Horizon 2020
European Union Funding
for Research & Innovation

X2Rail-1

Project Title:	**Start-up activities for Advanced Signalling and Automation Systems**
Starting date:	01/09/2016
Duration in months:	36
Call (part) identifier:	H2020-S2RJU-CFM-2015-01-1
Grant agreement no:	730640

Deliverable D5.3

Moving Block Preliminary Safety Analysis

Due date of deliverable	Month 32
Actual submission date	16/07/2019
Organisation name of lead contractor for this deliverable	SIE
Dissemination level	PU
Revision	3.0

Authors

Author(s)	Siemens (SIE)
Contributor(s)	Alstom (ALS)
	AZD (AZD)
	Bombardier (BTSE)
	CAF (CAF)
	Deutsche Bahn (DB)
	DLR (DLR)
	ERTMS Users Group (EUG)
	Hitachi Rail STS (STS)
	Mermec (MERMEC)
	Network Rail (NR)
	Thales (TTS)

Change History

Version.Revision	Date	Release Status	Change Reference
1.0	17/05/2019	Edition	1st Edition
2.0	16/07/2019	Edition	First official version
3.0	07/11/2019	Edition	After JU Expert Review

Executive summary

This Preliminary Safety Analysis is one of a group of documents produced by WP5 Moving Block in the Shift2Rail project X2Rail-1, in accordance with the X2Rail-1 Grant Agreement:

- **D5.1 Moving Block System Specification** which defines the behaviour of the ETCS Level 3 Moving Block system.
- **D5.2 Moving Block Operational and Engineering Rules** which defines additional Operational and Engineering Rules required for an ETCS Level 3 Moving Block system.
- **D5.3 Moving Block Preliminary Safety Analysis** (this document) which describes hazards identified as a result of operating an ETCS Level 3 Moving Block system, and also describes potential mitigations for those hazards.
- **D5.4 Moving Block Application Analysis** which describes the application of ETCS Level 3 Moving Block systems to different railway types.

These documents are Deliverables from X2Rail-1, with further work intended in both X2Rail-3 and X2Rail-5.

The group of documents assume ETCS Level 2 as a baseline. The work has aimed to minimise the changes required beyond ETCS Level 2. Anything which is the same as ETCS Level 2 is not described, except where some description is required to provide context.

In this deliverable the principal ETCS Level 3 Moving Block hazards have been identified, the causes considered, potential mitigations identified and linkage to the requirements and rules. [EN50126] have been used as reference for this analysis.

The results of this analysis have been used as an input for deliverables [D5.1] and [D5.2].There are still some requirements/rules to be added. A list of potential D5.1/D5.2 updates to be further addressed in X2RAIL-3 has been added into section 6.

As originally planned the significance of the hazards has not been formally assessed nor the effectiveness of any mitigations. The work is not finished in X2Rail-1 and further work is proposed to be carried out within the follow-on project X2Rail-3, and later X2Rail-5. The topics for further work in X2Rail-3 are listed in section 6.

Table of contents

List of Figures

1 Objective

The key objectives of this document are:

- Identify the Hazards for a Moving Block Signalling System based on ETCS Baseline 3, Release 2 [BL3 R2] and Change Request 940 [CR940], which are applicable across different railway types.
- Propose mitigations for those hazards, and link the mitigations with Requirements [D5.1] and/or Operational and Engineering Rules [D5.2]. Additions to D5.1 and D5.2 have been proposed to address hazards where these do not exist.

This Preliminary Safety Analysis is based on a qualitative methodology at this stage. The objectives do not include a quantitative analysis of the hazards or an assessment of the effectiveness of the mitigations.

2 Background

2.1 Shift2Rail Background

This document has been produced within Shift2Rail IP2 "Advanced Traffic Management and Control Systems". The work is part of the work on Technical Demonstrator TD2.3 Moving Block.

The document has been produced within the X2Rail-1 Work Package 5: Moving Block.

2.2 NGTC Background

The work in X2Rail-1 WP5 Moving Block has taken notice of the results of the "Next Generation of Train Control systems" (NGTC) project. The approach using analysis of scenarios follows from the work in the NGTC project [NGTCD51]. The principal difference is that the work in X2Rail-1 WP5 Moving Block has explicitly addressed the implementation of Moving Block using ETCS Level 3.

2.3 ETCS Reference

The work in X2Rail-1 WP5 Moving Block addresses the implementation of Moving Block signalling using ETCS Level 3. The term "ETCS Level 3 Moving Block" is used to mean a signalling system where Moving Block is implemented using ETCS Level 3.

The work in X2Rail-1 WP5 Moving Block has taken notice of the following objective from the introduction to the Description of Work in Annex 1 of the X2Rail-1 Grant Agreement:

> *To ensure the backward compatibility of ERTMS/ETCS technologies, notwithstanding the required functional enrichment of the future signalling and control systems.*

This document has used the ETCS Baseline 3 Release 2 [BL3 R2] as a starting point. In addition, the proposed solution to Change Request 940 [CR940] has been considered when preparing this document. Other CRs that are considered relevant are mentioned explicitly.

In accordance with the above stated X2Rail-1 objective, the impact on [BL3 R2] has been kept to a minimum.

2.4 Architecture Assumptions

In accordance with minimising the impact on ETCS Specifications [BL3 R2], the work in X2Rail-1 WP5 has assumed that the system architecture for ETCS remains unchanged. This architecture is summarised in

Figure 1:

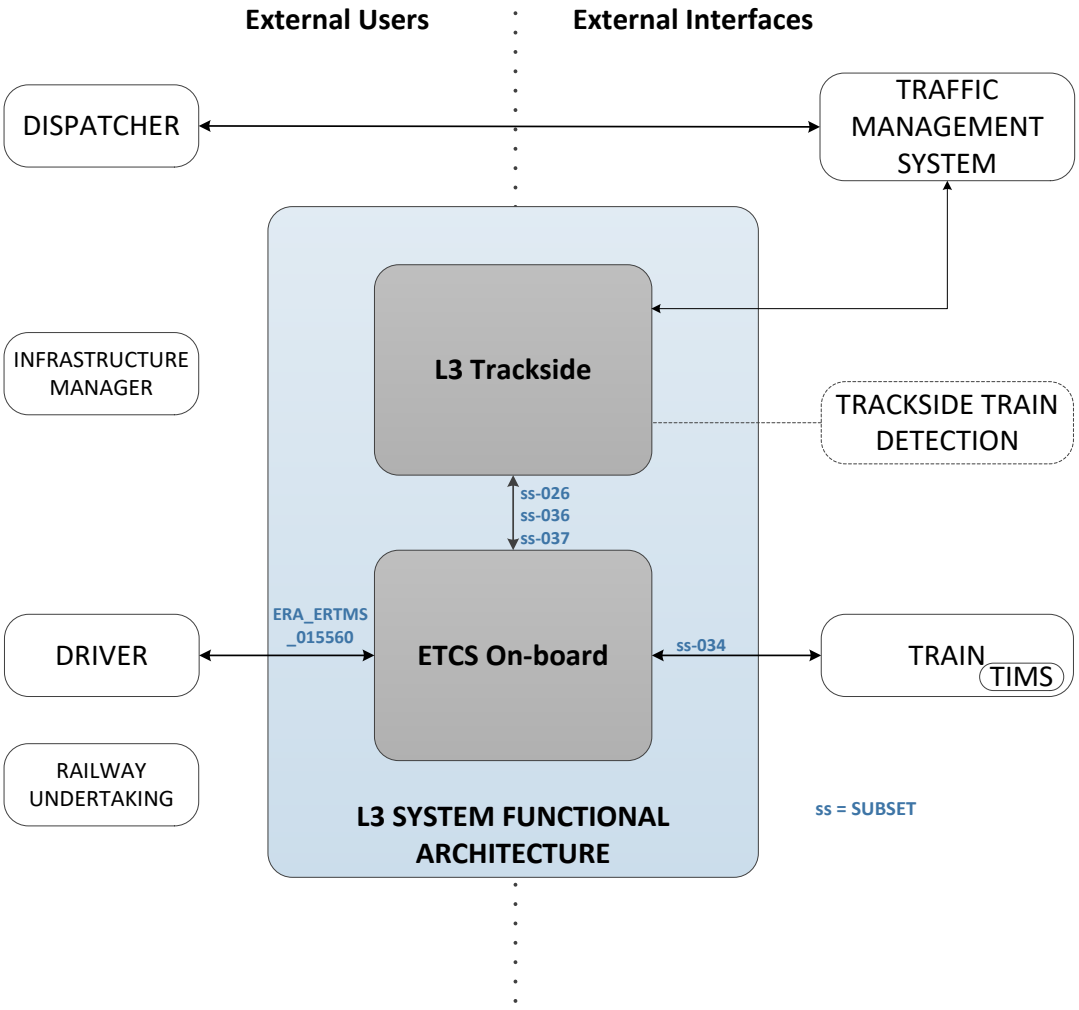


Figure 1 - Generic ETCS Level 3 Moving Block System Functional Architecture

From

Figure 1 the key external actors in this system are:

- Dispatcher – the operator of the Traffic Management System.
- Infrastructure Manager – the body responsible for the operation of the Railway and maintenance of infrastructure.
- Driver – the operator of the train.
- Railway Undertaking – Operation and maintenance of passenger/freight trains.

In this document, the L3 Trackside includes functionality traditionally considered part of the interlocking as well as the RBC functionality. The System Architecture in the ETCS Specifications [BL3

R2] does not consider the interlocking as part of the ETCS system. In an ETCS Level 2 system, although there is no defined interface between RBC and Interlocking, the separation of functions is clearer. In an ETCS Level 3 Moving Block system, Track Status is derived primarily from Train Position Reports, rather than Trackside Train Detection, and therefore the Track Status function is required to be in scope. This is shown in Figure 2 below. Throughout this document, the term "L3 Trackside" is used, which encompasses the Track Status Management function.

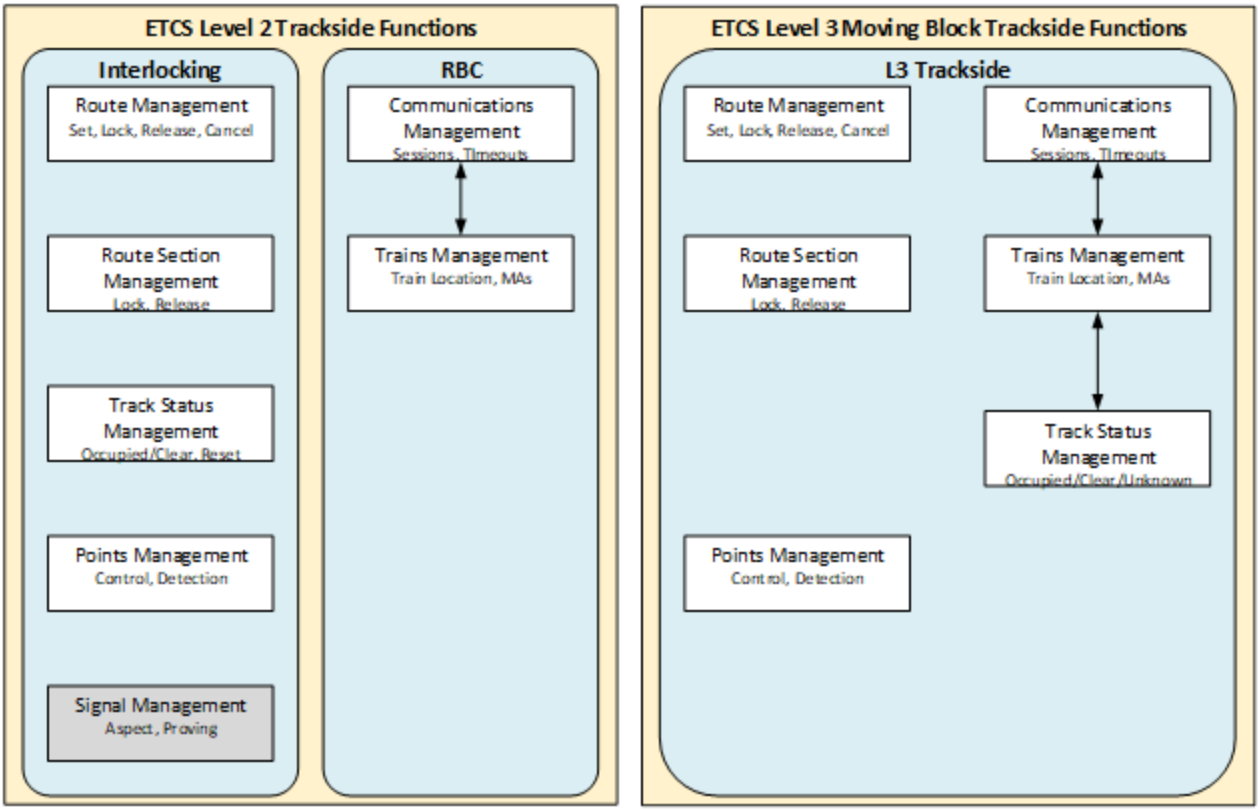


Figure 2 – Comparison of Functional Architectures for ETCS Level 2 and ETCS Level 3 Moving Block

The Traffic Management System shown in Figure 1 can be implemented in different ways, up to an automated Traffic Management System (TMS).

Note that this architecture is aligned with that developed by X2Rail-1 WP2: Technical coordination and System Coherence [D2.1].

3 Scope

3.1 Document scope

This document contains the description of all the L3 related hazards that have been identified as a result of preliminary safety analysis for an ETCS Level 3 Moving Block Signalling System. In addition, potential mitigations have been proposed to mitigate them.

There are companion documents for other aspects of ETCS Level 3 Moving Block Signalling Systems. The following table summarises the set of documents:

X2Rail-1 Deliverable	Title	Notes
D5.1	Moving Block System Specification	Defines System Requirements and Assumptions for an ETCS Level 3 Moving Block Signalling System, where those requirements are beyond what is required for an ETCS Level 2 system.
D5.2	Moving Block Operational and Engineering Rules	Defines Operational and Engineering Rules for an ETCS Level 3 Moving Block Signalling System, where those rules are beyond what is required for an ETCS Level 2 system.
D5.3	Moving Block Preliminary Safety Analysis (this document)	Contains hazard analysis of an ETCS Level 3 Moving Block Signalling System.
D5.4	Moving Block Application Report	Analysis of applying the ETCS Level 3 Moving Block system to different railway types (Urban/Suburban, High Speed, Overlay and Low Traffic/Freight).

3.2 Application Scope

3.2.1 Railway Types

The aim of this document is to identify hazards and propose mitigations that can be applied to different railway types.

Within the Grant Agreement, the following types of railway are explicitly listed for WP5 Moving Block:

- Urban /Suburban Railways
- Overlay Systems
- High Speed Lines
- Low Traffic and Freight Lines

It is the intent that these can all be handled by the same generic ETCS Level 3 Moving Block system. However, there will be differences in the way the L3 Trackside is applied to different types of railway. These differences are identified and analysed in [D5.4].

3.2.2 Grade of Automation

The ETCS architecture shown in

Figure 1 includes a Driver. The work on Preliminary Safety Analysis has assumed that there will be a Driver present. Therefore, this system is specified to be able to support Grades of Automation up to GoA2. It is not intended to cover systems without a driver, GoA3/4.

3.3 System Scope, Assumptions & Constraints

See the equivalent section in [D5.1]

4 Safety plan

4.1 Preliminary Safety Analysis Methodology

As stated in the Grant Agreement the objective of Task 5.5 is to examine the safety of an ETCS Level 3 Moving Block System.

In order to establish the contents of the Deliverables, the Work Package considered a series of scenarios regarding both normal and degraded operation of the L3 Railway. These scenarios were working documents (not deliverables) used as the basis for establishing the relevant L3 Trackside Requirements, Engineering and Operational Rules. Since they describe relevant events and the interaction of requirements and rules, these scenarios were used as the basis of the Preliminary Safety Analysis.

To this objective, hazard identification workshops were held according to [EN50126] in order to identify:

- Hazardous events in every scenario.
- Requirements, Operational/Engineering rules and assumptions to mitigate the hazards.

This corresponds to hazard identification in [CSM], with the system definition as defined in Section 2 above.

As a preparatory activity to be carried out before the workshop, the safety representative of the company responsible for that scenario met the author of the respective scenario description and pre-identified the possible hazards that could occur.

The pre-identified hazards are recorded as a part of the scenario document or in a separate document in order to be analysed during the workshop.

The team involved in the workshop reviewed the scenario description focusing on those open points (hot topics) to be discussed.

All pre-identified hazards were used as a reference during the workshop in order to identify the final hazards and mitigations.

After every workshop planned for the X2Rail-1 WP-5 Moving Block project all identified hazards were included in the Preliminary Safety Analysis.

The Preliminary Safety Analysis was updated after the workshops once the safety assessment was completed.

Figure 3 gives an overview of the process followed.

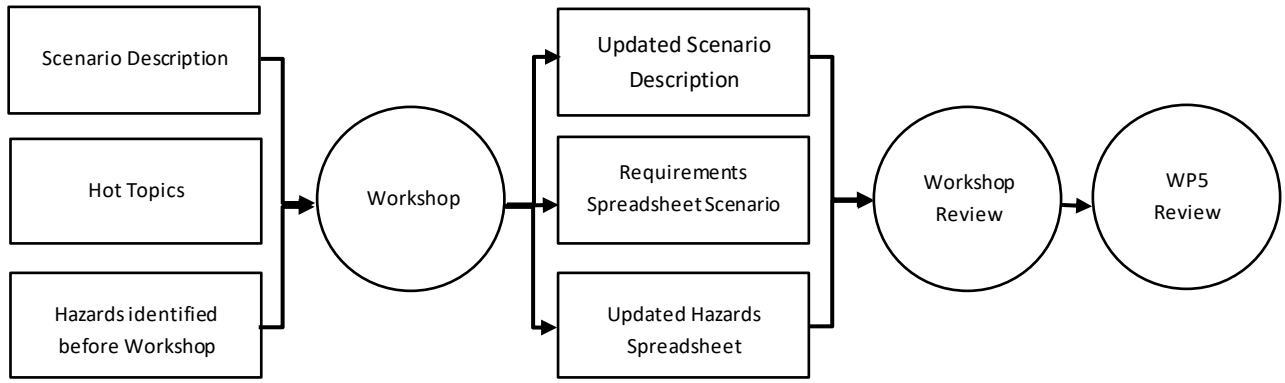


Figure 3: Workshop activity flow

Once all the hazards were identified, potential mitigations have been referenced to every hazard. Those mitigations related with existing requirements and/or rules have been traced as shown in Figure 4 below.

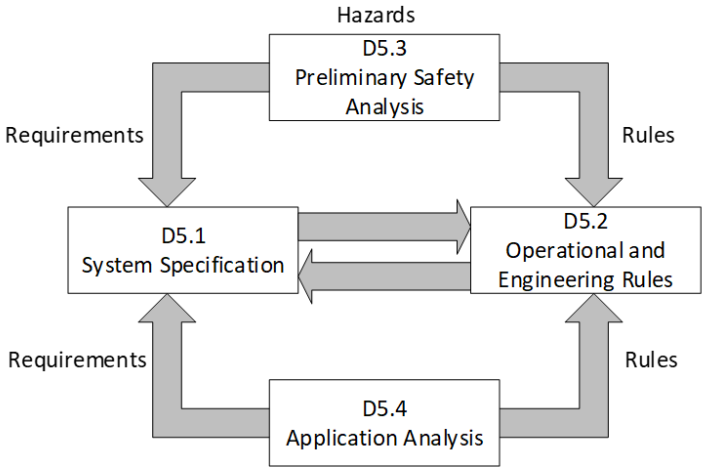


Figure 4 - Traceability between deliverables

D5.4 contains analysis of the Requirements (D5.1) and Rules (D5.2) as applied to different railway types.

Requirements and Rules linked to Proposed Mitigations do not necessarily fully mitigate the hazards.

Finally, the hazards have been classified gathering all different causes that could lead to the same hazard (see section 5).

4.2 Roles and functions

4.2.1 Task leader

Responsibilities:

- Planning and co-ordination of X2Rail-1 WP5 Moving Block Task 5.5 Safety activities.
- Creation and continuous update of Preliminary Safety Analysis.
- Creation and the maintenance of the Safety plan

4.2.2 Safety representatives

Responsibilities:

- Safety experts.
- Participation, if requested, in WP5 meetings/workshop.
- Identify the hazards that could occur in the steps of the scenarios.
- Propose mitigation measures for the hazards.
- Determine any additional hazard that could occur as a result of implementing a mitigation.

5 Hazards

For every hazard the following sections have been defined:

- **Hazard Headline:** general description of the hazard.
- **Hazard Description:** A potentially dangerous situation that could occur and the relevant scenario.
- **Potential mitigations:** Alternatives to be taken into account in order to reduce the frequency or severity of the hazards.
- **Related rules and requirements:** Reference to specific Requirements (REQ), Operational & Engineering rules (OPE/ENG) and Assumptions (ASM) related to the potential mitigations.

Where potential mitigations have been already covered by existing requirements/rules cross reference have been provided. Some further mitigations not yet present in [D5.1], [D5.2]are listed in section 6 Conclusions.

In the next phase requirements/rules identified as mitigation measures will be assessed by the quantitative analyses (Risk evaluation phase according to [CSM]). Severity and frequency of every hazard will be considered in order to assess the impact of mitigations on the risks. In case the residual risks after mitigations are not considered as tolerable, additional measures will be required. This may generate changes to system requirements [D5.1] and operational and engineering rules [D5.2].

The hazards have been classified according to the following table:

Section	Hazard	Summary	Causes
5.1	Track status erroneously cleared	This section describes causes which result in an area of track being considered clear by the L3 Trackside, when there is in fact an obstruction present	• Dispatcher interaction in L3 Trackside initialisation • Using invalid/outdated information for L3 Trackside initialisation • Deactivating shunting area • Driver confirms train integrity • Recovery of a failed train
5.2	Error in Train Location	This section describes causes which result in the location of a train as recorded within the L3 Trackside being different from the true location of the train	• Confidence interval reduced at End of Mission • Lack of linking information

Section	Hazard	Summary	Causes
5.3	Error in Train Length	This section describes causes which result in the Train Length of a train as recorded within the L3 Trackside being different than the true length of the train	• Reported train length shorter than actual • Reported train length longer than actual
5.4	CMD Erroneously Validates Position	This section describes the result of a CMD system erroneously validating the location of a train	• Wrong side failure of CMD
5.5	Undetected Movements	This section describes causes which result in undetected movement of a train	• Rollback after standstill • Movement in NP mode • At entrance to Level 3 area • After End of Mission • Loss of Train Integrity • Propelling train • Shunting train
5.6	TTD erroneously indicates track clear	This section describes the result of a TTD which erroneously indicates a section of track as Clear	• Wrong side failure of TTD
5.7	Points Moved under train	This section describes the result of moving a point after communications failure	• Points Moved After Communications failure

Additionally, one section has been included for hazards already existing in ETCS L2 systems. These are hazards identified by the work on Moving Block for ETCS L3, but which, after examination, were found to be already present in L2. They are included in section 5.8, as there are some specific ETCS L3 mitigations proposed.

5.1 Track status erroneously cleared

5.1.1 Dispatcher interaction in L3 Trackside initialisation

H-Clearing-001

Hazard headline:

Track status erroneously cleared during L3 Trackside initialisation by dispatcher leading to collision

Hazard description:

At L3 Trackside initialisation, in addition to communicating trains there could be non-communicating trains (e.g. in modes SH, NP, etc.) or other obstructions such as vehicles not equipped with ETCS, work areas, etc.

After initialisation (either in planned circumstances or as a consequence of a system fault) the Level 3 Trackside has to ascertain the location of all vehicles and obstructions in the Area.

If the L3 Trackside allows for a responsible person to declare tracks Clear, then it is critical that the area is only determined Clear when it is truly clear to avoid a Movement Authority into an area which is occupied, that could lead to a collision.

Potential mitigations:

At initialisation, L3 Trackside considers the Track Status of the entire L3 Area as Unknown and a process will be required to declare areas as Clear. These could include:

- Operational Rules to manage track occupancy – the rules are around identifying the occupied parts of the L3 area and whether the responsible person can declare the other Unknown areas as Clear in L3 Trackside.
- Using sweeping trains.
- Providing TTD.
- Storing information on track occupancy and movement authorities and using this information at initialisation to ensure all previously connected trains are accounted for. This is only applicable where the L3 Trackside fails or is restarted but was previously operational. The validity of stored information will reduce over time since uncertainty increases and each application will need to establish appropriate rules. (See section 5.1.2).

Related rules and requirements:

REQ-TrackInit-1, REQ-TrackInit-3, REQ-TrackInit-5, REQ-TrainLoc-9

OPE-TrackInit-2, OPE-TrackInit-3, OPE-TrackInit-5, OPE-OS-3

ENG-TrackInit-1

5.1.2 Using invalid/outdated information for L3 Trackside initialisation

H-Clearing-002

Hazard headline:

Track status erroneously cleared during L3 Trackside initialisation by system leading to collision

Hazard description:

At L3 Trackside initialisation, in addition to communicating trains there could be non-communicating trains (e.g. in modes SH, NP, etc.) or other obstructions such as vehicles not equipped with ETCS, work areas, etc.

After initialisation (either in planned circumstances or as a consequence of a system fault) the Level 3 Trackside has to ascertain the location of all vehicles in the Area.

If the L3 Trackside utilises stored information to set areas of track Clear, then it is critical that this information is correct to avoid a Movement Authority into an Occupied area, that would lead to a collision.

The information may no longer be correct and erroneously consider an occupied area as Clear.

Potential mitigations:

Operational and Engineering Rules shall be in place to safely establish whether stored information is still valid according to time-based criteria.

Related rules and requirements:

REQ-TrainLoc-9

OPE-TrackInit-1, OPE-TrackInit-5

ENG-TrackInit-1

5.1.3 Deactivating shunting area

H-Clearing-003

Hazard headline:

Track status erroneously cleared after deactivation of a shunting area leading to collision

Hazard description:

The L3 Trackside considers the track status in an active shunting area as Unknown, except for the location of communicating trains. When deactivating a shunting area, responsible staff may have the possibility to clear any remaining Unknown areas. Doing this, a part of the track that is occupied can be set to Clear leading to collision.

Potential mitigations:

Mitigations will be required to declare areas as Clear after deactivation of a shunting area. These could include:

- Operational Rules to manage track occupancy – the rules are around whether the responsible person can declare areas as Clear in the L3 Trackside system.
- Using sweeping trains.
- Providing TTD for temporary shunting areas.

Related rules and requirements:

REQ-TrackStatus-3, REQ-TrackStatus-8, REQ-TTD-3

OPE-Generic-1, OPE-SH-2, OPE-OS-2, OPE-OS-3.

5.1.4 Driver confirms train integrity

H-Clearing-004

Hazard headline:

Track status erroneously cleared by driver confirming Train Integrity leading to collision

Hazard description:

In case a train driver confirms Train Integrity after a part of the train has been lost, the lost part will be not detected (unless there is TTD), which could lead to collision with other trains approaching the area where the lost part is. This situation could occur when operating trains without TIMS or for a train with a failed TIMS.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Operational procedure to prevent driver errors about integrity confirmation.
- Infrastructure Managers can engineer the L3 Trackside to never accept Confirmation of Integrity by the Driver.
- Always use an external device to confirm integrity, avoiding human interaction.

Related rules and requirements:

REQ-LossTI-9

OPE-Generic-2

ENG-LossTI-3

ASM-Integrity-1

5.1.5 Recovery of a failed train

H-Clearing-005

Hazard headline:

Track status erroneously cleared by TIMS device not being able to detect loss of integrity after joining trains leading to collision

Hazard description:

When a train is coupled with another train they should be considered as one train with a common train integrity. However, this depends on if the TIMS devices in the coupled trains are compatible or if the TIMS in the rear part is operational.

In case the driver updates the train length to that of the coupled trains without knowing the status of the TIMS device in the rear part, a loss of integrity in the rear part will not be detected and reported by the TIMS in the front part of the train.

This could happen in a rescue situation when there is need to pull out a failed train and lead to a collision if the track is cleared based on information which is not valid for the complete train and a part of it is lost without being detected.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Operational rules are necessary to manage the situation when the TIMS devices do not match and the train integrity cannot be confirmed for the joined train.
- Isolate the TIMS device if it cannot cover the complete train after joining.
- The dispatcher could set an Unknown area to protect rescue operations.

Related rules and requirements:

OPE-REC-1, OPE-LossTI-2, OPE-Generic-6

5.2 Error in Train Location

5.2.1 Confidence interval reduced at End of Mission

H-TrainLoc-001

Hazard headline:

Error in Train Location from reduced confidence interval at End of Mission leads to collision

Hazard description:

The L3 Trackside needs to determine the area that could be occupied by a train performing End of Mission (EoM) in order to protect it. To that aim, the L3 Trackside is expected to use the location information received from the train with the addition of a Safety Margin.

However, as part of the ERA CCM Process an ambiguity in the specifications has identified which makes it is unclear how the ETCS On-board calculates the confidence interval reported at EoM. This is because linking information, including balise location accuracy used in the confidence interval, is deleted when changing to SB mode.

If the location accuracy of the LRBG has a larger value than the National Value (Q_NVLOCACC) and the ETCS On-board uses the National Value in the EoM Position Report, this could lead to a collision if the Unknown area for protecting the train is unduly shortened, not covering the whole length of the train.

Potential mitigations:

- All authorised ETCS On-board shall retain the last train location, which is safe and based on the location accuracy of the LRBG as previously received in linking information.
- L3 Trackside ignores the confidence interval in the EoM Position Report.
- Balises in the L3 Area are engineered with a location accuracy equal or better than the National Value.

Related rules and requirements:

REQ-EoM-3, REQ-EoM-4, REQ-EoM-6, REQ-TrainLoc-3

5.2.2 Lack of linking information

H-TrainLoc-002

Hazard headline:

Error in Train Location from lack of linking information leading to collision

Hazard description:

When relocation is done for a new balise group without linking information (Subset-026, 3.4.4 [BL3 R2]) the ETCS On-board uses the estimated distance travelled between the previous LRBG and the new LRBG. Figure 5 illustrates the potential issue that arises.

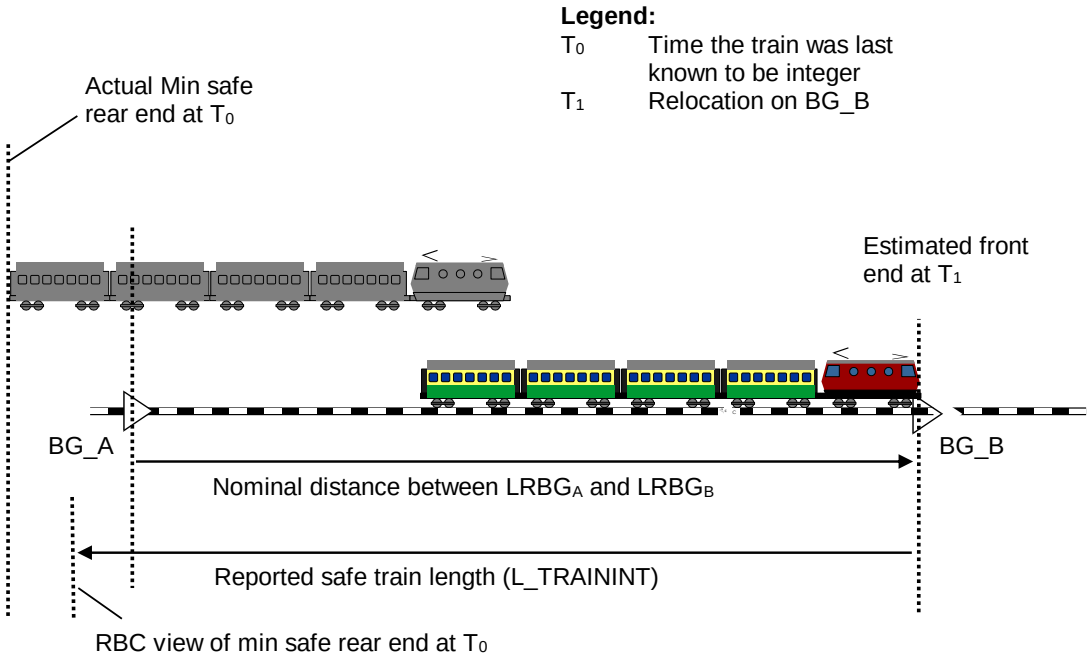


Figure 5: On-board mSRE relocation in the absence of linking information

At time T0 (i.e. the time when the train was last known to be integer), the LRBG was BG_A.

At time T1, BG_B is encountered, the ETCS On-board then relocates the min safe rear end at T0 to the new LRBG.

If linking information is not available or not used, the ETCS On-board then sends a position report to the L3 Trackside using the estimated distance between BG_A and BG_B when calculating the safe train length.

If this estimate is shorter than the real distance between BG_A and BG_B, the L3 Trackside believes that the confirmed rear end is closer to BG_A than it actually is.

This means that in case the train has been broken between time T0 and T1, but not yet detected by the TIMS device, there could be a part of the train in the section of track that was just cleared, but the L3 Trackside is not aware of this.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Use linking information on L3 lines (in all modes where linking is possible according to ETCS Baseline 3 Release 2 [BL3 R2]).
- Frequent position reporting in the position report parameters: if position reports are sent frequently, then this would limit the time (and distance) that a train can travel while storing the Min Safe Rear End position from when the train was last known to be integer. Limiting this distance means that the L3 Trackside may be able to more easily determine the LRBG that was the reference BG at the time the train was last known to be integer. In addition, the position report parameters could be set such that the ETCS On-board reports position when passing each LRBG compliant balise group. This would restrict the number of balise groups that can be passed before the train integrity information is reported to the L3 Trackside However, neither of these mitigations helps the L3 Trackside to determine the extent to which the train might be under-reading at the time of the relocation.
- Frequent reporting period of Train Integrity Monitoring System: this would limit the time and distance that the train can travel while storing Min Safe Rear End position when the train was last known to be integer. However, this mitigation does not help the L3 Trackside to determine the extent to which the train might be under-reading at the time of the relocation.
- L3 Trackside accounts for the possible error in the safe train length caused by lack of linking information in the safety margin added to the Train Location. However, this could have negative impact on operations if the added margin must be large.

Related Rules and requirements:

REQ-MovSR-4, REQ-MA-8

ASM-Integrity-6

5.3 Error in Train Length

5.3.1 Reported train length shorter than actual

H-TrainLength-001

Hazard headline:

Train Length value shorter than the actual length leading to collision, derailment or exceeding speed limits

Hazard description:

In case the Train Length given in the Validated Train Data to the L3 Trackside is shorter than the physical train length, this could result in:

- Another train being authorised beyond the rear of this train located in front, OR
- Infrastructure released (points moved) under the train, OR
- Train does not achieve calculated braking curves, OR
- Train permitted to accelerate earlier after speed restrictions.

The error in Train Length could be caused by:

- Incorrect train length provided by an external system.
- Incorrect train length entered by the Driver at Start of Mission.
- Driver does not update the train length after joining.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Use an external system providing the train length to avoid the risk of human errors.
- Operational rule for the Driver to validate the train length from external systems.
- Operational rule for the Driver to update the train length at Start of Mission.
- Operational rule for the Driver to update the train length after joining.
- Consider using the TMS or L3 Trackside (or both) to evaluate the train length for a Train Running Number based on information in the TMS for this train.
- Use TTD in places where trains are likely to change formation (split or join).

Related Rules and requirements:

OPE-Generic-4, OPE-StartTrain-1

5.3.2 Reported train length longer than actual

H-TrainLength-002

Hazard headline:

Train Length value longer than the actual length leading to collision or exceeding speed limits

Hazard description:

In case the Train Length given in the Validated Train Data to the L3 Trackside is longer than the physical train length, this could result in a part of track that is Occupied or Unknown being cleared while still occupied by another vehicle, or that the calculated braking curves are not met by the train.

The error in Train Length could be caused by:

- Incorrect train length provided by an external system.
- Incorrect train length entered by the Driver at Start of Mission.
- Driver does not update the train length after splitting.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Use an external system providing the train length to avoid the risk of human errors.
- Operational rule for the Driver to validate the train length from external systems.
- Operational rule for the Driver to update the train length at Start of Mission.
- Operational rule for the Driver to update the train length after splitting.
- Consider using the TMS or L3 Trackside (or both) to evaluate the train length for a Train Running Number based on information in the TMS for this train.
- Use TTD in places where trains are likely to change formation (split or join).

Related Rules and requirements:

OPE-Generic-4, OPE-StartTrain-1

5.4 CMD erroneously validates position

5.4.1 Wrong side failure in CMD

H-CMDerror-001

Hazard headline:

CMD erroneously validates a position which is incorrect leading to collision or derailment

Hazard description:

In case CMD validates the position of a train after being moved in NP mode, the L3 Trackside can give this train a Movement Authorisation based on the position at End of Mission while the train is now somewhere else. This may lead to derailment or collision.

Note that some CMD equipment may allow for a short movement of a train whilst still reporting "no cold movement detected".

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Hazardous failure rate for CMD to be considered.
- Use linking reaction for the first expected Balise Group in the linking chain when authorising trains to move, which will brake the train if it is not found as expected.
- Use TTD where trains start after NP mode. However, this is not enough on its own.

Related rules and requirements:

REQ-EoM-3, REQ-EoM-4, REQ-TrainLoc-3

ENG-EoM-2

5.5 Undetected movements

5.5.1 Rollback after standstill

H-Movements-001

Hazard headline:

Undetected backward movement after standstill leading to collision

Hazard description:

If a train moves backwards after reaching standstill, it could compromise the authorisation for another train. Depending on the frequency with which the TIMS is able to confirm integrity, it can take some time before the L3 Trackside can react on this potentially hazardous situation and try to prevent a collision.

Potential mitigations:

The L3 Trackside shall add a Safety Margin in rear of a train to mitigate for the potential rollback.

Related rules and requirements:

REQ-TrainLoc-3

ENG-Generic-6

5.5.2 Movement in NP mode

H-Movements-002

Hazard headline:

Undetected movement in NP mode leading to collision or derailment

Hazard description:

In case a train is moved in NP mode, the L3 Trackside has no knowledge of this and may authorise a conflicting train movement.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Consider NP movement in the Safety Margin added around trains at EoM. However, this might not be operationally feasible if the distance to consider is large.
- Operational rules for staff to inform Dispatcher before moving trains in NP mode and for the Dispatcher to protect this movement by an Unknown area.
- Operational rule to forbid movement in NP mode except in areas with TTD.

Related rules and requirements:

REQ-TrainLoc-3, REQ-EoM-3, REQ-EoM-4

ENG-EoM-2

5.5.3 At entrance to Level 3 area

H-Movements-003

Hazard headline:

Undetected movement entering the L3 area leading to collision

Hazard description:

In degraded situations, it could occur that a train incorrectly enters the L3 Area when it is not authorised and it is not detected by the L3 Trackside.

Potential mitigations:

Mitigation measures have to be implemented to protect other train movements in the L3 area. These could be:

- Detecting a non-communicating train by using TTD at the border to the L3 area.
- Not authorising a non-communicating train into a Level 3 Only area by keeping the last lineside signal at Danger or using special access control signals.
- Managing non-communicating trains through the use of balise telegrams
- Operational rule to assign an Unknown area in the L3 Trackside to make it possible for a non-communicating train to enter the L3 area in a controlled way.

Related rules and requirements:

REQ-LevelTrans-1

OPE-LossComms-1

ENG-LevelTrans-1

5.5.4 After End of Mission

H-Movements-004

Hazard headline:

Undetected movement after End of Mission leading to collision

Hazard description:

If a train in SB mode rolls away, Standstill Supervision will result in a brake application once the train moves beyond the distance D_NVROLL. This results in the train being brought to a halt, after which the driver can acknowledge the standstill supervision, releasing the brake. There is no limit on the number of acknowledgements the driver is allowed to make, since this may inhibit Splitting operations.

This functionality can enable the driver to use consecutive acknowledgements of the standstill supervision activation to move the train. Figure 6 illustrates the movement that could occur.

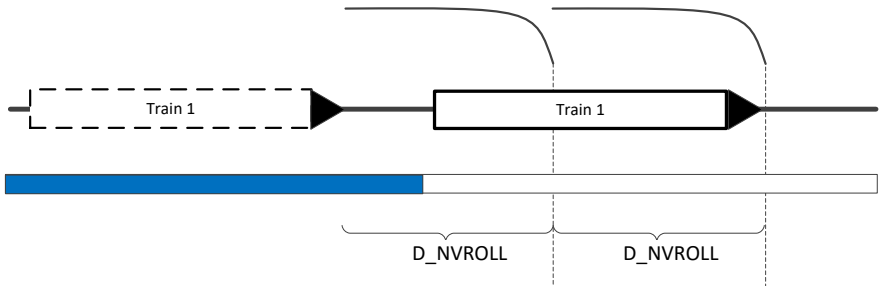


Figure 6: Train exiting the Unknown protective area after EoM

This creates a risk where the train could move outside the Unknown area created at EoM for protection, because ETCS does not prevent the use of consecutive roll away movements.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- An operational rule could state that the driver is not allowed to consecutively acknowledge the brake command thus releasing the brake application, in case a roll away has happened.
- Maintain a communication session in SB mode (after EoM) so that ETCS On-board could continue sending position reports. However, this would require a significant change to the current specifications.
- An operational rule could state that the driver powers off the ETCS On-board after End of Mission as in NP mode the emergency brake is permanently applied. However, this could be seen as operationally unacceptable.
- Selective use of TTD at locations where trains are normally parked so that the L3 Trackside can detect an unexpected movement.
- Recalculate safety margins in front and rear of the train at End of Mission to consider consecutive roll-away movements. However, this could have impact on operations if the value to consider is large.

Related rules and requirements:

REQ-EoM-3, REQ-EoM-4, REQ-TrainLoc-3

OPE-Generic-5

ENG-EoM-1

5.5.5 Loss of Train Integrity

H-Movements-005

Hazard headline:

Undetected movement of a part of the train after loss of integrity leading to collision

Hazard description:

In case train integrity has been lost and part of the train rolls backwards due to the gradient profile, this may result in a collision with other vehicles. In case of derailment, collisions can also occur on adjacent tracks.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Once Loss of integrity is reported to the L3 trackside, it could extend the Unknown area in rear of the CSRE.
- L3 Trackside informs the Dispatcher about the loss of integrity, giving a chance to apply further protective actions; this could include adjacent tracks.

It is noted that the Rolling Stock TSI requires automatic brake application after loss of integrity. However, this could fail.

Related rules and requirements:

REQ-TrackStatus-9, REQ-TrackStatus-10, REQ-HO-2

OPE-LossTI-1, OPE-LossTI-2

ENG-LossTI-5

5.5.6 Propelling train

H-Movements-006

Hazard headline:

Undetected movement beyond the secured area for a propelling train leading to collision

Hazard description:

In case a train is pushing another train in front of it (propelling movement) there is a risk that the front of the propelled train overpasses the area reserved for this movement as the driver in the propelling train cannot see where the front is. This can happen if there is need to rescue

a failed train from the rear. The rescue train will then be propelling a piece of rolling stock in front of it that cannot report its position.

If the front of this movement overpasses the reserved area, a collision may occur as the L3 Trackside is not aware of the real "front end" (belonging to the failed train) and able to react on this situation to protect other movements.

Potential mitigations:

The following consideration could be taken as mitigation measure:

- Operational rules are necessary to manage rescue movements.

Related rules and requirements:

OPE-Generic-6, OPE-REC-1

5.5.7 Shunting train

H-Movements-007

Hazard headline:

Undetected movement out of an activated shunting area leading to collision

Hazard description:

Shunting movements may unintentionally move beyond the border of an active shunting area without the L3 Trackside being aware of this and therefore being unable to protect other movements in the vicinity of the shunting area.

Potential mitigations:

There are the following options to protect against movements leaving an active shunting area:

- Operational rules are necessary to manage the shunting movements.
- Use of balises with Danger for Shunting or list of balises for SH area.
- Use of moveable infrastructure (e.g. points) that prevents leaving the shunting area.
- Use TTD to detect movements leaving the shunting area.

Related rules and requirements:

OPE-Generic-6

5.6 TTD erroneously indicates track clear

5.6.1 Wrong side failure of TTD

H-TTDfailure-001

Hazard headline:

TTD erroneously indicates a track Clear leading to collision or derailment

Hazard description:

If TTD is used to clear track irrespective of Train Locations, then:

- An Unknown area could be cleared without being swept,
- Infrastructure could be released or moved under a train,
- A Movement Authority could be extended beyond the CSRE of another train.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Define circumstances when TTD will not clear an Unknown area, e.g. active shunting areas and Unknown areas not allowed to be swept.
- Define whether infrastructure can be released solely on TTD information.
- Do not extend authorisations beyond the CSRE of trains.

It is noted that in ETCS Level 2, TTD information is relied upon to confirm the track is clear in all circumstances.

Related rules and requirements:

REQ-TTD-2, REQ-TTD-3

5.7 Points moved under train

5.7.1 Points Moved After Communications failure

H-Points-001

Hazard headline:

A point is moved in an Unknown area with a train over it, or when it is about to pass over it, leading to derailment

Hazard description:

The Dispatcher needs to move a train inside an Unknown area to a new location.

Figure 7 illustrates the situation with a train approaching a set of points inside an Unknown area.

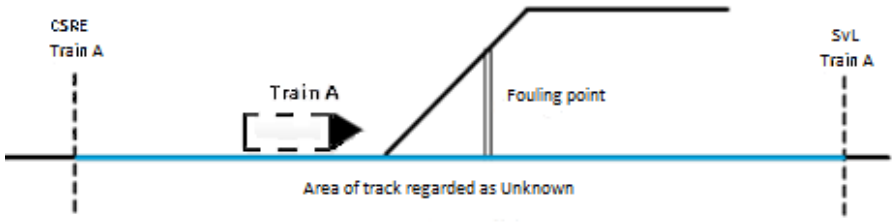


Figure 7: Unknown area due a Communication failure

The Dispatcher would need to move points so that the train can be moved to a siding.

In the absence of TTD, moving a point could cause a derailment if moved when a train is over or about to pass it.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Prevent the movement of points in an Unknown area, except by use of a special operational procedure to be followed by the Dispatcher.
- Use TTD over the points, and prevent points movement when the TTD is occupied, as in traditional signalling.

Related rules and requirements:

REQ-PTS-1, REQ-PTS-3

OPE-LossComms-1

5.8 Hazards identified but present already in ETCS L2

The hazards in this section were also identified by the work on Moving Block/L3, but, after examination, were found to be already present in L2.

In some cases, there are additional mitigations possible in ETCS Level 3 Moving Block, which are given in the proposed mitigations.

5.8.1 Mixed traffic

H-Level2-001

Hazard headline:

Non-ETCS train erroneously enters a route for an ETCS L3 train leading to collision

Hazard description:

Drivers that operate both ETCS and non-ETCS fitted trains may mistakenly use a 'proceed for ETCS' aspect when operating a non-ETCS train due to confusion of ETCS and non-ETCS experience. Such a situation may result in a SPAD (Signal Passed At Danger) and a collision. This could happen at borders to the L3 Area but also inside an area with mixed traffic where L3 is used as an overlay to a conventional system with optical signals.

This hazard is the same as in Level 2. It is the same situation as a non-ETCS train erroneously entering a route set for a Level 2 train in a mixed traffic area.

Potential mitigations:

Mitigations for this hazard should be project specific. Suggested mitigations are:

- A non-ETCS train passing an ETCS signal shall be tripped as it would when passing a signal at danger, for example using a Class B system.
- TTD at the L3 boundary to detect non-ETCS trains entering the area.

Related rules and requirements:

ENG-LevelTrans-1

5.8.2 Reversing

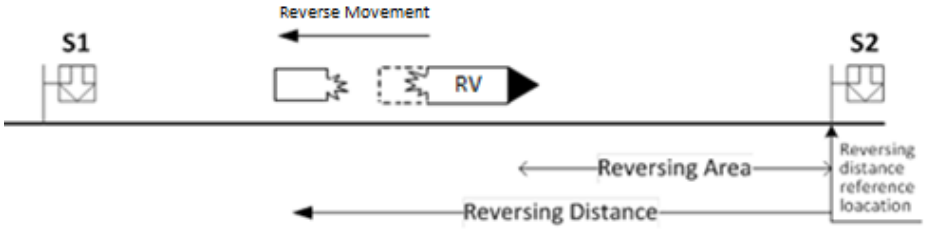
H-Level2-002

Hazard headline:

Train moves backwards after loss of integrity leading to collision

Hazard description:

In case a train needs to reverse after a loss of integrity it may collide with the part of the train that



was lost (see

Figure 8).

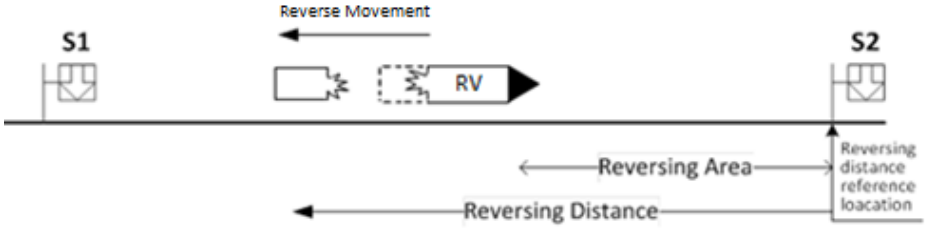


Figure 8: Train reversing after loss of integrity

This hazard is the same as in Level 2, and in conventional signalling.

Potential mitigations:

There are additional potential mitigations in Level 3:

- Reversing could be prevented if Loss of Train Integrity is detected.
- The Driver can be alerted if Loss of Train Integrity is detected.
- The Dispatcher can be alerted if Loss of Train Integrity is detected.

Related rules and requirements:

REQ-LossTI-4

ASM-Integrity-1

5.8.3 Loss of train integrity

H-Level2-003

Hazard headline:

Derailment after loss of integrity causes adjacent tracks to become occupied leading to collision

Hazard description:

After a loss of integrity, the lost part of the train could derail causing an obstruction in the adjacent track resulting in a collision.

This hazard is the same as in Level 2, and in traditional signalling.

Potential mitigations:

There are additional potential mitigations in Level 3:

- Once Loss of integrity is reported to the L3 trackside, it could extend the Unknown area to cover adjacent tracks around the area where the loss of integrity occurred.
- L3 Trackside can inform the Dispatcher about the loss of integrity, giving a chance to apply protective actions.

It is noted that the Rolling Stock TSI requires automatic brake application after loss of integrity, but this could fail.

Related rules and requirements:

REQ-TrackStatus-9, REQ-TrackStatus-10, REQ-HO-1

OPE-LossTI-1

6 Conclusions

The Preliminary Safety Analysis is focused on ETCS L3 Moving Block operational scenarios developed by X2Rail-1 WP5 Moving Block.

This analysis has considered and reviewed 16 different scenarios to identify hazards resulting from Level 3 operation.

Potential mitigation measures have been proposed. When possible, specific requirements and rules in the WP5 deliverables D5.1 and D5.2 have been traced to each hazard as potential mitigations.

In some cases, specific assumptions related with external systems to ETCS have been identified in D5.1 as possible mitigation.

This Preliminary Safety Analysis is not quantitative. The frequency and severity have not been quantified for the hazards at this stage. Therefore, it is not possible to assume that the proposed mitigations reduce the risks to tolerable levels. Further analysis is required to demonstrate whether the referenced requirements and rules fully address the hazards.

Future work to be developed in X2Rail-3 will include:

- Additional requirements or rules to cover the potential mitigations have been identified. The following potential updates to D5.1/D5.2 will be addressed in X2RAIL-3.

Section	Additional requirements or rules
5.1.3	There is a missing Operational rule about establishing a temporary shunting area is clear before deactivating.
5.2.1	The last mitigation suggests a need for an Engineering Rule regarding the designed balise accuracy and the NV.
5.2.2	The first mitigation suggests an Engineering Rule that Linking must always be used in L3 areas
5.4.1	The second mitigation suggests an Engineering Rule to apply linking reaction should be considered.
5.5.1	An Operational rule about moving in SB should be considered.
5.5.2	The 2nd and 3rd mitigations imply the need for potential Operational rules.
5.5.4	The 1st mitigation infers the need for an Operational Rule.

Section	Additional requirements or rules
5.5.6	The linkage to OPE-REC-1 might mean update is needed to the rule.
5.5.7	The last mitigation could give rise to an Engineering Rule.
5.7.1	Engineering rule to cover TTD over points (see 2nd mitigation)

- Quantitative analyses will be undertaken to confirm the significance of the hazards and the effectiveness of the mitigations checking that the linked requirements and rules fully address the identified hazards.
- As further work is performed (for example working with TIMS, Hybrid L3 [HL3], etc.) additional new hazards might be identified, and therefore, the Preliminary Safety Analysis should be updated accordingly.

7 References

The following documents are referenced in this document:

Reference	Document Name
[BL3 R2]	Set of specifications # 3 (ETCS baseline 3 and GSM-R baseline 1)" within the CCS TSI.
[CRProcess]	Change Control Management process ERA_ERTMS_0001_v.2.0
[CR940]	Opinion ERA/OPI/2017-2 (https://www.era.europa.eu/sites/default/files/library/docs/opinion-advice/opinion_era-opi-2017-2_en.pdf)
[CSM]	Commission Regulation on the adoption of a common safety method on risk evaluation and assessment as referred to in Article 6(3)(a) of Directive 2004/49/EC of the European Parliament and the Council
[EN50126]	EN 50126-1:2017: Railway Applications -The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
[D2.1]	X2Rail-1 Deliverable D2.1 "Reference Architecture"
[D5.1]	Moving Block System Specification
[D5.2]	Moving Block Operational and Engineering Rules
[D5.4]	Moving Block Application Report
[HL3]	Hybrid ERTMS/ETCS Level 3 Principles, ERTMS Users Group, V. 1C 13/07/2018
[NGTCD51]	"D5.1 Moving Block Principles" "D5.2 Validation of Moving Block Principles" Deliverables from EU project: Next Generation of Train Control systems Seventh Framework Programme EC Contract Number: FP7 605402
[X2R glossary]	X2R2-WP2-T-DBA-004-01_-_IP2_integrated_glossary.