Horizon 2020
European Union Funding
for Research & Innovation

Shift2Rail

X2RAIL 5

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 D4.1

Moving Block Specification

Part 6 – Safety Analysis

Due date of deliverable	Month 24
Actual submission date	21-Dec-2022
Organization name of lead contractor for this deliverable	SMO
Dissemination level	PU
Revision	Final

Version Management

The Version history below refers to Part 6 of Deliverable D4.1.

Version Management		
Version Number	**Modification Date**	**Description / Modification**
01	26-Feb-21	Import from X2Rail-3 D4.2, no changes
02	30-Apr-21	Add X2Rail-3 cross-reference tags
03	25-May-21	Update for X2Rail-3 Train Location Open Points
04	28-Oct-22	Updated for remaining X2R5 Open Points
05	18-Nov-22	Updated after first WP4 Review
06	25-Nov-22	Updated for TMT/SC review
07	25-Nov-22	Clean version for TMT/SC review
08	20-Dec-22	Updated after TMT/SC review and further WP4 review
09	21-Dec-22	Clean version of 08
10	21-Dec-22	PDF version of 09

Table of Contents

Table of Figures

Table of Tables

1 Background

This document is Part 6 of Deliverable D4.1 “Moving Block Specifications” from the Project titled “Completion of activities for Adaptable Communication, Moving Block, Fail Safe Train Localisation (including satellite), Zero on site Testing, Formal Methods and Cyber Security” (Project Acronym: X2Rail-5; Grant Agreement No 101014250).

Deliverable D4.1 is made up of several different parts. This is Part 6 – Safety Analysis. See Part 1 – Introduction for a list of the different Parts of this Deliverable.

All terms and abbreviations, and all references for all parts of D4.1 are located in Part 1 – Introduction.

In this document the principal ETCS Level 3 hazards have been identified, the causes considered, potential mitigations identified and linkage to the requirements and rules has been established.

The Risk analysis of the hazards has been formally assessed in section 5. [EN50126] was used as reference for this analysis.

This safety analysis follows the phases described on [CSM-RA]:

- Hazards identification 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.
- Risk estimation based on the frequency and severity estimated for every hazard.
- The requirements and rules from D4.1 Parts 3, 4 and 5 have been traced as mitigations for the hazards in order to reduce the level of risk.

2 Scope

2.1 Document scope

This is one part of a set of documents that cover aspects of ETCS Level 3 systems as described in D4.1 - Part 1.

This document contains the description of all the ETCS Level 3 related hazards that have been identified as a result of the safety analysis for an ETCS Level 3 system. Potential mitigations have been proposed for all these hazards.

In addition, for some hazards already present in ETCS Level 2, possible additional mitigations were found in ETCS Level 3.

2.2 Application Scope

2.2.1 Railway Types

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

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

Mixed Traffic Lines for example may include passenger and freight trains.

It is the intent that these can all be handled by the same generic ETCS Level 3 system. However, there will be differences in the way the L3 Trackside is applied to different types of railways.

2.2.2 Grade of Automation

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.

2.3 System Scope, Assumptions & Constraints

See D4.1 - Part 2 System Definition.

3 Safety Analysis

There has been dedicated Safety Analysis work performed within X2Rail-1 and X2Rail-3. Within X2Rail-5 the Safety Analysis has been updated as part of the work to complete the Moving Block Specification. The following subsections describe the work performed in each of the three X2Rail projects where there was work on Moving Block.

This project applied the methodology defined by Common Safety Method for Risk Evaluation and Acceptance [CSM-RA].

According to CSM the following phases shall be followed:

- System definition (see D4.1 - Part 2)
- Hazard identification and classification (see section 4)
- Explicit risk estimation (see section 5)
- Risk evaluation (this phase should be completed at specific application level)

3.1 X2Rail-1 Methodology

The Safety Analysis work in X2Rail-1 included the System Definition (see D4.1 Part 2) and the Hazard Identification.

The project held a series of specific workshops and defined scenarios covering both normal and degraded operation of the L3 Railway.

Working Scenario Description documents were produced which were used as the basis for establishing the relevant L3 Trackside Requirements, Engineering and Operational Rules.

Since these documents describe relevant events and the interaction of requirements and rules, they were used as an input for the hazard identification phase. The resulting hazards are contained in section 4 below.

Scenario Descriptions were reviewed by the Safety Representatives in order to identify:

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

3.2 X2Rail-3 Methodology

During X2Rail-3, the Scenario Descriptions from X2Rail-1 were reworked as Use Case Descriptions.

The Safety Analysis work in X2Rail-3 was to:

- Recheck the Hazards identified in X2Rail-1, using the Use Case Descriptions
- Perform a Risk Assessment of the Hazards

Each hazard has been assessed in accordance with the risk acceptance principles allowed by [CSM-RA] in order to complete the Explicit risk estimation phase. The results of the Risk Assessment are shown in section 5.

According to the Risk Assessment most hazards have been considered as Intolerable and mitigations are required in order to lower the risk level.

Requirements, Operational Rules and Engineering Rules have been traced as potential mitigations for every hazard to lower the risk to a tolerable level.

In accordance with [CSM-RA], Risk evaluation shall be undertaken at specific application project level to confirm whether the chosen mitigations reduce the risks to a tolerable level.

3.3 X2Rail-5 Methodology

There was no explicit Safety Analysis task within X2Rail-5, and therefore no specific safety team. The work in X2Rail-5 has been to update the Hazard Analysis, including the links to Requirements (Part 3), Operational Rules (Part 4) and Engineering Rules (Part 5).

3.4 Roles and functions

The Roles and Functions described below apply to the work performed during X2Rail-1 and X2Rail-3, when there was a dedicated safety team.

3.4.1 Safety Task leader

Responsibilities:

- Planning and co-ordination of Safety activities.
- Creation and continuous update of Safety Analysis.

3.4.2 Safety Representatives

Responsibilities:

- Safety assessment.
- Identify the hazards that could occur in the steps of the Scenario Descriptions and Use Cases.
- Propose mitigation measures for the hazards.

4 Hazard identification and classification

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 requirements, rules and assumptions**: 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.

The hazards have been classified according to the following table:

Section	Hazard	Summary	Causes
4.1	Track status erroneously cleared	This section describes causes which result in a Clear Track Status Area by the L3 Trackside, when there is in fact an obstruction present	• Dispatcher interaction in L3 Trackside initialisation • Using invalid/outdated stored information for L3 Trackside initialisation • Deactivating Temporary Shunting Area • Driver confirms train integrity • Recovery of a failed train
4.2	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
4.3	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
4.4	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

Section	Hazard	Summary	Causes
4.5	Undetected Movements	This section describes causes which result in undetected movement of a train	• Rollback after standstill • Unreported Movement • At entrance to Level 3 area • After End of Mission • Loss of Train Integrity • Propelling train • Shunting train
4.6	TTD erroneously indicates track clear	This section describes the result of a TTD which erroneously indicates a section of track as Clear Track Status Area	• Wrong side failure of TTD
4.7	Points Moved under train	This section describes the result of moving a point after communications failure	• Points Moved After Communications failure

Table 1 – Hazard Classification

Additionally, section 4.8 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.

4.1 Track status erroneously cleared

4.1.1 Dispatcher interaction in L3 Trackside initialisation

H-Clearing-001 [X2Rail-3 D4.2 H-Clearing-001]

Hazard headline:

Track Status Area 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 Train Location of all vehicles and obstructions in the Area.

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

Potential mitigations:

At initialisation, L3 Trackside considers the entire L3 Area as Unknown Track Status Area and a process will be required to declare areas as Clear Track Status Areas. This 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 Track Status Areas as clear in the 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 4.1.2).

Related rules and requirements:

REQ-TrackInit-1, REQ-TrackInit-2, REQ-TrackInit-3, REQ-TrackInit-4, REQ-TrackInit-5, REQ-TrainLoc-2, REQ-TrackStatus-27, REQ-RecoveryMgmt-2, REQ-RecoveryMgmt-3

OPE-TrackInit-1, OPE-TrackInit-2, OPE-TrackInit-3, OPE-TrackInit-4, OPE-Generic-1, OPE-Generic-2

ENG-TrackInit-1, ENG-TrackInit-2

4.1.2 Using invalid/outdated information for L3 Trackside initialisation

H-Clearing-002 [X2Rail-3 D4.2 H-Clearing-002]

Hazard headline:

Track Status Area 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 Train Location of all vehicles in the Area.

If the L3 Trackside utilises stored information to clear Track Status Areas, 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 the track clear when it is still occupied.

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-2, REQ-TrackStatus-27, REQ-TrackInit-4

OPE-TrackInit-1, OPE-TrackInit-2, OPE-TrackInit-3, OPE-TrackInit-4

ENG-TrackInit-1, ENG-TrackInit-2

4.1.3 Deactivating Temporary Shunting Area

H-Clearing-003 [X2Rail-3 D4.2 H-Clearing-003]

Hazard headline:

Track Status Area erroneously cleared after deactivation of a Temporary Shunting Area leading to collision

Hazard description:

The L3 Trackside considers the track status in an Active Shunting Area as Unknown Track Status Area, except for the Train Location of communicating trains. When deactivating a Shunting Area, responsible staff may have the possibility to clear any remaining Unknown Track Status Area. Doing this, an occupied area of track could be set to clear, leading to collision.

Potential mitigations:

Mitigations will be required to declare Clear Track Status Areas after deactivation of a Shunting Area. These could include:

- Operational Rules to manage track occupancy – the rules are around whether the responsible person can remove or reduce Unknown Track Status Areas in the L3 Trackside system.
- Using sweeping trains.
- Defining Temporary Shunting Areas on areas where TTD are available.

Related rules and requirements:

REQ-TTD-7, REQ-TrackStatus-14, REQ-TrackStatus-24

OPE-Generic-1, OPE-Generic-2, OPE-SH-2

4.1.4 Driver confirms train integrity

H-Clearing-004 [X2Rail-3 D4.2 H-Clearing-004]

Hazard headline:

Track Status Area 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 a device to confirm integrity, avoiding human interaction.

Related rules and requirements:

REQ-TrainLoc-9

OPE-Generic-3, OPE-SoM-1, OPE-REC-1

ENG-LossTI-2

4.1.5 Recovery of a failed train

H-Clearing-005 [X2Rail-3 D4.2 H-Clearing-005]

Hazard headline:

Track Status Area erroneously cleared by TIMS device not being able to detect loss of train integrity after coupling 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 in the front part of the train if it cannot cover the complete train after joining.
- The Dispatcher could set an Unknown Track Status Area to protect rescue operations.
- Use a safe TIMS, compatible between trains.

Related rules and requirements:

REQ-TrackStatus-22, REQ-TrackStatus-23

OPE-Generic-7

4.2 Error in Train Location

4.2.1 Confidence interval reduced at End of Mission

H-TrainLoc-001	[X2Rail-3 D4.2 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.

However, as part of the ERA CCM Process an ambiguity in the specifications has been identified which makes it 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 Track Status 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. See CR1318.
- L3 Trackside ignores the confidence interval in the EoM Position Report and uses the latest Train Position Report before the one reported in SB for determining the confidence interval.
- Balises in the L3 Area are engineered with a location accuracy equal or better than the National Value.

Related rules and requirements:

REQ-EoM-4

ENG-Generic-4

4.2.2 Lack of linking information

H-TrainLoc-002 [X2Rail-3 D4.2 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. Next figure illustrates the potential issue that arises.

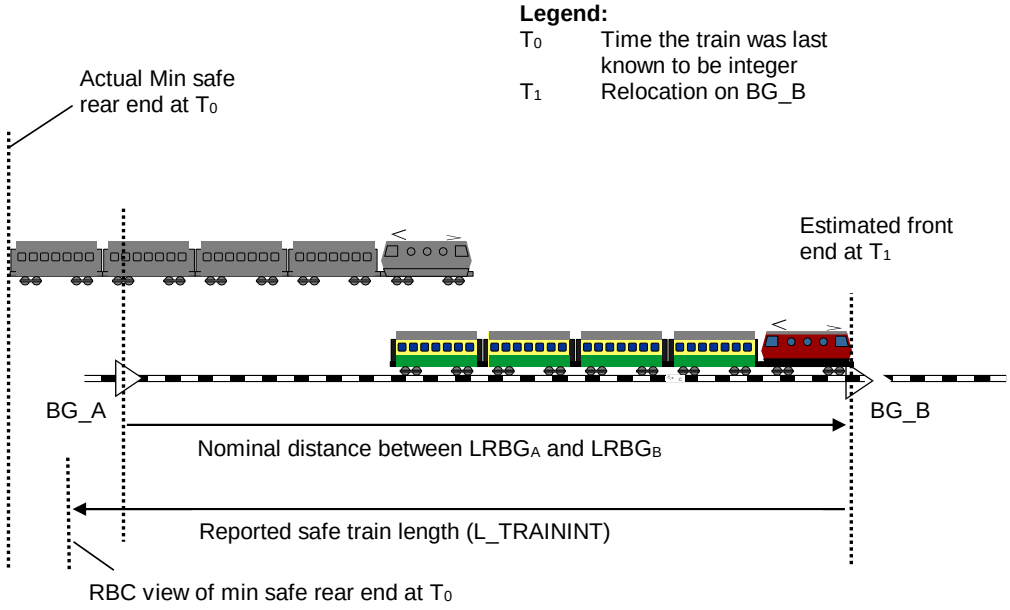

Figure 1: On-board mSRE relocation in the absence of linking information

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 TIMS: 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.

Related Rules and requirements:

REQ-MA-6

ENG-Generic-8

ASM-Integrity-7

4.3 Error in Train Length

4.3.1 Reported train length shorter than actual

H-TrainLength-001 [X2Rail-3 D4.2 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 a safe 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:

REQ-TrainLoc-6

OPE-Generic-5

ASM-Length-1

ASM-Length-2

4.3.2 Reported train length longer than actual

H-TrainLength-002 [X2Rail-3 D4.2 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 Track Status Area which 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 a safe 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.
- TMS providing information about the train length for a certain train running number. L3 trackside could compare this length with the one reported by the train and provide a warning in the case they don't match.
- Use TTD in places where trains are likely to change formation (split or join).

Related Rules and requirements:

REQ-TrainLoc-6

OPE-Generic-5

ASM-Length-1

ASM-Length-2

4.4 CMD erroneously validates position

4.4.1 Wrong side failure in CMD

H-CMDerror-001 [X2Rail-3 D4.2 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 Authority 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-TTD-9, REQ-TTD-10, REQ-TTD-12

ENG-EoM-1, ENG-Generic-8

4.5 Undetected movements

4.5.1 Rollback after standstill

H-Movements-001 [X2Rail-3 D4.2 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. 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 consider the potential rollback when issuing Movement Authorities.

The L3 Trackside can be engineered with a L3 Margin. When defining the MA for a Train 1, a distance not shorter than the L3 Margin shall be introduced between the EoA and the DP (located at CRE of Train 2), as shown in Figure 2.

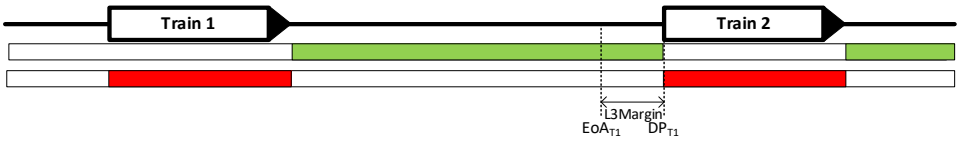

Figure 2: Margin between EoA and DP

The following risk assessment supports this mitigation:

- **Event 1:** Train 1 is rolling back (Frequency estimated as *Probable*)
- **Event 2:** Train 2 exceeding EoA (Frequency estimated as *Occasional*)
- Event 1 and Event 2 happen simultaneously (Frequency for Train 2 exceeding EoA when Train 1 has rolled back estimated as *Rare*)
- **Hazard:** Collision at low speed (Severity for this hazard estimated as *Marginal*)

These estimates were agreed according to [EN50126] by safety and railways representatives during a specific workshop (see [RiskWShop]).

As a conclusion the risk for Train 1 rolling back and Train 2 exceeding EoA at the same time could be considered as *Tolerable.*

Other potential mitigation would be:

- 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 ETCS specifications.

Related rules and requirements:

REQ-MA-2, REQ-MA-2, REQ-EoAExclusionArea-4

ENG-Generic-5 ENG-PTS-1, ENG-PTS-2

OPE-Generic-6

4.5.2 Unreported Train Movement

H-Movements-002	[X2Rail-3 D4.2 H-Movements-002]

Hazard headline:

Unreported Train movement leading to collision or derailment

Hazard description:

If a non-communicating train is moved, the movement is not reported to the trackside, and therefore the L3 Trackside has no knowledge of the movement, and may authorise a conflicting train movement.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Operational rules for staff to inform Dispatcher before moving non-communicating trains and for the Dispatcher to protect this movement by an Unknown Track Status Area.
- Operational rule to forbid movement of non-communicating trains without protection provided by the Dispatcher, even in areas with TTD.

Related rules and requirements:

REQ-TTD-9, REQ-TTD-10, REQ-TTD-12

OPE-Generic-6, OPE-LossComms-1

ENG-EoM-1

4.5.3 At entrance to Level 3 area

H-Movements-003 [X2Rail-3 D4.2 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 must be implemented to protect other train movements in the L3 area. These could be:

- Detecting a non-communicating train by using short TTD sections at the borders of the L3 Area of Control.
- 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 Track Status 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, REQ-TTD-9, REQ-TTD-10, REQ-TrackStatus-22, REQ-TrackStatus-23

OPE-Generic-7, OPE-LossComms-1

ENG-LevelTrans-1

4.5.4 After End of Mission

H-Movements-004 [X2Rail-3 D4.2 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 3 illustrates the movement that could occur.

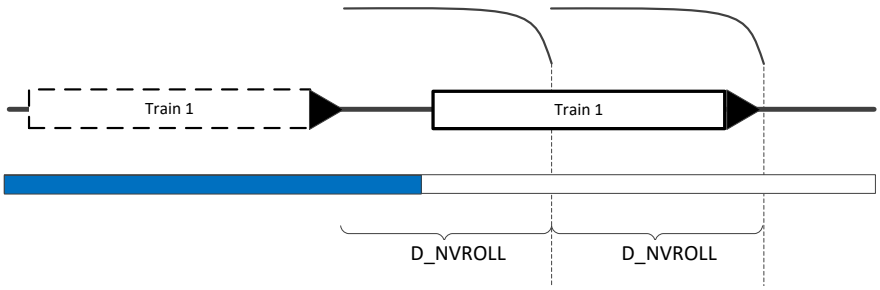

Figure 3: Train exiting the Unknown protective area after EoM

This creates a risk where the train could move outside the Unknown Track Status 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 ETCS 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. (In areas with TTD the L2 risk for more than one train in the same TTD still remains.)
- Train movements in SB mode must have protection provided within the L3 Trackside, for example via an Unknown Track Status Area created by the Dispatcher.

Related rules and requirements:

REQ-TTD-9, REQ-TTD-10, REQ-TTD-12, REQ-TrackStatus-22, REQ-TrackStatus-23

OPE-Generic-6

ENG-EoM-1

4.5.5 Loss of Train Integrity

H-Movements-005 [X2Rail-3 D4.2 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 Track Status Area in rear of the CRE.
- 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-LossTI-1, REQ-LossTI-2, REQ-LossTI-3, REQ-LossTI-4, REQ-LossTI-6

OPE-LossTI-1

ENG-LossTI-4

4.5.6 Propelling train

H-Movements-006 [X2Rail-3 D4.2 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. As mSFE and Train length doesn't match with the real train this could lead to a wrong track status.

Potential mitigations:

The following consideration could be taken as mitigation measure:

- Operational rules are necessary to manage rescue movements.
- (e.g. OS movement authority is provided in such manner that the propelling train has to stop before the propelled train goes beyond the area reserved for the rescue.)
- Use of TTD.

Related rules and requirements:

REQ-TTD-9, REQ-TTD-10

OPE-Generic-7, OPE-OS-2, OPE-REC-1

4.5.7 Shunting train

H-Movements-007 [X2Rail-3 D4.2 H-Movements-007]

Hazard headline:

Undetected movement out of an Active 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:

REQ-TTD-9, REQ-TTD-10, REQ-TTD-12

OPE-SH-1

ENG-SH-1

4.6 TTD erroneously indicates track clear

4.6.1 Wrong side failure of TTD

H-TTDfailure-001 [X2Rail-3 D4.2 H-TTDfailure-001]

Hazard headline:

TTD erroneously indicates a Clear Track Status Area leading to collision or derailment

Hazard description:

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

- An Unknown Track Status Area could be cleared without being swept,
- Infrastructure could be released or moved under a train,
- Erroneously updating the CRE of the train in front, and consequently providing an MA to a following train that could result in a collision.

Potential mitigations:

The following considerations could be taken as mitigation measures:

- Define circumstances when TTD will not clear an Unknown Track Status Area, e.g. Active Shunting Areas and Non-Sweepable Unknown Track Status Areas.
- Define whether infrastructure can be released solely on TTD information.
- Do not extend authorisations beyond the CRE 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-1, REQ-TTD-4, REQ-TTD-12, REQ-SH-2

ENG-TTD-1

4.7 Points moved under train

4.7.1 Points Moved in an Unknown/Occupied/Reserved area

H-Points-001 [X2Rail-3 D4.2 H-Points-001]

Hazard headline:

A point is moved in an Unknown/Occupied/Reserved Track Status 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, Occupied or Reserved Track Status Area to a new location.

Figure 4 illustrates the situation with a train approaching a set of points inside an Unknown Track Status Area.

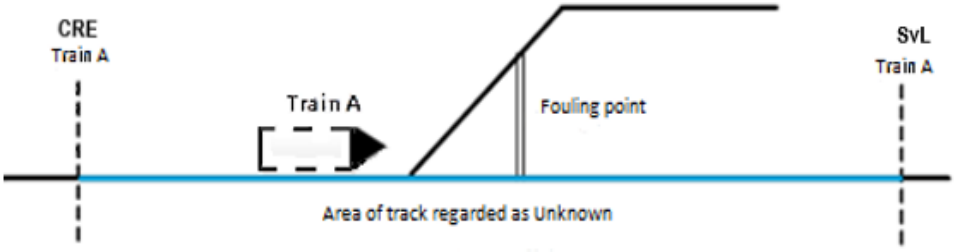

Figure 4: Unknown Track Status Area due a Communication failure

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, Occupied or Reserved Track Status 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.
- Moving the train in SR mode would mitigate the risk before passing over the points.

Related rules and requirements:

REQ-PTS-1, REQ-PTS-2, REQ-PTS-3, REQ-EoAExclusionArea-4

OPE-Generic-8

ENG-PTS-1, ENG-PTS-2, ENG-Generic-2

4.8 Hazards identified but present already in ETCS L2

The hazards in this section were also identified by the work on ETCS Level 3, but after examination, were found to be already present in L2.

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

4.8.1 Mixed traffic

H-Level2-001 [X2Rail-3 D4.2 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.
- A short TTD section at the L3 border to detect non-ETCS trains entering the area.

Related rules and requirements:

REQ-LevelTrans-1

OPE-LossComms-1

ENG-LevelTrans-1

4.8.2 Reversing

H-Level2-002 [X2Rail-3 D4.2 H-Level2-002]

Hazard headline:

Train moves backwards after loss of train integrity leading to collision

Hazard description:

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

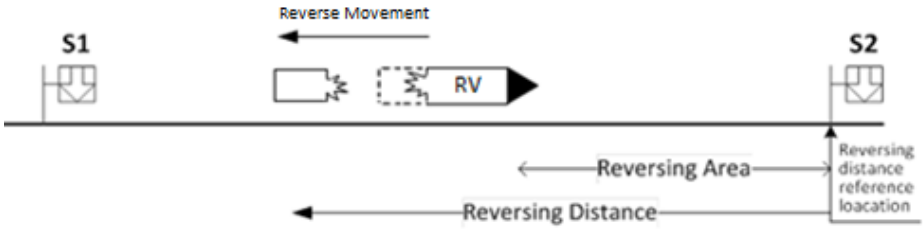

Figure 5: Train reversing after loss of integrity

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

Potential mitigations:

There are additional potential mitigations in Level 3:

- 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-3

OPE-LossTI-1, OPE-LossTI-2

ENG-LossTI-4

4.8.3 Loss of train integrity

H-Level2-003 [X2Rail-3 D4.2 H-Level2-003]

Hazard headline:

Derailment after loss of train integrity causes obstruction in adjacent tracks leading to collision

Hazard description:

After a loss of train 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 Track Status 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-LossTI-3

OPE-LossTI-1, OPE-LossTI-2

ENG-LossTI-4

5 Explicit risk estimation

This section contains the results of the risk assessment completed according to [EN50126] in order to identify the level of risk for every hazard as defined for the Risk evaluation phase according to [CSM-RA].

This Risk Assessment considers the hazards and causes for a generic ETCS Level 3 system. Differences between Full Moving Block and Fixed Virtual Blocks have not been considered for this analysis.

This analysis is based on two factors:

- how likely are the hazards to occur?
- what the consequences might be?

The risk estimation before mitigations for every hazard is based on severity and frequency estimations agreed by Safety representatives and railways experts during a workshop [RiskWShop].

The frequency levels used are those from [EN50126], and are shown in Table 2.

Frequency level	Description
Frequent	Likely to occur frequently. The event will be frequently experienced.
Probable	Will occur several times. The event can be expected to occur often.
Occasional	Likely to occur several times. The event can be expected to occur several times.
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.

Table 2 – Frequency level table from [EN50126]

The severity categories used are those from [EN50126], and are shown in Table 3.

Severity category	Consequences to persons or environment	Consequences on service/property
Catastrophic	• Affecting a large number of people and resulting in multiple fatalities, and/or • extreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	• Affecting a very small number of people and resulting in at least one fatality, and/or • large damage to the environment	Loss of a major system
Marginal	• No possibility of fatality, severe or minor injuries only, and/or • minor damage to the environment	Severe system(s) damage
Insignificant	• Possible minor injury	Minor system damage

Table 3 – Severity categories table from [EN50126]

The estimated frequency and severity for each hazard were then used to derive a risk category. The risk categories used are those from [EN50126], and are shown in Table 4.

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	**Intolerable**	**Intolerable**	**Intolerable**
Probable	Tolerable	Undesirable	**Intolerable**	**Intolerable**
Occasional	Tolerable	Undesirable	Undesirable	**Intolerable**
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			

Table 4 – Risk Categories table from [EN50126]

The results of the Risk Analysis for each hazard are shown in Table 5.

For non-operational hazards related to technical failures (H-TrainLoc-001, H-TrainLoc-002, H-CMDerror-001 and H-TTDfailure-001) no frequency has been estimated; the hazard will appear every time the device fails.

Requirements, Operational rules, Engineering rules and Assumptions have been traced as potential mitigations for every hazard, as shown in the entries in section 4. In accordance with [CSM-RA], Risk evaluation shall be undertaken at specific application project level to confirm whether the chosen mitigations reduce the risks to a tolerable level.

Hazard	Causes	Hazard ID	Severity	Frequency	Risks before mitigation
Track status erroneously cleared	Dispatcher interaction in L3 Trackside initialisation	H-Clearing-001	Catastrophic	Occasional	Intolerable
	Using invalid/outdated information for L3 Trackside initialisation	H-Clearing-002	Catastrophic	Rare	Undesirable
	Deactivating Temporary Shunting Area	H-Clearing-003	Catastrophic	Rare	Undesirable
	Driver confirms train integrity	H-Clearing-004	Catastrophic	Probable	Intolerable
	Recovery of a failed train	H-Clearing-005	Catastrophic	Rare	Undesirable
Error in Train Location	Confidence interval reduced at End of Mission	H-TrainLoc-001	Catastrophic		Intolerable
	Lack of linking information	H-TrainLoc-002	Catastrophic		Intolerable

Hazard	Causes	Hazard ID	Severity	Frequency	Risks before mitigation
Error in Train Length	Reported train length shorter than actual	H-TrainLength-001	Catastrophic	Frequent	Intolerable
	Reported train length longer than actual	H-TrainLength-002	Catastrophic	Frequent	Intolerable
CMD Erroneously Validates Position	Wrong side failure of CMD	H-CMDerror-001	Catastrophic		Intolerable
Undetected Movements	Rollback after standstill	H-Movements-001	Catastrophic	Probable	Intolerable
	Movement in NP mode	H-Movements-002	Catastrophic	Rare	Undesirable
	At entrance to Level 3 area	H-Movements-003	Catastrophic	Probable	Intolerable
	After End of Mission	H-Movements-004	Catastrophic	Probable	Intolerable
	Loss of Train Integrity	H-Movements-005	Catastrophic	Improbable	Undesirable
	Propelling train	H-Movements-006	Catastrophic	Probable	Intolerable
	Shunting train	H-Movements-007	Catastrophic	Occasional	Intolerable

Hazard	Causes	Hazard ID	Severity	Frequency	Risks before mitigation
TTD erroneously indicates track clear	Wrong side failure of TTD	H-TTDfailure-001	Catastrophic		Intolerable
Points Moved under train	Points Moved After Communications failure	H-Points-001	Catastrophic	Probable	Intolerable

Table 5 – Risk Assessment Table

6 Conclusions

The Safety Analysis is based on ETCS Level 3 Use Cases developed by X2Rail-3 WP4 Moving Block, and updated during X2Rail-5 WP4 Moving Block.

After reviewing all Use Cases this analysis confirms the list of hazards identified from X2Rail-1 WP5.

Specific requirements and rules have been traced to each hazard as potential mitigations.

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

The risk level of every hazard could be mitigated by the application of those requirements, rules and assumptions identified as mitigations.

In accordance with [CSM-RA], further Risk analysis is required at specific application level to demonstrate whether the referenced mitigations fully address the hazards for a project.

In case the residual risks after mitigations are not considered as tolerable, additional measures will be required.