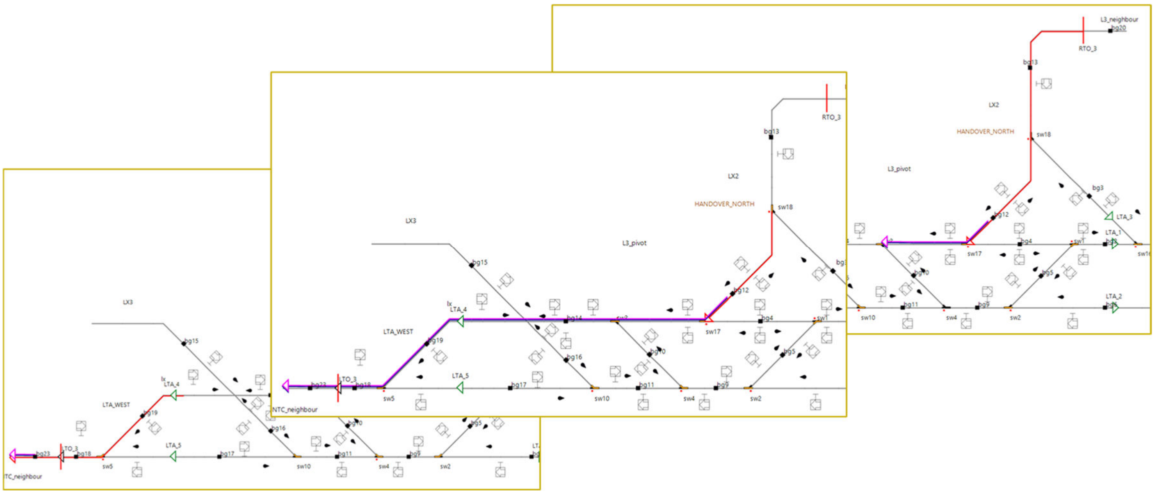

Figure 8 Counter example visualization

The V&V helped identify several intermittent issues and mistakes in the model along the way (e.g., because the system was contradictory, or did not allow a certain event sequence), and missing assumptions (e.g., because unrealistic behaviour was allowed).

The V&V helped identify nominal mode assumptions required to prove properties of interest, e.g., if a train has been authorised (in On Sight mode) to enter another train Unknown train location path (TLP), and the TLP transitions to Occupied, the TLPs shall not become overlapping because of the TLP transitioning to Occupied (without this assumption, Occupied train location paths could become overlapping). This assumption was deemed reasonable for the purpose and scope of this analysis. Figure 9 illustrates a situation in which this nominal mode assumption applies:

- Train T1 loses communications, causing its TLP to become Unknown.
- Train T2 is authorised to enter the Unknown TLP of train T1, using an On Sight mode profile.
- Train T2's TLP enters the TLP of Train T1.

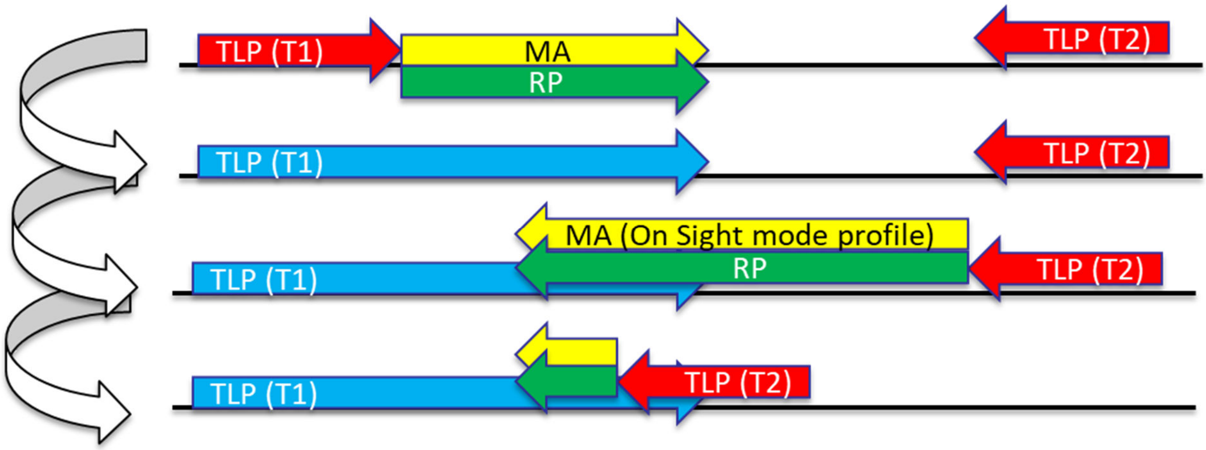

Figure 9 Train T1 loses communications, and then T2 is authorised to enter T1's Unknown TLP

V&V results also raised questions about what the proper behaviour of L3 trackside shall be in various situations, e.g., if a Movement Authority becomes overlapping with an Occupied train location path even if this is not related to a join operation (presumably, L3 trackside shall react to transition the system to a safe state based on requirement REQ-TrainLoc-12 [2]).

V&V results also include identified issues in the moving block specification, e.g., that two conflicting reactions by L3 trackside are specified by requirements REQ-Rev-3 and REQ-LossTI-2 [2], if train reports entering RV mode at the same time as it reports loss of integrity.

6.3 B-Method Refinement-Based Approach

This section presents the formal verification activity carried out on the B Model of the Moving Block system created within WP10 of X2Rail-5 project. Section 6.3.1 presents the general principles of formal verification of a B Model constructed by stepwise refinement. Section 6.3.2 deals with the properties defined in the B Model of the Moving Block that must be formally verified. First, it presents the concepts used by the properties, then the properties themselves, and finally the actions that must preserve them. Section 6.3.3 presents the traceability of the properties identified in the safety analysis in Section 5 with the properties of the B Model. Section 6.3.4 deals with the verification results and with some general remarks on the formal verification activity.

6.3.1 Verification of a B Model Created by Stepwise Refinement

The B Model of the Moving block system was created following a refinement-based approach. This is a stepwise method to incrementally create formal models of systems. The first step is an abstract, and generally incomplete, model of the system defining important properties of its data and actions. The N+1th step transforms the model of step N into a more detailed, complete or concrete model defining the properties of the introduced data and actions and the relationships between the data and actions of this step and the data and actions of the previous step.

In the B-Method a formal model involves at most three parts. The definition of static data, formalised by constants and their properties; the definition of dynamic data, i.e., the state of the system, formalised by variables and their properties; and the definition of the initial state of the system and of the actions that change its state, the latter formalised by guarded commands. A guarded command is defined by a condition triggering the action and an assignment defining the effect of the action on the state of the system.

From a V&V perspective, one of the goals of the stepwise refinement process is to allow to break down the proof of a complex model into the proofs of simpler models. Thus, the formal verification of a model created by stepwise refinement consists in the formal verification of the model of every refinement step. More precisely:

- The verification of the model of the 1st step aims to ensure that the initial state of the system defined in step 1 satisfies the properties of the state of the system defined in step 1, and that every action A_1 of the system defined in step 1 preserves those properties.
- The verification of the model of the N+1th step aims to ensure: 1) that the initial state defined in step N+1 satisfies the properties of the state of the system defined in step N+1 and is consistent with the initial state defined in step N; and 2) that every action AN+1 of the system defined in step N+1 preserves the properties of the state of the system defined in step N+1 and that its effects are consistent with the effects of a corresponding action AN defined in step N.

Thus, the formal verification of the models of all the refinement steps ensures that the model of the last step encompasses the properties of all the steps, that its initial state establishes these properties and that each of its actions has effects consistent with the corresponding actions of previous refinements and preserves all the properties.

Four refinement steps were performed to create the B Model of the Moving Block system.

- The 1st step, named RSS0, defines a very basic system essentially managing train protection areas to ensure that trains moving in two different train protection areas avoid front-to-front, rear-to-front and rear-to-rear collisions.
- The 2nd step, named RSS1, adds to the model of the 1st step some basic interlocking principles to ensure that trains moving in a train protection area avoid flank collisions and do not derail.
- The 3rd step, named RSS2, adds to the model of the 2nd step general protection areas which are a generalisation of train protection areas introduced in the 1st step and model concepts of the Moving Block specification, notably, Track Status Areas.
- The 4th step, named RSS3, adds to the model of the 3rd step a very basic the model of the onboard system and of data exchanged between trackside and onboard systems. The aim of this step is to formalise the interactions between the trackside system and the onboard systems.

6.3.2 B Model of the Moving Block

This section presents the three parts of the B Model of the Moving Block. The first subsection presents the concepts used to define the static data of the B Model, the second subsection presents the concepts used to define the dynamic data of the B Model. Based on the static and dynamic data concepts, the third subsection presents the properties to be verified, and the last subsection lists the actions of the system modelled by the B Model.

6.3.2.1 Static data

The static data of the B Model of the Moving Block is created with the concepts presented in the Table 3 below. The first column of the table presents the name of the concept. The second column presents the name of the refinement step at which the concept was introduced in the B Model. The third column presents a brief description of the formal structure of the concept. And the fourth column presents the rationale or the idea behind the concept.

Concept	Step	Description	Comment
Train	RSS0	A train identifier	
Location	RSS0	An atomic referenceable portion of a track	The set of all locations is an unorganised representation of the AoC.
Area	RSS0	A set of locations	An area is an unorganised representation of part of the AoC.
Speed limit on location	RSS0	Natural number associated to a location	Maximum speed allowed on locations.
On-sight speed	RSS0	Natural number	Maximum speed in potentially hazardous areas. It is not necessarily the speed of ETCS OS mode.
Protection	RSS0	Protection identifier	A protection id identifies an area of the AoC.
Switch	RSS1	A switch identifier	
Next (S)	RSS1	Given a set S of uniquely positioned switches (a switch configuration), Next (S) is a binary relation on oriented locations.	Next (S) is an organised representation of the AoC defining the consecutivity of oriented locations taking into account the position of switches defined by S.
Path	RSS1	Given a switch configuration S, a path is a totally ordered set of consecutive oriented locations according to Next (S).	A path represents an oriented continuous section of track.
Incompatible locations	RSS1	Couple of locations	Locations that cannot be locked simultaneously
Switch locking area	RSS1	Area associated to a switch	Locations aimed to keep locked the switch if they are occupied or reserved for a train.
Route	RSS1	Route identifier	A route is a statically named path.

Concept	Step	Description	Comment
Route locking area	RSS1	Area associated to a route	Locations at the rear of a route aimed to keep the route locked if they are occupied or reserved for a train.
Switch sweeping area	RSS2	Area associated to a switch	Locations that must be swept simultaneously.
Shunting	RSS2	Shunting area identifier	
Shunting area	RSS2	Area associated to a shunt	Locations out of the responsibility of the system when the shunting area is active.
EoA Exclusion	RSS3	EoA exclusion area identifier	
EoA exclusion area	RSS3	Area associated to an EoA exclusion	Locations forbidden for MAs to end.
Radio hole	RSS3	Radio hole identifier	
Radio hole area	RSS3	Area associated to a radio hole	Locations where a movement authority cannot be.
Mute Timer	RSS3	Natural number	Timeout before communication loss.
Session Timer	RSS3	Natural number	Timeout before end of session.
Integrity Timer	RSS3	Natural number	Timeout before integrity loss.
Length of locations	RSS3	Natural number associated to a location id.	1 for FMB, block length for FVB, in the measurement unit.

Table 3 Concepts of the static data of the B Model of the Moving Block

6.3.2.2 Dynamic data

The dynamic data, i.e., the state, of the B Model of the Moving Block system are created with the concepts presented in below.

Concept	Step	Description	Comment
Status of trains	RSS0	Train status associated to a train id.	Status of trains known to FMB. A train is Active if it is allowed to move, Inactive, otherwise.
Protection area of trains	RSS0	Area associated to a protection id.	Locations where trains can move safely. Several trains may be associated to the same train protection area.
Protection of trains	RSS0	Protection id associated to a train id.	The id of the protection area of a train.

Concept	Step	Description	Comment
Locations of trains	RSS0	Area associated to a train id.	Locations occupied by known trains. Some known trains may not have locations if they are not yet/anymore localised in the AoC.
Speed of trains	RSS0	Natural number associated to a train id.	Speed of known trains
Available areas	RSS0	Area	Locations that can be allocated to trains.
Forbidden areas	RSS0	Area	Locations where the trains cannot enter or move.
Speed limits on locations	RSS0	Natural numbers associated to locations	Current maximum allowed speed on locations.
Position of switches	RSS1	Switch position associated to a switch id.	Current position of the switches of the AoC. A switch can be in Left or Right position, or not positioned.
Requested areas	RSS1	Area	Areas requested to be locked.
Locked oriented areas	RSS1	Set of oriented locations.	Areas where trains can move without risk of derailment.
Protection areas	RSS2	Area associated to a protection id.	A protection does not have a particular shape unless it is the protection area of a train, in which case it is a path.
Status of protections	RSS2	Protection status associated to a protection id.	Status of a protection: Nominal, Reversing, Shunting, Sweepable or Unsweepable.
Date of protections	RSS2	Natural number associated to a protection id.	The date of the last update of the protection.
Rear end of protections	RSS3	Oriented location associated to protection id.	Rear end of the protection area associated to a train.
Front end of protections	RSS3	Oriented location associated to protection id.	Front end of the protection area associated to a train.
Length of trains	RSS3	Natural number associated to a train id.	
Integrity of trains	RSS3	Boolean associated to train id.	
MA of trains	RSS3	Oriented location associated to a train id.	Movement authority of localised (trains with locations) trains.
Min safe rear end	RSS3	Oriented location associated to a train id.	Location of the rear end of the area occupied by the train considering a location error.

Concept	Step	Description	Comment
Max safe front end	RSS3	Oriented location associated to a train id.	Location of the front end of the area occupied by the train considering a location error.
Confirmed rear end	RSS3	Oriented locations associated to train id.	Last rear end of the area occupied by a train with confirmed integrity.
Min safe front end	RSS3	Oriented locations associated to a train id.	Current location of the front end of the area occupied by the train considering a location error.
Active EoA exclusion areas	RSS3	Area	Current locations forbidden for MAs to end.
Date of sent movement authorities	RSS3	Natural number associated to a train id.	Dates of the last sent MAs to onboards.
Date of received position reports	RSS3	Natural number associated to a train id.	Dates of the last position received reports from onboards.

Table 4 Concepts of the dynamic data of the B Model of the Moving Block

6.3.2.3 Properties

The B Model of the Moving Block defines the following properties. These are the properties that the initial state of the system must satisfy and that all the actions of the system must preserve.

Every known train moves in, and is protected by, a train protection area

P-1 Every train has an associated train protection area.

Trains moving in distinct train protection areas avoid front-to-front, front-to-rear and rear-to-rear collisions

P-2 The area occupied by a train is included in the protection area of the train.

P-3 Two distinct train protection areas are disjoint.

P-4 The train protection areas are included in locked areas.

Areas that may be allocated to trains do not conflict with already allocated areas

P-5 Available areas and train protection areas are disjoint.

P-6 Available areas and forbidden areas are disjoint.

P-7 Train protection areas and forbidden areas are disjoint.

Trains moving in train protection areas do not derail and avoid flank collisions

P-8 The opposite oriented areas of the locked oriented areas are not locked.

P-9 Incompatible locations are not locked simultaneously.

P-10 Every train protection area is a path, i.e. a continuous oriented section of the AoC according to the current position of switches of the AoC.

Consistency properties

P-11 Train protection areas are the protection areas associated to trains.

P-12 The rear end of a protection is the first location of the path underlying the protection.

P-13 The front end of a protection is the last location of the path underlying the protection.

P-14 Active shunting areas and train protection areas are disjoint.

P-15 Available areas are all areas which are not protection areas, not forbidden and not active shunting areas.

Compliance of speed of trains with speed limits

P-16 Every localised train has an associated speed.

P-17 The speed of localised trains is smaller than the smallest of the speed limits on the locations where they move.

P-18 The speed of inactive localised trains is 0.

Compliance with FMB requirements on speed limitations, notably in sweepable or unsweepable protections and particular train protection areas (REQ-MA-3).

P-19 The current speed limit on locations is smaller than the absolute speed limit on locations.

P-20 The current speed limit in a sweepable or unsweepable protection is On sight speed.

P-21 The current speed limit in a train protection area associated to several trains is On sight speed.

Compliance with FMB requirements on EoA Exclusion areas and Radio holes (REQ-EoAExclusionArea-4, REQ-RadioHole-2).

P-22 Radio holes are EoA exclusion areas.

Consistency of the relevant locations of trains, MAs, and train protection areas

P-23 Relevant locations of trains, MAs and train protection areas must be ordered according to Figure 1.

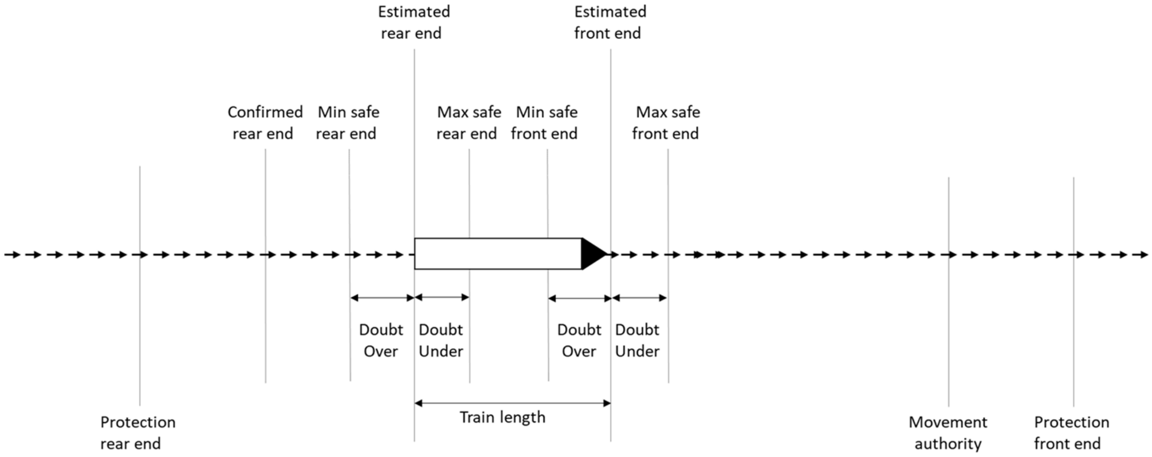

Figure 1: Correct order of train, MA, and train protection end locations.

6.3.2.4 Actions

The B Model defines different sorts of actions.

Actions to manage trains data

- Log in/out, activate/deactivate trains
- Create/update/remove locations of trains

Actions to manage areas

- Lock/unlock area/route/switch
- Make area available/unavailable
- Make area more/less restrictive
- Activate/deactivate shunting/EoA exclusion area

Actions to manage protections

- Create/extend/reduce/join/split/remove/change status

6.3.3 Traceability with Safety Analysis Properties

The following Table 5 presents the traceability of the properties identified by the safety analysis of Section 5 (blue background cells) with the properties formalised in the B Model of the Moving Block (white background cells).

It must be noticed that the concept of "forbidden area" in the safety analysis and "forbidden area" in the B Model differ. In the sense of the safety analysis a forbidden area is an area where there should be no train, while in the sense of the B Model it might be a train in a forbidden area, but it cannot move. However, in both senses trains can't enter forbidden areas. Forbidden areas, in the sense of the safety analysis, are managed with mix of not locked areas and forbidden areas, in the sense of the B Model.

T0a: Trackside shall correctly update (creating, removing, extending, reducing) the areas where trains or sets of railway vehicles may potentially be.
Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train.
T0b: Any authorisations sent directly or indirectly by Trackside to a train shall be within the maintained area where this train may potentially be.
Preservation of property: P-1: Every train has an associated train protection area. P-23: Relevant locations of trains, MAs and train protection areas must be ordered according to Figure 1.
T0c: Trackside shall correctly update (creating, removing, extending, reducing) the areas where obstacles may potentially be.
Preservation of properties: P-1: Every train has an associated train protection area.

P-2: The area occupied by a train is included in the protection area of the train. P-3: Two distinct train protection areas are disjoint. P-4: The train protection areas are included in locked areas. P-5: Available areas and train protection areas are disjoint. P-6: Available areas and forbidden areas are disjoint. P-7: Train protection areas and forbidden areas are disjoint. P-14: Active shunting areas and train protection areas are disjoint.
T1: L3 trackside shall never authorize a train movement over a moveable piece of track if it has not been reported traversable to L3 trackside.
Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train. P-4: The train protection areas are included in locked areas. P-23: Relevant locations of trains, MAs and train protection areas must be ordered according to Figure 1.
T2: L3 trackside shall never allow change of a moveable piece of track to a non-traversable state if it authorized a train movement over that piece of track and the train has not yet reported beyond that piece of track.
Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train. P-4: The train protection areas are included in locked areas. P-23: Relevant locations of trains, MAs and train protection areas must be ordered according to Figure 1.
T3: L3 trackside shall never compute speed limits to be sent to a train wrongly too high.
Preservation of properties: P-16: Every localised train has an associated speed. P-17: The speed of localised trains is smaller than the smallest of the speed limits on the locations where they move. P-18: The speed of inactive localised trains is 0. P-19: The current speed limit on locations is smaller than the absolute speed limit on locations. P-20: The current speed limit in a sweepable or unsweepable protection is On sight speed. P-21: The current speed limit in a train protection area associated to several trains is On sight speed.
T4: L3 trackside shall never authorize a train movement over a piece of track that is known to be occupied or to be used by a vehicle unless in OS mode, SR mode or for joining.
Preservation of properties: P-1: Every train has an associated train protection area.

P-2: The area occupied by a train is included in the protection area of the train. P-16: Every localised train has an associated speed. P-20: The current speed limit in a sweepable or unsweepable protection is On sight speed. P-21: The current speed limit in a train protection area associated to several trains is On sight speed.
T5: L3 trackside shall never authorize a vehicle movement into a forbidden area.
Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train. P-7: Train protection areas and forbidden areas are disjoint.
T6: L3 trackside shall never authorize a train movement without having established forbidden areas at (a) each track branching from the authorized track and (b) each track that has an overlapping clearance gauge with the authorized track, such that the forbidden areas prevent vehicles from flank and touching collisions with the authorized train when not entered, even when the train exceeds the structure gauge.
Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train. P-4: The train protection areas are included in locked areas. P-9: Incompatible locations are not locked simultaneously.
T7: L3 trackside shall never remove a forbidden area if it authorized a train movement that is protected by that forbidden area at some branch or track with overlapping clearance gauge and the train has not yet reported beyond the branch or track with overlapping clearance gauge.
Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train. P-3: Two distinct train protection areas are disjoint. P-4: The train protection areas are included in locked areas. P-9: Incompatible locations are not locked simultaneously.
T8: L3 trackside shall never authorize a too far vehicle movement towards a forbidden area for a vehicle that exceeds the clearance gauge.
Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train. P-4: The train protection areas are included in locked areas. P-9: Incompatible are not locked simultaneously.
T9: L3 trackside shall never wrongly remove or change its information about a vehicle and its position.

Preservation of properties: P-1: Every train has an associated train protection area. P-2: The area occupied by a train is included in the protection area of the train. P-16: Every localised train has an associated speed. P-17: The speed of localised trains is smaller than the smallest of the speed limits on the locations where they move. P-18: The speed of inactive localised trains is 0. P-23: Relevant locations of trains, MAs and train protection areas must be ordered according to Figure 1.
T10: L3 trackside shall never authorize a train movement over an LX which has not reported protected status to it and does not report its status to a LEU without having included sufficient restrictions to pass the LX safely.
Level crossings are not considered in the B Model.
T11: L3 trackside shall never command/agree to opening of a level crossing over which it authorized a train movement2 and the train has not yet passed the level crossing.
Level crossings are not considered in the B Model.
T12: L3 trackside shall never compute track condition “sound horn” to be sent to a train wrongly or miss to include them in an MA for approaching/passing a passive level crossing, unless only driver information via trackside signs is foreseen.
Alarm is not considered in the B Model of the Moving Block.
T13: L3 trackside shall apply a safety reaction immediately if an obstacle on a piece of track where it authorized a train movement becomes known.
Alarm is not considered in the B Model of the Moving Block.
T14: L3 trackside shall never authorize a train movement without having included sufficient restrictions to pass any obstacle on the authorized piece of track that has been reported to L3 trackside and has not yet been reported no longer present.
Preservation of properties: P-20: The current speed limit in a sweepable or unsweepable protection is On sight speed. P-21: The current speed limit in a train protection area associated to several trains is On sight speed.

Table 5 Traceability of Safety Analysis Properties

6.3.4 Remarks

As explained above, the verification of the B Model of the Moving Block followed the refinement steps. The verification, i.e., inductive proof with Atelier-B[12] of the first 3 steps, RSS0, RSS1 and RSS2 last more or less 8 working days and did not pose any particular technical problem

[12] Atelier-B is a toolset supporting the creation and formal verification of B models. It is commercialised by Clearsy Company.

because the models, as wanted, are quite simple. It nevertheless pointed out modelling errors and inconsistencies in the data and actions of every step and inconsistencies between the data and actions of one step and the data and actions of the next step. The verification of RSS3 was not completed because the concepts and properties of this step were not fully finalised, notably the interactions between the trackside system and the on-board system.

Summarizing, the verifications made were useful for superficially correcting the B Model, but not for validating its relevance and adequacy. Traceability with the safety analysis of Section 5 contributes to that validation, but it is insufficient. A thorough analysis of the B Model by experts in the Moving Block specification would have been necessary. More generally, to save effort and time, the relevance and adequacy of a formal model should be validated, either by experts review or, if possible, by model animation, simulation, or testing whether the model is executable, before proceeding to full inductive proof. This is particularly true in the case of stepwise refinement, because proving a lower step may lead to modify upper steps.

7 Summary and Conclusions

The aim of this document has been to describe safety-related requirements for L3 Trackside with full moving block, including safety hazards and safety requirements that, if fulfilled, ensure hazards are mitigated. This document has also described results in V&V activities. This chapter provides a summary of work done, and conclusions.

7.1 Summary

One of the objectives of WP10 has been to illustrate how FMs contribute to the definition of rigorous and consistent safety requirements for the L3 Trackside system, as defined in the moving block specification [2].

Ideally, safety requirements mitigate the hazards identified by a systematic safety hazard analysis for the system of systems, apportioning the hazards that apply to each subsystem (including L3 Trackside). Traceability from each hazard to safety requirements would enable validation of completeness of safety requirements (based on completeness of hazards). This document has described how this approach can be applied using fault trees (see Section 5).

The moving block specification does not systematically distinguish which requirements are to be considered safety requirements. Furthermore, as identified in the requirement analysis of the moving block specification, several issues complicate to determine the safety requirements for L3 trackside (see Section 6.1). One issue is that the moving block specification is a partial requirement specification in many respects (necessitating to make many assumptions for reasoning about safety). Another issue is the Track Status Area (TSA) concept in the moving block specification: to model this central concept[13], and to define safety requirements in terms of it, would not be straight-forward, and add unnecessary complexity both to properties and provability. At least this was the view in the two FMs application approaches applied (see Section 6). For this reason, different, but more FMs-friendly concepts were used as basis for safety properties. The purpose was to formulate as simple safety properties as possible and to promote provability, while capturing “the spirit” of the moving block specification. The two FMs application approaches describe how requirements in the moving block specification can be represented to (a) investigate their consistency and (b) prove that desirable system properties follow (under the additional assumptions made).

The FMs application did not pose challenge in itself: ontology concepts and associated properties could be defined and used as basis for V&V of consistency and that desired properties follow.

V&V results identified issues in the moving block specification. That FMs can help to expose gaps in requirements, and to increase their quality, matches experience from FMs application in general as well as from TD2.7’s previous work [12].

[13] And more generally the Track State concept, which combines the TSA and the Reserved Area concepts.

7.2 Conclusions

The moving block specification defines a new system (L3 Trackside), based on Full Moving Block. For any such new system definition ("system inception"), it is an objective to determine system requirements that are clear how they shall be implemented and verified, and how they meet user needs. For critical railway signalling systems, an objective is also to "design in" a whole class of desired properties (e.g., related to interoperability, safety, reliability, and standards compliance) to permeate system behaviour, because it is hard (impossible) to add this as an afterthought. For complex systems, it poses a challenge to create a clear and simple definition of principles and requirements that will ensure all these properties.

To use FMs for system inception is very relevant, since FMs provide the means to define clear and simple principles and requirements, to prove them consistent, and to prove that desired system properties follow (e.g., related to safety). This case study used requirements in the moving block specification as input for FMs application, as illustrated in Figure 10; while user needs and safety analyses should be inputs to the process, they were not available for this case study (a complication factor).

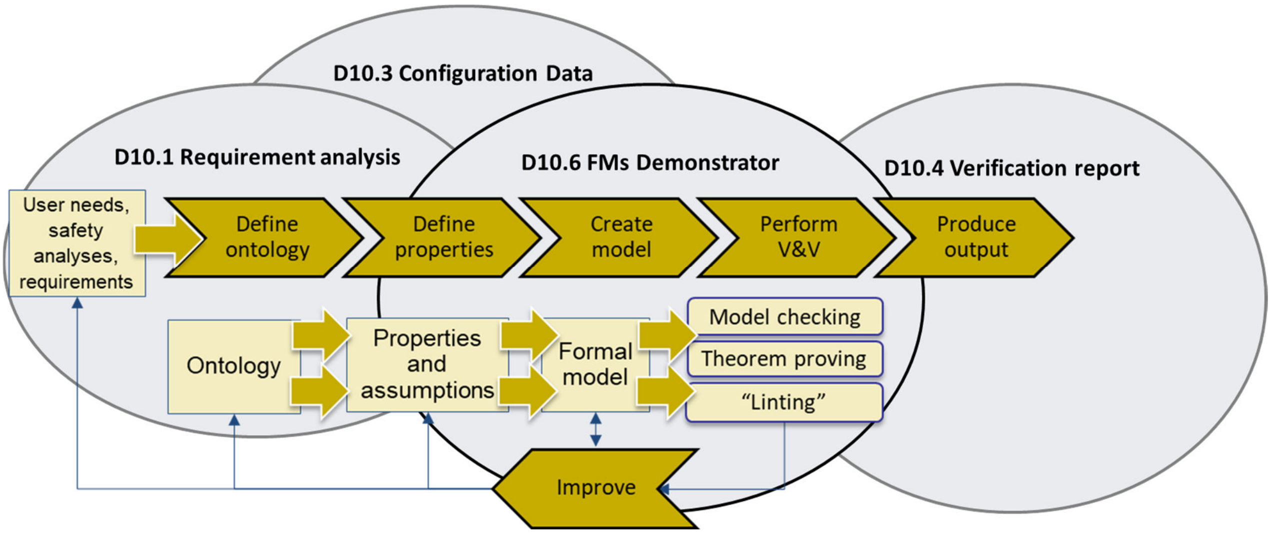

Figure 10 Scope overview (a copy of Figure 1)

The case study work highlights what FMs application for system inception requires:

- Understanding of the user requirements to be met.
- Appropriate ontology concepts, as basis for properties such as safety requirements.
- Knowing which properties are safety requirements.
- Availability to domain experts, for questions and answers, and advice.
- Validation of the models created in the FMs application.

This case study highlights that to make FMs application for system inception efficient and effective ("FMs-friendly"), the following are useful activities to plan for:

- Perform a system requirement analysis to determine the static and dynamic ontology concepts necessary to define the essential system properties and behaviour.

- Determine the ability to customise the system for different applications (including static configuration data such as the track layout, but also different system types such as moving block, fixed virtual block and other variations that may be relevant).
- Perform a systematic hazard analysis and derive the hazards relevant to the system studied.
- Define safety requirements that prevent the hazards for the system studied and validate, using FMs-based analyses, that they mitigate all hazards.
- If FMs are not used as an integral part of requirement definition when system inception starts, establish close collaboration with FMs practitioners for this task.
- Validate output from FMs application by domain experts, e.g., model animation of the formal model. Ideally, domain experts can validate the formal model created, e.g., with respect to meeting user needs, and to identify issues. If a formal model is executable, this can make it easier for domain experts to perform such validation (using simulation and test).

8 References

[1] X2Rail-5 Grant Agreement 101014520.

[2] X2Rail-5 Deliverable D4.1 Moving Block Specifications, Dec 21, 2022 (received Jan 9, 2023).

[3] X2Rail-3 Deliverable D4.2 Moving Block Specifications, Dec 18, 2020.

[4] X2Rail-5 Deliverable D10.1 Requirement Analysis and Scope, 2023.

[5] X2Rail-5 Deliverable D10.3 Configuration Data, 2022.

[6] X2Rail-5 Deliverable D10.6 Formal Methods Demonstrator, 2023.

[7] X2Rail-5 Deliverable D10.9 Formal Methods Guidebook, 2023.

[8] SUBSET-026: ERTMS/ETCS System Requirements Specification, Issue 3.6.0, 13/05/2016.

[9] IEC 61025:2006 Fault tree analysis (FTA)

[10] Ladkin P. B. – *Causal System Analysis* – 2005, Springer, ISBN 9781852336530

[11] Günther H., Herr A., Schütte, J., Geisler M., Püttner R. – *Concept and Contexts of the ROSA Model* – 2008, WP1 Deliverable of ROSA project. Included in the final ROSA project report, 2009, doi: 10.2314/GBV:634017071

[12] Holistic Study of Formal Methods and Standardization in Specification, Development, Verification and Validation of Railway Signalling System Software. Dissemination paper by TD2.7 based on results in X2Rail-2 project, World Congress on Railway Research (WCRR), 2022.

Appendix A: Ownership of results

The following Table 6 lists the ownership of results for this deliverable.

Ownership of results			
Company	Percentage	Short Description of share/ of delivered input	Concrete Result (where applicable)
Trafikverket			
Alstom			
DLR			

Table 6: Ownership of results

This deliverable is jointly owned by the organisations listed above. The last three columns in the table are intentionally left empty.