General Concept ETCS Interlocking

Dieses Dokument ist im Programm smartrail 4.0 in Bearbeitung. Sein Inhalt kann sich noch ändern und hat noch keinen verbindlichen Charakter. Die Vollständigkeit und Korrektheit der Inhalte dieses Dokumentes ist noch nicht gewährleitstet bzw. noch in Überprüfung.

This document is a DRAFT version which is still under construction. Its content may change, is not completely verified and is not yet finalized.

1 Change History

Version (revision)	Updated	Changes	Last status
1.0 (49206)	Grabowski David (I-AT-SAZ-SIH) Mon Feb 26 10:06:19 CET 2018	Release for "Sicherheitsstelle SR40"	Published
1.01 (49234)	Current	Release to publish	
1.2 (132432)	31.08.2018	Release for "Sicherheitsstelle SR40"	

2 Glossary

Term	Abbrev.	Description
Clear Track Signalling Installation	CTS	Trackside installation that indicates track clearance (occupation or non-occupation).
Communications-based train control (CBTC)	CBTC	**Communications-based train control** (**CBTC**) is a railway signalling system that makes use of the teleomunication between the train and track equipment for the traffic management and infrastructure control. By means of the CBTC systems, the exact position of a train is known more accurately than with the traditional signaling systems. This results in a more efficient and safe way to manage the railway traffic.
Danger Area	DA	A Danger Area (DA) is an Utilization Permission (UP) on an overlapping free but not necessarily connected set of Edge Sections. A DA can temporarily change the Utilization Conditions (UC) of this area. A Danger Area represents e.g. a construction site, a speed restriction, or an unmonitored area.
ETCS - On Board Unit	ETCS-OBU	The on board unit is the part of the ETCS equipment which is responsible for the safe ETCS supervision of the engine.
ETCS Interlocking	EI	ETCS cab-signalling based interlocking comprising the Radio Block Center (RBC). Its dynamic, rule based and geometric safety logic controls all movements of the objects and all changes of the state of the Trackside Assets (TA) within the EIs effective range. All operational logic is moved to the higher-level systems.
GLAT	GLAT	German Acronym "Genau Lokalisierbare sichere und Allgemeinverwendbare EndgeräteTechnik" translates to "exactly locatable safe all purpose end device technology". Official English translation to achieve acronym consistency: Generic Location Aware Toolbox. Example usages of GLAT: Locate people close to / on the track, locate the trailing end of a train.
Guided Movable Object		A guided moveable object within the smartrail 4.0 terminology is any rolling stock, guided by rails. (guided) MOBs have a Movement Permission (MP). The opposite are non-guided movable objects, which can not be controlled by an interlocking and therefore are associated with a Danger Area (DA) instead of a MP.
Infrastructure Manager	IM	An authority responsible in particular for establishing, managing and maintaining railway infrastructure, including traffic management and control-command and signalling. (Oftentimes the owner of the railway infrastructure as well).
Infrastructure Object	IO	An Infrastructure Object represents a track side asset in the Object Controller (OC). Examples: a point, a level crossing, a track segment, a signal
Infrastructure Object Element	IOE	Item which represents a part of the infrastructure object. Can be a node, edge, vector, edge transition or any other topo based item.
Infrastructure Object Element State	IOES	Infrastructure Object Element State is a generic term for the state of an Infrastructure Object Element. States of an IOE may be e.g. of the specific type DPL (drive protection level).
Moveable Object	MOB	A Moveable Object (MOB) is a representation of a real movable object (TO or NTO) in the Operating State. Any real movable object which is detected as such by a person or system with safety responsibility will be represented as a MOB in the Operating State.
Movement Permission	MP	A Movement Permission is an authorization for a track bound Moveable Object (MOB) to move in a defined direction, along a defined path on the track network. A Movement Permission includes all

		conditions under which the movement of the MOB can be performed safely. A Movement Permission always refers to exactly one MOB.
Object Controller	OC	The Object Controller connects the ETCS Interlocking (EI) with the trackside assets (TA) by translating Commands/Messages between ETCS Interlocking and trackside asset (e.g. point motor).
Object Identification	OI	The Object Identification is a functionality of EI Object Aggregation. It merges all status information on Movable Objects and Infrastructure Objects from different channels into one consistent Operating State.
Object Manager	OM	The Object Manager is a part of the IL and provides the current operating state for all consumers of EI.
Object Manager Element	OME	OMEs are virtual elements in EI's operating state, which represent the functionality of infrastructure objects. IOEs (but not just IOEs) are represented by OMEs.
Object Manager Element State	OMES	State of an Object Manager Element
Operating State		The Operating State is the representation of all relevant objects known to the EI, including their state. It is the only true representation of all safety critical objects and their states.
Radio Block Center	RBC	Trackside safety unit used in ETCS level 2 and 3 applications. Generates the Movement Authority from dynamic and static data.
Safe Topology		Topology data that are proven to be error free with respect to safety. This means that the data should be as error-free as possible, and if errors in the data occur, they fall to the safe side and are safely disclosed.
Safety Actor	SA	A safety-actor is, depending on the configuration, responsible for defining and/or modifying utilization conditions, as well as verifying the compliance of topology utilizations (and utilization requests) to those conditions. Example of safety actors: ETCS Interlocking, human operator with the appropriate role, other authorised systems.
Safety Logic	SL	A safety function that checks all requests in regard to safety and feasibility. It rejects any request that does not meet all predefined criteria.
Safety Responsibility	SR	Safety Responsibility is the obligation to monitor and enforce a specific behaviour of a system.
TopoHandler	TH	TopoHandler supervises the topology update process for all components that need safety relevant topology data.
Traffic Management System	TMS	The production systems for planning, scheduling, disposition which control (CCS)- and (ATO) Systems.
Utilization Condition	UC	An Utilization Condition sets the conditions under which an Utilization Permission (UP) can be created/conceded and to which conditions it must comply to during its existence. See also: SOCUR. Examples of UCs are max. point speed, allowed driving direction, allowed train type.
Utilization Permission	UP	A Utilization Permission (UP) is a permission to utilize a geometric area of the track network topology under defined Utilization Conditions (UC).

3 Scope of the document

This document is a refinement to the documents SRP-2658 - Kerndokumente des Gesamtkonzeptes SR40 and describes the ETCS interlocking in a general way.

This document describes the functionalities and basic concepts of the ETCS Interlocking and shows how a high safety level can be achieved.

The document does not deal with migration and its financing or with systems/applications connected to the ETCS interlocking (e.g. ETCS).

It also does not deal with authorization and homologation questions.

4 Summary

The ETCS interlocking (EI) is a core element of the smartrail 4.0 system. It will be used in combination with a high-level Traffic Management System (TMS), which is able to plan and control the traffic in real time and in every detail. The ETCS interlocking will replace the legacy interlocking but not all line side installations like points and level crossings. These elements will be controlled by so called object controllers which in turn are controlled by the ETCS interlocking.

The following picture shows the schematic description of the smartrail 4.0 system and the context of the ETCS interlocking. The Traffic Managament System is responsible for planning and steering the entire network traffic. It sends requests for movement executions or line side installation state changes (e.g. position of a point) to the ETCS interlocking. The ETCS interlocking itself checks if the request can be executed safely and sends a demand to the appropriate controller. The controller on the one hand delegates the execution to the object and on the other hand provides information of the objects state to the ETCS interlocking. The ETCS Interlocking stores all object states, localization and topology information and makes it available to the respective consumers (e.g. to Traffic Management System) via the "operating state".

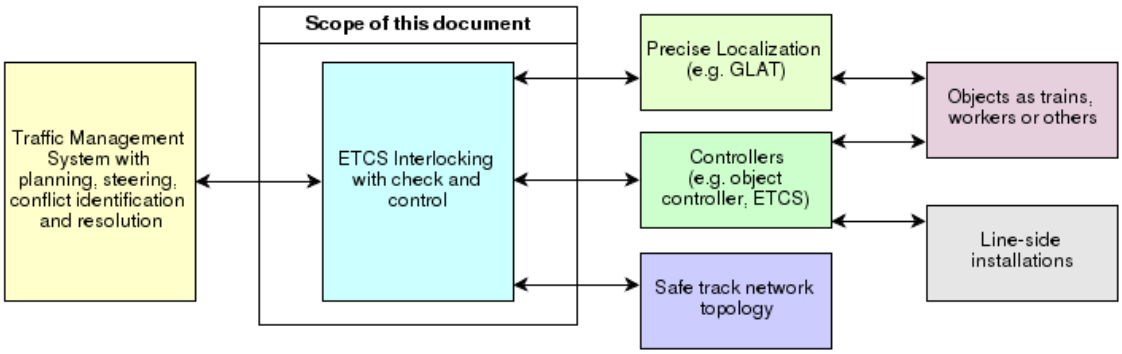


Figure 1 : Schematic description of the smartrail 4.0 system. The scope of this document is the ETCS interlocking.

ETCS interlocking functions

The ETCS interlocking is not only responsible for safe execution of movements or object state changes. Following is a list of all main functions including a short description:

Verification of safe movements or object state changes

As described above the ETCS interlocking verifies if the requested movement (e.g. train movement) or object state change (e.g. throw the points) is safe. This means that the ETCS interlocking checks that there will not be a collision and that the object is not occupied by another movement.

Demand of infrastructure asset state changes (e.g. points)

The ETCS interlocking is the only application allowed to demand a state change of an object (e.g. level crossing). After the safety check of the requested state change (sent e.g. by the Traffic Management System) the ETCS interlocking demands the state change from the corresponding object via the object controller.

Demand of object movements

After checking that the requested object movement is safe, the ETCS interlocking sends a demand to the appropriate controller (e.g. to the ETCS RBC).

Make available the operating state

The operating state is the "heart" of the whole system. All current states (e.g. moving objects) and demanded state changes are stored in it. The object aggregation (is part of the ETCS interlocking) deduces the state of the real objects from the information it collects from all the objects (e.g.trains, points, etc.) and stores these states in the operating state.

Safeguard

The ETCS interlocking monitors all operations on the network through the operating state. If the ETCS interlocking detects a violation of the safety rules, it triggers a measure to minimize the risk (e.g. emergency brake, warning). Following are two examples, there will be other risk minimizing measures.

Demand of emergency stop

The ETCS interlocking may demand emergency stops if a violation of a safety rule is detected (e.g. train runs over the limit of permission).

Demand of warning

The ETCS interlocking may demand a warning if an object violates a safety rule (e.g. worker is too close to a train movement).

The ETCS Interlocking explicitly ensures only safety of movements, but does not consider any operational implications (e.g. does this movement lead to a congestion). This deliberate design decision enforces a strict separation of concerns which provides several benefits, like separate lifecycles of the business logic and the safety logic, thus enabling fast, innovative and cheap improvements of the business logic and reduced development and maintenance costs for the ETCS interlocking.

Basic Conditions

To ensure safe movements, the following three basic conditions must be met.

1. Topology sections are exclusively reserved and locked for a specific movement
2. Movements occur only within the reserved topology section
3. Reserved topology sections may not overlap, or may do so only under defined conditions

Furthermore, the goal for the ETCS interlocking is to be able to safely allow as many concurrent operational movements as possible and thus guarantee the highest possible capacity.

Basic Concepts

Basic concepts have been developed to satisfy the basic conditions. In the following the most important basic concepts are described:

Utilization Permission

A utilization permission is a permission to utilize a geometric area of the network topology under defined utilization conditions. There are two types, **Movement Permission** and **Danger Area**.

Movement Permission

A movement permission is an authorization to move in a specific direction for a specific distance according to a given speed profile. The movement permission is requested by the traffic management system and verified by the ETCS interlocking. Out of this movement permission a demand for a movement is sent to the moving object (e.g. Movement Authority in ETCS application). A movement object must stay inside its movement permission at all times. Movement permissions may overlap under certain conditions (e.g. joining).

Danger Area

It is possible to set a danger area over a certain part of topology (e.g. track segment). A danger area request is typically submitted due to an exceptional situation (e.g. landslide, maintenance work, etc.). This request may be submitted by the traffic management system but also by the ETCS interlocking safety manager application (Watch Dog). A danger area and a movement permission may overlap under certain conditions (e.g. construction vehicle must enter in a construction site).

Utilization Condition

A utilization condition defines how a certain geometric area may be used (e.g. maximum speed, allowed driving direction, allowed train type).

Safe Distance

The safe distance between two consecutive utilization permissions is needed for safety reasons. To ensure these safe distances, **Risk Buffers** will be set at the boundary of the utilization permissions (e.g. movement permission).

Safety Actor

The safety concept defines that all safety critical state changes need a supervisor who is responsible for the safe execution of the state change at all times: this supervisor is called **Safety Actor**. The Safety Actor (a system or a human being) that ensures that the **Safety Responsibility** is never violated must have certain capabilities to do so. The ETCS interlocking is responsible to verify and to monitor if the **Safety Responsibilities** and their **Safety Actor** match and in case of a violation to take corrective action.

Example: A train driver cannot ensure that no collisions will occur for a train running at 200 km/h. In this case only a technical system (e.g. ETCS) may take over the role as Safety Actor. The ETCS Interlocking ensures for example that no train driver is handed over the responsobility to prevent collisions if the train is running at such a speed.

The functionalities together with the basic concepts allow the realization of the basic conditions and the execution and monitoring of safe operations within a traffic network.

5 Premises and requirements

5.1 Premises

Safe Topology

To control and monitor all movable objects and relevant line side installations of the traffic network safely, safe topology data are needed. Since the ETCS Interlocking makes all safety checks based on the operating state, the operating state must be safe. This requires that a safe topology must be present.

Traffic Management System (TMS)

The ETCS Interlocking is a passive system except for safety monitoring (Watch Dog). The ETCS Interlocking only checks if a movement or line side installation state change (e.g. point) must be executed if an other system sends a request to do so. Therefore a traffic management system is needed being able to request movements and line side installation state changes.

CBTC System

The ETCS interlocking presupposes a Communications-based train control (CBTC) system (e.g. ETCS L3) which does not need line side signaling system anymore. However, there still will be the possibility to use line side signaling systems to control simple movements (e.g. shunting).

Object Controllers

The line side installation system (e.g. switch) must be able to interpret the demands coming from the ETCS Interlocking and be able to send back information about the state of it. Therefore, object controllers must be developed, able to receive and send appropriate information.

CBTC System controller

The CBTC System controller (e.g. ETCS RBC) must be able to translate ETCS Interlocking movement demands into specific system information (e.g. ETCS Movement Authority). It also has to translate movable object information (e.g. position report) into information which can be interpreted by the ETCS interlocking.

5.2 Requirements

The requirements of the ETCS interlocking are defined in SR40 Preliminary Customer Requirements. Besides those requirements, the following ETCS interlocking targets have to be reached.

5.2.1 General requirements

Support of localisation systems

The ETCS Interlocking (EI) shall support different localisation systems. It shall be able to deal with conventional clear track signaling systems (e.g. axle counters) but also with not yet developed position systems. These may be satellite and/or inertial-based systems or fibre optic sensing, among other technologies.

Support of different CBTC Systems

The EI is designed for use in CBTC-type environments (e.g. ETCS). It assumes a continuous connection to the train.

Safety

The safety logic of the EI supports the usage of various technologies and architectures (e.g. GLAT) with the aim to minimize the transfer of the safety responsibility to a human operator. Since it is therefore assumed that the transfer of the safety responsibility to a human operator or to a third-party system must be possible and configurable.

Topology

The safe control of track utilization shall be possible for any topology that is compliant with EI topology (any topology built according to the rules for EI topology). This shall always be achieved with the same high (parameterizable) safety level. This also includes the safe control, at any time, of any existing trackside asset.

Applicability

A broad applicability to different railways and in various types of traffic and operational processes shall be possible. The requirement of a "operational process independent safety" means that any manoeuver that contradicts the parameterized safety requirement shall be prevented at any given location, given the full localization and direct (online) control connection.

Scalability

The functional architecture of the EI shall not prohibit a high degree of scalability (up to the use in large data centres) and the dynamically adaptive performance of control and monitoring. This requires high degrees of versatility in the processing of the information flows:

a. Control and monitoring of a variable quantity of fixed-installations (infrastructure assets or moveable objects)
b. Connection of different types of fixed-installations in different combinations (for regional transport, metros, secondary lines with very favourable technology, up to main lines equipped for very dense traffic). These combinations can also vary along a single track.
c. Control and monitoring of moveable objects (trains, people, obstacles) with technical equipment (sensors, actors, operating surfaces) in various levels of accuracy.
d. Control of moveable objects under degraded modes (e.g. impaired systems or trains), which may occur also in combination. These must enable a production that is still safe and as efficient as possible within the given restrictions.

Safe production

EI enables a generic homologation ("Plangenehmigungsverfahren") with respect to the safety-relevant tests. This means that the functional design of the EI should enable a safe production during the period of construction (commissioning of the EI segment of the topology), provided that a precise and safe recording of the topology and its functionality is always available.

Costs

Due to constant increase in project costs for building interlocking systems, the functional scope of the EI is reduced to the essential minimum. All non-safety-related functionalities shall be relocated to other architectural levels (e.g. traffic management system).

5.2.2 Functional Requirements

From the functional point of view, the EI outlines the complete infrastructure-based functional scope required for guaranteeing safety of the movements on a track. EI therefore combines (integrates) e.g. a part of today's interlocking and Radio Block Centre functions, whereby only the minimum necessary functional scope is assumed, namely, only the scope which is necessary for safeguarding all movements. All other functions are assigned to other higher-level traffic management systems (TMS).

EI features include only the minimum functional scope necessary to:

a. verify the safety of higher-level commands to track users or infrastructure installations prior to their execution.
b. monitor track users or infrastructure assets, and, if necessary, implement safety measures so that they do not interfere with each other beyond a defined degree.

Extension of the monitoring range

Current interlocking systems regard only a few safety aspects such as speed, overlapping-free movement and “safely closed” path for the movements along the track. However, from a feasibility and cost-effectiveness point of view, it is necessary to investigate whether the range of objects for safety monitoring can be extended. This relates to all conceivable safety-relevant route and track-related user properties that can be checked, (hereinafter referred to as “extended safety aspects”), e.g.

a. structure gauges
b. hazardous goods
c. monitoring hazards measured by train control units
d. untypical temporary braking behaviour, hot-box
e. excessive axle loads or transverse forces

Not included in the EI are the safety functions of object controllers (OC) and localization systems, e.g.

a. the safe recording of system conditions
b. the setting of system conditions with a secure fault release
c. the detection of the position of moveable objects and the position accuracy

Various configurations

EI can be deployed in various configurations. However, it can only provide a safety function if these configurations meet the following criteria:

a. The topology is a true image of the real physical infrastructure
b. The localization architecture (not part of EI), which is made available to the EI object recognition, enables the localization of all moveable objects (track occupation) from a data availability and completeness point of view.
c. The command architecture (not part of EI, e.g. vehicle equipment or mobile devices for human operators) provided to EI Command can bring any moveable object to a safe state or warn it at any time, either by means of an EI command or otherwise through an autonomous reaction (EI safety monitor) e.g. emergency breaking, warning (for non-rail-guided moveable objects).

5.2.3 Requirements for the application conditions

Minimum of exported application

It is required that each function, which may later be used as an isolated partial product (for example, the object recognition), only defines a minimal set of requirements for its communication partners in the information flow. In other words, the number of exported application conditions must be limited to the minimum and essential extent, with which a correct use of the function can still be achieved. For this requirement, terms such as “functional robustness” or “functional adaptability” are commonly used.

Upward compatibility

Upward compatibility to new technologies must be ensured. In the future it is to be expected that more precise and detailed information will be available (e.g. for the positioning of movable objects). This information may be redundant, come from different sources and offer different levels of accuracy and granularity. The functions must therefore be modelled in such a way that they can take advantage of such redundancy as much as possible, e.g. to increase/decrease the precision or reliability of their outputs. The term “functional evaluation capability” is used for this requirement.

Rule-based information processing

The intended broad applicability – specifically, the process-independence and the flexibility with respect to safety regulations - leads to a further requirement: the “high functional parameterization” i.e. data configuration instead of software change. In this implementation, rule-based information processing shall be used (e.g. object recognition with changing hardware equipment), whereby rules are not to be described in the software, but in configuration data, which can be incrementally certified. Hazard patterns shall be described by individually certified configuration data. This leads to configurable safe reactions, which in turn can be configured as a certified pattern. The interplay of several actors with the same function at the same point in the network must be described in the configuration via configurable certified distribution patterns (e.g. an old automatic train protection device and an ETCS on-board unit, which monitors a train at one particular location). The appropriate modelling of the configuration data and their secured lifecycle is therefore another requirement for functional modelling.

6 Design process for the EI

Process and system independence

The *process and system independence* is paramount for the EI. This means that the EI always controls the safe utilization of a track, regardless of how the topology is built, provided only that the control has not been transferred or assigned to some other safety actor (e.g. localization and control of the route users, i.e. “moveable objects"). For a safe track utilization under EI control, there should be (nearly) no need to export safety requirements, safety-related use constraints, processes or layouts of trackside assets. This is meant to allow the use of new technologies, which may cover, replace or even extend current operational processes, without the need to redesign the EI (upward compatibility).

Current design process

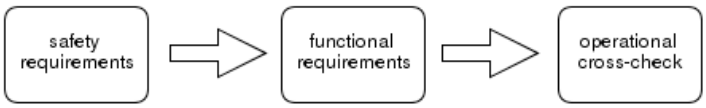
The usual design process for safety systems is the *bottom-up* approach. This means that detailed functional processes are derived from a list of all operational scenarios and sequences, and then aggregated to form the entire system. This traditional approach involves several risks. The derived examples are often too specific for a particular scenario. They can easily lead to isolated solutions, that cannot be transferred to other subsequent applications (lack of parameterization). For example, the “optimal” solution for a process X might not be necessarily extendable to other processes. If a very similar process Y has to be addressed, a new solution must be developed. Additionally, it generates also the risk of incompleteness, which leads to the need of frequent updates for each specific solution. This traditional design process follows the subsequent basic procedure (“waterfall” approach):

operational application -> safety requirements -> functional requirement

The safety requirements fulfil the overall safety objective

Design process for EI

In this document, an attempt is made to derive the safe control of movements following a *top-down* approach (deductive generic analysis). A high degree of abstraction is thus introduced and operational process examples are only used for cross-check purposes. This approach shall allow an easy extension of the ETCS interlocking when new functionalities or applications are requested.



The safety requirements fulfil the overall safety objective

The operational cross-check is thus not the first, but the last step in the design process. For the cross-check of the logic presented in this functional concept (FC) a simulator using many different process examples shall be built.

Technical terms

Furthermore, for higher abstraction, currently used technical terms which inevitably trigger fixed associations are avoided. Traditional distinctions (such as between shunting movement and train movement) are also avoided, since they present only slight differences for the parametrization of the safety control.

7 Domain Overview

The ETCS interlocking (EI) System can be divided into different functional topics or application domains. The following overview shows the main application domains and the basic data flow of how they interact.

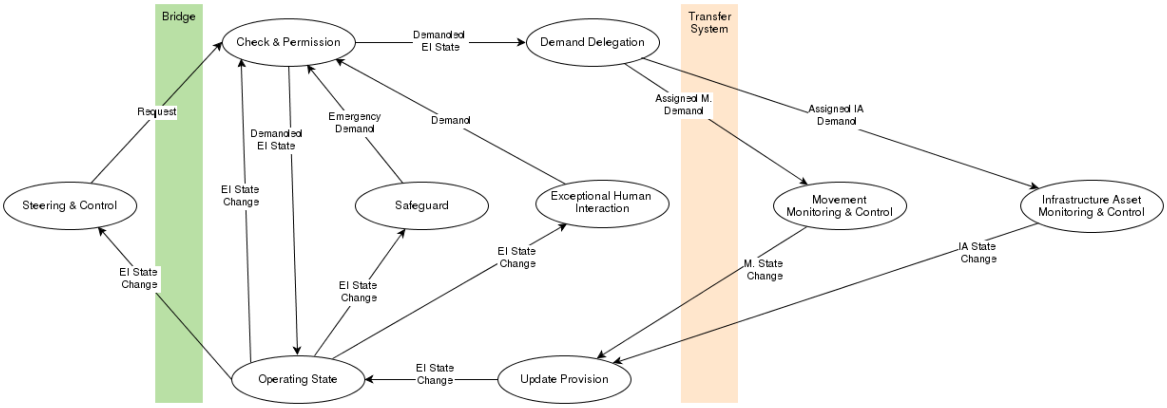


Figure 2 Application domains overview

7.1 Main barriers

7.1.1 Bridge

The *Bridge* stands between the safety relevant and the non safety relevant parts of the system and ensures that the non safety relevant parts don't impede the safety relevant parts.

7.1.2 Transfer System

The *Transfer System* connects the system parts running in the data center with the remote systems running close to the physical devices. These remote systems can be devided into unmoveable objects (trackside assets, etc.) and movable objects (trains, etc.)

7.2 Main application domains

7.2.1 Steering & Control

Purpose:

The purpose of the application domain (AD) **Steering & Control** is to steer and control planned train movements. Based on a representation of the current overall EI operating state it generates requests for train movements, which are evaluated after a variety of conditions in the receiving AD.

Received Communication:

- The AD **Steering & Control** receives "EI State Change" from the AD **Operating State**
- This received interface is defined in it's generating AD

Transmitted Communication:

- The AD **Steering & Control** sends "Requests" to the AD **Check & Permission**
- The "Requests" can contain:
  - Intention to change the state of an infrastructure asset
  - Intention to change the state of a train movement
  - etc

7.2.2 Check & Permission

Purpose:

The purpose of the application domain (AD) **Check & Permission** is to check incoming requests for reasonability, feasibility and safety violations. If the request was proved to be reasonable, feasible and safe, it will be granted. If any of these conditions does not apply, the request will be rejected.

Received Communication:

- The AD **Check & Permission** receives "Request" from the AD **Steering & Control**
- The AD **Check & Permission** receives "EI State Change" from the AD **Operating State**
- The AD **Check & Permission** receives "Emergency Demand" from the AD **Safeguard**
- The AD **Check & Permission** receives "Demand" from the AD **Human Interaction**
- These received interfaces are defined in their generating ADs

Transmitted Communication:

- The AD **Check & Permission** sends "Demanded EI State" to the AD **Demand Delegation**
- The "Demanded EI state" can contain:
  - Permitted state change of an infrastructure asset
  - Permitted state change of a train movement
  - etc

7.2.3 Demand Delegation

Purpose:

The application domain (AD) **Demand Delegation** is responsible for delegating the permitted demands to the correct Monitoring & Control AD. This means that this domains connects the generic safety logic to the specific devices of the real world.

Received Communication:

- The AD **Demand Delegation** receives "Demanded EI State" from the AD **Check & Permission**
- This received interface is defined in it's generating AD

Transmitted Communication:

- The AD **Demand Delegation** sends "Assigned IA Demand" to the AD **Infrastructure Asset Monitoring & Control**
- The "Assigned IA Demand" can contain:
  - Assigned state change of a infrastructure asset
  - etc
- The AD **Demand Delegation** sends "Assigned M. Demand" to the AD **Movement Monitoring & Control**
  The "Assigned M. Demand" can contain:
  - Assigned state change of a train movement
  - etc

7.2.4 Update Provision

Purpose:

The application domain (AD) **Update Provision** is responsible for processing and integrating information updates from the Monitoring & Control ADs.
Many single pieces of information are merged with their matching counterparts to create a more reliable and complete picture of the real world, which is then transmitted to receiving ADs.

Received Communication:

- The AD **Update Provision** receives "M. State Change" from the AD **Movement Monitoring & Control**
- The AD **Update Provision** receives "IA State Change" from the AD **Infrastructure Asset Monitoring & Control**
- These received interfaces are defined in their generating ADs

Transmitted Communication:

- The AD **Update Provision** sends "EI State Change" to the AD **Operating State**
- The "EI State Change" can contain:
  - Updated state change of an infrastructure asset
  - Updated state change of a train movement
  - etc

7.2.5 Infrastructure Asset Monitoring & Control

Purpose:

The application domain (AD) **Infrastructure Asset Monitoring & Control** is responsible to update and change the state of infrastructure assets (e.g. railway crossing gates). It processes the received demands to change the state and sends an update of the state.

Received Communication:

- The AD **Infrastructure Asset Monitoring & Control** receives "Assigned IA Demand" from the AD **Demand Delegation**
- This received interface is defined in it's generating AD

Transmitted Communication:

- The AD **Infrastructure Asset Monitoring & Control** sends "IA State Change" to the AD **Update Provision**
- The "IA State Change" can contain:
  - Updated state change of an infrastructure asset
  - Installation and registration of a new infrastructure asset
  - etc

7.2.6 Movement Monitoring & Control

Purpose:

The application domain (AD) **Movement Monitoring & Control** monitors and controls the execution of a controlled movement of a trackbound object. This ensures that the movement happens in a safe and reliable manner.

Received Communication:

- The AD **Infrastructure Asset Monitoring & Control** receives "Assigned M. Demand" from the AD **Demand Delegation**
- This received interface is defined in it's generating AD

Transmitted Communication:

- The AD **Infrastructure Asset Monitoring & Control** sends "M. State Change" to the AD **Update Provision**
- The "M. State Change" can contain:
  - Updated state change of a train movement
  - etc

7.2.7 Operating State

Purpose:
The application domain (AD) **Operating State** stores the current operating state and represents the single source of truth regarding the operating state.

Received Communication:

- The AD **Operating State** receives "EI State Change" from the AD **Update Provision**
- The AD **Operating State** receives "Demanded EI State" from the AD **Check & Permission**
- These received interfaces are defined in their generating ADs

Transmitted Communication:

- The AD **Operating State** sends "EI State Change" to the ADs **Steering & Control, Check & Permission, Safeguard and Human Interaction**
- The "EI State Change" can contain:
  - Updated state change of an infrastructure asset
  - Updated state change of a movable object
  - Updated movement permissions and danger areas
  - etc

7.2.8 Safeguard

Purpose:
The application domain (AD) **Safeguard** ensures that all safety states of all objects in the operating state are safe. Both current and emerging hazards are evaluated. If an unsafe safety state is found, an emergency safety reaction is executed.

Received Communication:

- The AD **Safeguard** receives "EI State Change" from the AD **Operating State**
- This received interface is defined in it's generating AD

Transmitted Communication:

- The AD **Safeguard** sends "Emergency Demand" to the AD **Check & Permission**
- The "Emergency Demand" can contain:
  - Emergency stop of a movable object
  - state change of an infrastructure asset
  - etc

7.2.9 Exceptional Human Interaction

Purpose:

The application domain (AD) **Exceptional Human interaction** is responsible for providing an interface for all exceptional, yet safety relevant interactions performed by humans. This includes visualizing the operating state and capturing the user input as demands.

There might be other human interfaces provided by other systems, e.g. Steering & Control, that even might interact with the interlocking. But these interfaces are not safe and can only send requests, not demands.

Received Communication:

- The AD **Exceptional Human Interaction** receives "EI State Change" from the AD **Operarting State**
- This received interface is defined in it's generating AD

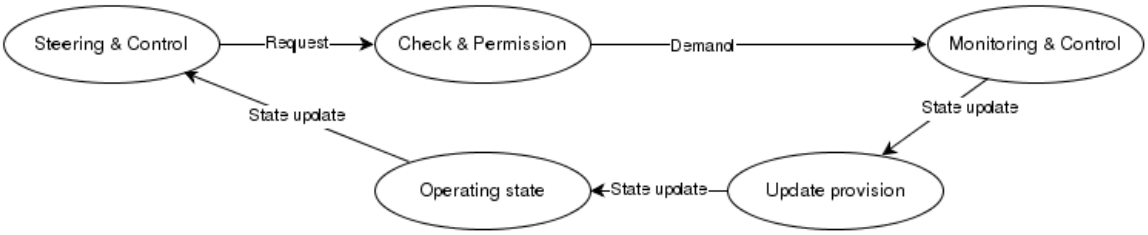
Transmitted Communication:

- The AD **Exceptional Human Interaction** sends "Demand" to the AD **Check & Permission**
- The "Demand" can contain:
  - Movement permissions in exceptional situations, e.g. construction site
  - Changes to the infrastructure, e.g. changes to the configuration of infrastructure assets
  - etc

7.3 Generic data flow and processes

7.3.1 Processing of requests

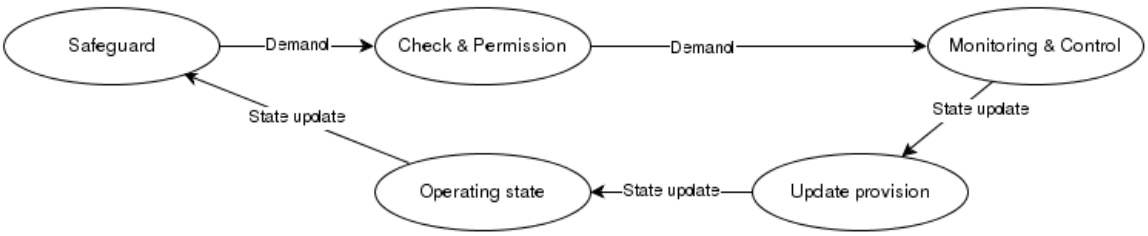
The main data flow and processing pipeline is as follows:



Any request is checked for safety concerns. This check is based on the current operating state and the defined safety rules. Once a request is permitted, it turns into a demand and is transmitted to the physical device for execution. The execution is constantly monitored and controlled. Any state changes are published by the device to the update provision where they are processed and if necessary aggregated to produce a consistent operating state.

7.3.2 Safeguard

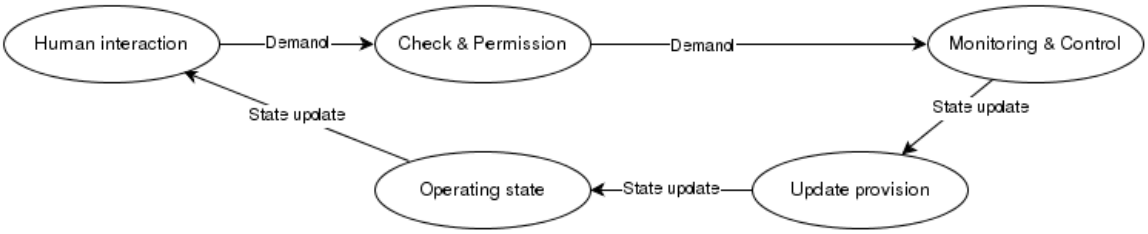
The operating state is constantly monitored for safety concerns.



As soon as a safety concern is detected, an emergency safety reaction is performed which results in demands being sent to the domain *Check & Permission* to enter the main processing pipeline.

7.3.3 Human interaction

Despite a high level of automation, there remain certain processes that need human interaction.



who belongs to the human interactors (where are they in physical reality), Display includes operating state and a demand

8 Basic conditions to ensure safe movements

8.1 Overview

Overview basic conditions

To ensure safe movements, the following conditions must be met.

1. Topology sections are exclusively reserved and locked for a specific movement
2. Movements occur only within the reserved topology section
3. Reserved topology sections may not overlap, or may do so only under defined conditions

The following diagram visualizes the basic conditions.

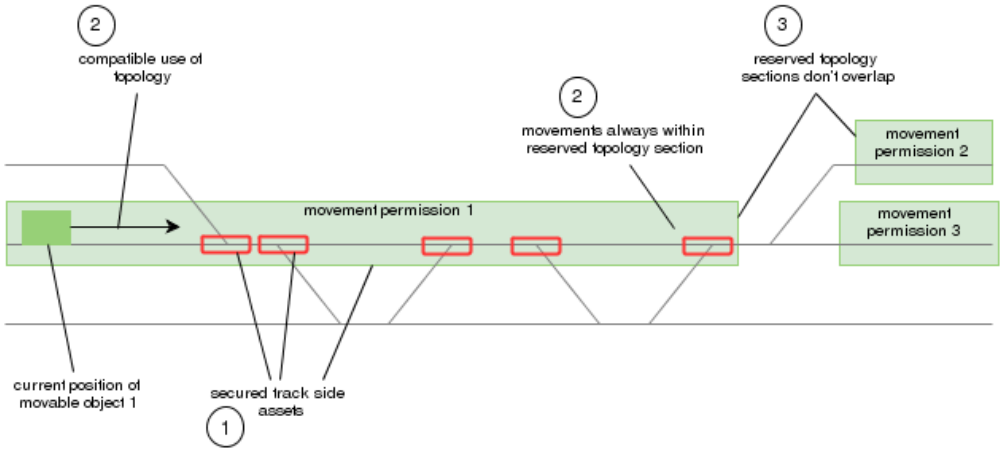


Figure 3 Visualization of the basic conditions for the EI application

The outlined basic conditions are explained in more detail in the following chapters.

Requirements common to all conditions

The following requirements are common to all outlined conditions:

- Error-free detection and identification of movable objects, their properties, capabilities and states
- Error-free network topology, including its properties, capabilities and states
    - Delivery of error-free infrastructure asset states or of a fail safe state

The EI provides an operating state that is based on the topology and is constantly kept up-to-date to reflect the current state of the infrastructure assets, movable objects and demanded state changes.

The topology is represented using a node-edge model. The granularity, as well as the capabilities, properties and states are derived from the infrastructure assets of which the topology consists.

All moving objects, utilization permissions and reserved topology sections are mapped to the topology and are part of the operating state.

The EI relies on safe monitoring devices to know the current state of the infrastructure assets and movable objects.

8.2 Topology sections are exclusively reserved and locked for a specific movement

A topology section must be secured and locked by the EI; the underlying infrastructure assets can never change their state during a movement (switch position, level-crossing barriers, etc.)

The implementation of this basic condition requires:

- Ensuring that an infrastructure asset state can be changed only if the EI has previously allowed that change
- Check any requested change of an infrastructure asset state for safety violations
    - Prevention of any change of an infrastructure asset state within the range of a movement permission (*logical closure*)
- Continuously monitoring the infrastructure asset states and triggering safety reactions in the event of any safety violations

8.2.1 Ensuring that an infrastructure asset state can be changed only if the EI has previously allowed that change

As shown in the summary, the ETCS interlocking delegates the execution of a demand to dedicated controllers. The system architecture ensures, with the corresponding protocols and technologies, that at all times only one source can send demands to the controllers and that at all times the current source is unambiguously known.

8.2.2 Check any requested change of an infrastructure asset state for safety violations

Following is an outline of the checks that are applied to any request to change the state of an infrastructure asset:

1. Is the requested infrastructure asset controllable?
2. Is the requested infrastructure asset part of a reserved topology section?
    a. Does the requested infrastructure asset state change cause a safety violation for any of the utilization conditions of the reserved topology section?
3. Lies the requested infrastructure asset within the saferty distance of a reserved topology section and is the resulting safety distance still safe?

These checks ensure that within the range of a movement permission, no state change can be performed which would conflict with the infrastructure asset states required for that movement permission. Infrastructure asset state changes that do not affect the safe implementation of the movement permission (e.g. information displays or warning systems) are excluded from this condition.

8.2.3 Continuously monitoring the infrastructure asset states

EI ensures the continuous detection and the correct mapping of infrastructure asset states and continuously checks the states for safety violations. The monitoring of infrastructure asset states for safety violations and the performance of safety reactions in case of a violation are described in further detail in Concept EI SM.

8.3 Movements occur only within reserved topology section

Movable objects do not move without a movement permission and never violate their movement permission. The utilization conditions of the movement permission do not violate any utilization conditions of the topology or any of the movable objects capabilities (e.g. maximum speeds, lateral forces, structure gauge, etc.).

The implementation of this basic condition requires:

- Ensuring that a movable object can't move without a movement permission
- Checking any requested movement permission for safety concerns
- Check that the required infrastructure asset states comply with the requested movement permission before granting any movement permission
- Continuously monitoring the movable objects states and triggering safety reactions in the event of any safety violations

8.3.1 Ensuring that a movable object can't move without a movement permission

Every movable object is equipped with a CBTC-like onboard unit which allows to monitor and control any movement. Depending on the capabilities of the onboard unit, EI ensures that only operating modes are used that allow full control over the movable object.

8.3.2 Checking any requested movement permission for safety concerns

The following checks follow the same pattern and meet the same criteria as for setting up a movement permission in a conventional electronic interlocking. However, they include only the infrastructure assets that are required for a CBTC system:

1. A movement permission is always based on the safe EI topology and is always gap- and overlap-free
2. All train control elements (signalling or direct control) must be configured according to the movement permission.
3. All elements providing environment warning as well as influencing elements must be in a state conformable to the movement permission and shall have acknowledged their state (e.g. point in the right position).
4. No controllers within the range of the requested movement permission reports a hazard warning

8.3.3 Check that the required infrastructure asset states comply with the requested movement permission before granting any movement permission

The safety logic checks the states and properties of every infrastructure asset within the reserved topology of the requested movement permission for compliance with the utililization conditions of the requested movement permission.

8.3.4 Continuously monitoring the movable objects states and triggering safety reactions in the event of any safety violations.

The EI system ensures that the topology section occupied by a movable object coincides at all times with the movable objects assigned movement permission (movement authority (MA) in ETCS). Furthermore, a movable object can only move in compliance with the utilization conditions set by its movement permission e.g. speed, direction.

For non trackbound movable objects (e.g. rail workers, dumpers), only warning functions are possible, e.g. over handheld-devices. Since the movement of non trackbound movable objects cannot be controlled by a movement permission, it is protected by a danger area.

All movements of a movable objects are continuously monitored by the EI. In case of utilization violations or hazardous

situations, safety reactions are triggered (e.g. emergency stop for trackbound movable objects, warning for non trackbound movable objects).

Compliance with the condition that a movable object always moves only within its allocated topology section can be either assured by a train protection device (e.g. ETCS OBU) or by the EI. In the latter case, compliance with the basic condition would require safely locating the movable object, mapping its geo-coordinates to the track topology and determining whether the movable object lies within its movement permission. From the movable object control point of view, there is no need to locate the movable object within a movement permission if an onboard unit is active that monitors and controls the movement (e.g. ETCS L2 or L3 onboard unit). From the operation point of view, however, there is the need to locate the movable object in order to release the topology sections reserved for its corresponding movement permission and to be able to trigger any safety reactions in case of an emergency.

8.4 Reserved topology sections may not overlap

The distance between reserved topology sections is always large enough to eliminate the risk of accidentally entering the reserved topology section of an adjacent movement (slipping, escaped wagon, etc.). The length of the safety distance depends on the properties and states of the current movement permission and reserved topology section. Reserved topology sections may touch or overlap only under clearly defined rules.

The implementation of this basic condition requires:

- For every requested movement permission the safety distance is determined and checked for safety violations against the already permitted movement permissions
- Overlapping movement permissions are checked for compliance with the defined rules for overlap

8.4.1 For every requested movement permission the safety distance is determined and checked for safety violations against the already permitted movement permissions

Two rules may be applied to determine the (geographical) extent of a safety distance on the topology:

1. Extending the utilization permission in the direction of movement beyond the reserved topology section (comparable to slip distances today) i.e. the so-called **risk buffer**. Applying the rules for risk buffers is the default when checking safety distances.
2. Identifying *all* paths that lead from the requested utilization permission to any existing utilization permission i.e. the so-called **risk paths**. Risk paths are used when the length of the safety distance depends on specific properties of the two users, e.g. a movable object with dangerous goods demands a longer safety distance. If no other area is found within a parameterized geometric distance, the navigation to determine a risk path is aborted.

Determining the extent of a risk buffer or identifying a risk path includes navigating over the topology. Navigating over the topology always considers the current state (e.g. current navigability of an intersection in the topology) and the properties of the topology (e.g. some intersections can be forced to be navigable, independent of their current state) .

A safety distance is comprised of two main values, its length and its extent on the topology. For *risk buffers*, the length of the safety distance is calculated based on the properties of the user and the properties of the utilization permission. Then the extent on the topology is determined. For *risk paths*, first the paths are determined and then the length of the safety distance for every path is calculated, based on the properties of both users and both utilization permissions.
Depending on the rules applied, there can be several safety distances that apply to a utilization permission, each one with a different extent.

The requested utilization permission, including its determined risk buffers or risk paths, is checked for overlap with existing and secured utilization permissions and/or their risk buffers or risk paths.

9 Basic Concepts

9.1 Generic approach for the EI core

The core task of the ETCS interlocking, namely to ensure safety between moveable objects, also applies to other areas. For example, autonomous vehicles such as cars, trucks or drones could be monitored according to the same rules. The EI safety logic is therefore designed generically to support these applications.

These moveable objects could include but are not limited to:

- trains
- construction vehicles
- cars
- trucks
- trackable construction workers
- etc.

within the following (not yet complete) list of scenarios :

- passenger transportation
- cargo transportation
- etc.

The EI safety logic is a fundamental part of the EI core and uses a model which is independent of

- the used safety systems (train protection system)
- a specific topology
- connected trackside objects (signals, points, barriers, etc.)
- localisation technologies (track circuits, axle counters, train position reports, GLAT, etc.)
- and control systems (TMS, train control).

By using suitable parameterisation, the safety logic can be adapted to the corresponding application.

The following diagram illustrates how the generic EI core is linked to the technology-specific environment via protocols.

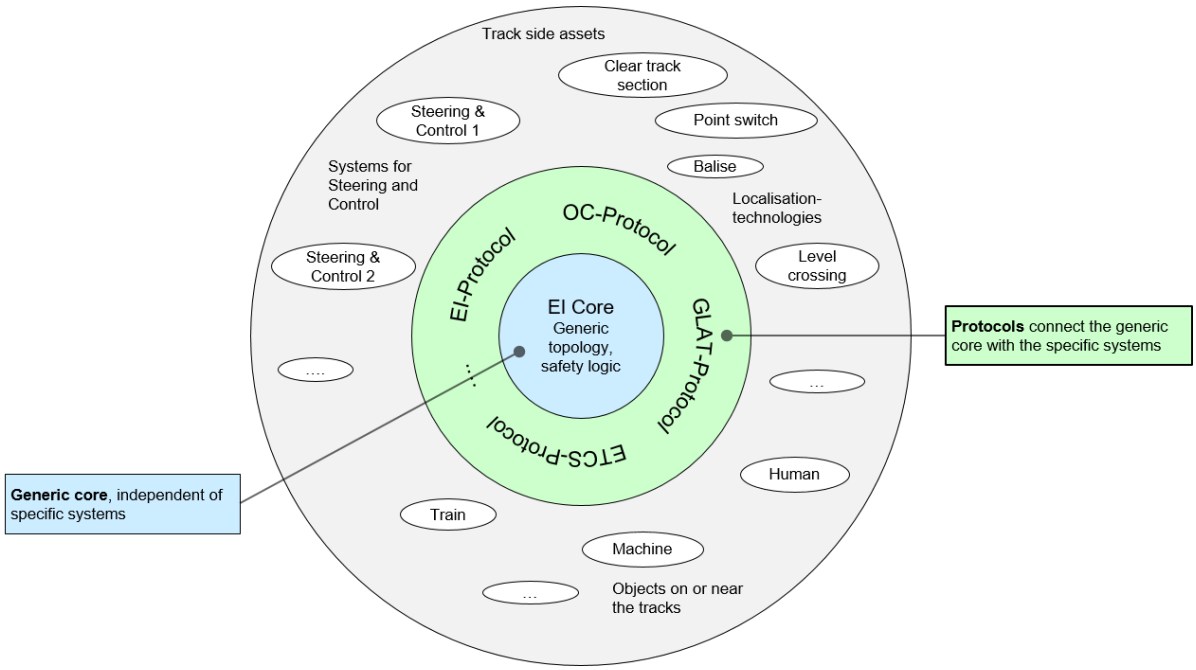


Figure 4 Generic approach of the ETCS interlocking

9.2 Safety Responsibility

Safety Responsibilities (SR) enable the ETCS interlocking to remain in a safe state at all times during its operation. This is achieved by Safety Actors (SA) being assigned to SR's. SR's may thus be seen as rules which must be fulfilled to keep EI in a safe state (e.g. stay within the maximum velocity in a movement permission). SA's will check the current state of the system based on their assigned SR's and will trigger corrective actions if the conditions specified by the SR's are not met. Corrective actions to be taken shall be specified in the SR.

SA's are enabled to check the current system state by SR's being associated to data objects represented in the operating state. Data objects represented in the operating state may be movable objects, infrastructure objects and SA's. SA's represented as data objects in the operating state can also have associated SR's. This will allow to create hierarchies of SA's where necessary. In case of failure of lower level SA's, higher level SA's will not provide a one to one fallback for the failed SA but will rather provide supervision and corrective action at their appropriate level.
Example: In ETCS full supervision (FS) mode an OBU is the assigned SA at the lower level to take the SR "Distance" and the Safety Manager (SM) is the assigned higher level SA which supervises the OBU (the OBU associated SR's are assigned to the SM). If SR "Distance" is not guaranteed, the OBU will take corrective action by braking the train. However if the OBU shows that braking action due to specific circumstances is insufficient to remain within risk distance the higher level SA Safety Manager (SM) may take corrective action by creating a Danger Area (DA) which safeguards a larger area around the moveable object (containing the OBU) indicating a problem.

In order to assign a SA to a SR the SA must provide specific capabilities. These capabilities are configurable such that they can be matched to the specific environment EI has to deal with. EI will allow assignment of SR's to SA's only when the capabilities provided by the SA match those required by the SR. This check will be performed during initial assignment but also when a SR handover is to be performed.

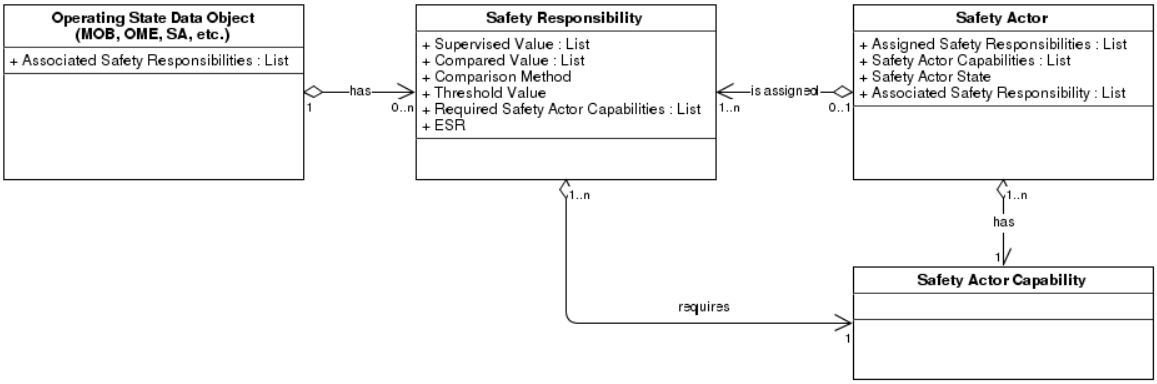


Figure 5 : Building blocks for the Safety Responsibility

Handovers of SR's may be performed on request. Requests may come from outside EI. A request will be checked to ensure the proposed new SA provides the correct capabilities. If this is assured a SA supervises the handover such that situations where SR's are unassigned or assigned to two SA's at the same time can be prevented.
Examples:

- *SR "Collision" handover from OBU to Driver*
- *SR C/P/S and location of OME is true from OC to an operator at the IOE location (e.g. override of a erroneously reported IOE state)*

9.3 Fundamental working principles of the EI

One of the essential requirements of the EI is the capability to guarantee safety in geographical areas while observing and monitoring the so-called utilization conditions. This chapter is intended to convey a conceptual approach without assigning the individual functions to the functional components. The latter can be found in 20 Konzept ES-IA Verfeinerung System Definition.

The EI is a *purely reactive system* and gets triggered by and reacts to

- requests from its users, which may be other systems or humans.
- any change to the operating state
- unexpected safety violations

The *evolution of time is not taken into account* by the EI when checking for safety violations. It only knows the current state and checks the request against this state. Any events that are planned and may happen in the future and that would make the current check to be accepted are not considered.

The EI does *not alter any requests*. If a safety check fails, the request is rejected, no matter how seemingly small the correction to make it acceptable would be. Most often a correction would not be possible anyway, because it takes time to change the operating state (points have to move, barriers have to close, etc.) and to track such a change would violate the fundamental working principle of not taking into account time evolution.

9.3.1 Movement permission

The concept requires that each and every movement of rail-guided MOBs occurs only via a corresponding MP. Movement of non rail-guided MOBs shall occur within a DA.
A **movement permission (MP)** is an authorization to move in a specific direction (the permitted direction is clearly defined and may also be "backwards and forwards") for a specific distance and according to a given speed profile. The speed profile considers the MOB's properties known by the interlocking as well as the speed profile for the specific track.

A MP comprises:

- a fixed, gap-free and limited topology segment, given as a list of all nodes and edge sections comprising the movement

permission path.

- a clear reference to one, and only one, specific MOB.
- a speed profile defining the maximum speed with which the MOB is allowed to move
  Note: This maximum speed may be the maximum speed permissible to remain in a safe envelope defined by the properties, capabilities and state of the TO and the claimed topology or a lower value speed profile defined by the system requesting the MP. In either case it will be ensured that the TO will not exceed the maximum speed defined in the MP.
- other IOE outside the movement permission path, such as the required protection IOE, including their required state (IOES).

A MP is requested by a system outside of EI. The EI will then verify the request and, if deemed safe, forward it to the MOB. The EI will lock in its Operating State the IOE's required to ensure the safe state of the MP. This action will ensure that any request intending to change a locked IOES will be rejected.
Note: The OC controlling the IOE will ensure that the IOES is maintained as long as there is no new demand. Should the OC fail to ensure this safety responsibility the corresponding emergency safety reaction will be triggered.

A MP can be modified (e.g. shortened, extended) by request. For example, a MP shortening would be requested when the MOB has finished its movement. A MP shortening would also be requested when the MOB has cleared parts of the movement permission path. A MP shortening is meant to release the MP's 'lock' on infrastructure object elements (IOE) so that they can be used for another train movement.

MPs may include permissions to move forwards and backwards.
Note: This may be used for shunting or service MOBs, which must travel a few meters forward and then a few meters backward for the catenary maintenance, without having to specify the exact distance and direction to be driven each time. In this case, the MP is used to ensure that infrastructure element states are not changed (points must not change position under the MOB). The movement permission (MP) shall only be modified after the work has been completed.

A MOB may also receive movement permission updates, which allow the continuation of the movement, in this case a MP extension. Movement permission updates are based on MP requests, such as from a TMS. A MP is transformed into the respective language of the applied train control technology (e.g. ETCS Movement Authorities) by the corresponding EI function.

Non rail-guided MOB are permitted to leave their danger area (DA). The DA can geometrically overlap another DA if the utilization conditions of the other DA are met by the overlapping part of the DA assigned to the MOB.

To ensure that a MP request is granted, any infrastructure element states that do not match the MPs conditions first have to be set to the necessary state by the requesting system (e.g. TMS). All utilization conditions that are not met have to be set to the right state or the MP corrected by the requesting system. The EI will only check the request against the current operating state, but never modify the MP, should any check fail.

Each MOB type (parameterizable), which is not permitted to move, is enclosed within a MP or a DA (or both), which has among its utilization conditions vmax = 0 km/h. If such a MOB type moves, EI would identify the movement as an infringement of the utilization conditions and trigger the relevant safety response.

9.3.2 Danger area

A **danger area (DA)** has the following characteristics:

- A DA has non-overlapping topology segments, but is not necessarily gap-free (e.g. DA for a construction site can be placed across a station entrance).
- A DA can restrict the use of a MP (yes/no, MOB type, speed), so that all utilization conditions can still be ensured by the EI.

The following may be considered as danger areas (DA): adjacent railway network topologies of other infrastructure

undertakers, industrial facilities, shunting and storage systems, barriers, construction sites.

- A DA may allow a geometric overlap of MPs, resulting in the delegation of the safety responsibility for some of the utilization conditions to another safety-actor.

For example, the person with safety responsibility for a construction site (safety-actor) can specify the utilization conditions for his/her site. If a TMS wants to issue a MP geometrically in this DA, the MP must comply with the utilization conditions of the DA for the overlapping section so that the EI can approve this overlap. A DA, as described in this example, thus represents a special authorization area. In principle, several MOBs can travel within a DA.

9.3.2.1 Differentiation between DA-request and DA-demand

A danger area (DA) can be created within the EI as a request from the TMS or as a demand from a safety actor. A request can be rejected by the EI. A DA request is typically submitted due to operational reasons; a DA demand, however, is necessarily due to an exceptional situation (e.g. landslide, maintenance work, etc.).

A DA demand is time-critical and shall be carried out immediately by the EI safety logic or by an external actor via the EI input & operation. A DA demand can overwrite the EI safety function and is always carried out by the EI (i.e. cannot be rejected).

Once a DA is created, it does not matter who created it. The creator does not automatically have the right to revoke or modify it. The utilization conditions of a DA determines which safety-actor can change or cancel it. However, this does not have to be the same actor that created it. This depends solely on the permissions of the safety-actor.

9.3.2.2 Removing or changing a danger area

If a DA is removed or changed, the safety is ensured by the requirement that only safety-actors with the appropriate authorization have the permission to perform this kind of operation.

For example, if a DA-change is necessary for the inspection of a track-side asset , the change can only be performed by a safety-actor on site and not by a remote safety-actor.

9.3.3 Overriding infrastructure asset states

A trackside asset, which is controlled by the EI via the object controller (OC), is used to form a topology movement permission path and/or to influence the movement of MOBs.

In general, it is the OC's duty to report the IOES. This also applies to faulty operations, where the OC shall report the degraded capability of the trackside asset according to the fault type (e.g. lower speed and instructions for driving on sight). Such cases require a new or modified utilization permission, if the degraded element is already part of an existing (= originally declared as safe) utilization permission. This should be automatically created by the EI Safety Monitor. Otherwise, the EI would simply continue working with the degraded element capabilities for new utilization permissions until the degradation is cleared by the OC (usually after being serviced by a maintenance worker).

However, in some situations this operation may not be sufficient from an efficiency point of view, in particular, during fault conditions with loss of connection to the OC and a known-to-be-false or very suspicious status message (e.g. sudden occupancy status report from a track circuit). In such cases, the EI will, if so configured, apply an extended functionality referred to as "overriding the infrastructure object element state".

1. If an OC reports an IOES that cannot be true (due to other information sources available to the EI, e.g. redundant localisation systems), the EI will then overwrite the internal display of the IOES in the operating state under predefined conditions. No automatic danger area will be created by EI in this case.
2. If an IOES is missing entirely, then the EI may, in some cases, be able to compensate the missing information procedurally/algorithmically. This compensation, however, must not automatically lead to new or modified utilisation permission. For example:

1. A typical functional case is the compensation for a failed or faulty track circuit. After the section has been automatically “cleared” by a MOB, the faulty section is virtually incorporated into a surrounding section.
2. If separate OCs for level crossing barriers (closed) and street signals (undefined state) have different states, a safety rule can be configured to produce a differentiated behaviour. This may, for example, create a danger area which may be passed with reduced speed.
3. The safe element state change can, at request from the TMS, be re-assigned to the responsibility of a safety-actor (e.g. person or another safety system). For this purpose, a danger area is first requested by the TMS around the faulty element. Subsequently, the element state is overridden. This means that the safety responsibility for the safety condition “IOES is true” is delegated to the safety-actor responsible for that danger area. This also ensures that the utilization conditions on the danger area can only be removed/modified if the safety-responsibility is returned.

The overwritten element state also directly overwrites the value stored on the EIs operating state. In this way, every system involved will observe the same element state.

9.3.4 Utilization conditions (UC)

For the EI, an utilization condition is the basis for:

- checking if a MP/DA request is safe or not -> ensure safe changes of state
- comparison with the identified reality, in order to identify violations -> enable monitoring of safe states.

If a request would lead to a violation of one or more utilization conditions, the EI will not grant the request. If a violation of a utilization condition is detected, then a safety response will be carried out by the EI, with the aim of restoring a safe state. Utilization conditions arise from three sources:

- provisions defined by regulatory authorities, IMs, etc. which can be valid e.g. for the entire network topology (for example: only MOB types 1, 2, 3 and 4 are allowed to run on the infrastructure network).
- due to the physical properties of the topology used, such as structural gauge or maximum load on a bridge.
- due to operational limitations, such as in areas undergoing construction or maintenance work.

In order for a MOB to move safely on the network topology, the MOB states must comply with the utilization conditions of the network, as shown in the following table.

Table 1: Examples of utilization constraints

	Moveable Object	***MOB***	***MOB state***		
Infrastructure object element (IOE) ↓		Type	Current speed	Current max. axle load	Current max. structure gauge
IOE property	vMax (iron)		<shall not be exceeded		
	vMaxMOBTyp		<shall not be exceeded		
	Permissible axle load			<shall not be exceeded	
	Minimum structure gauge				<shall not be exceeded
IOE state	Suitable for driving MOB types x,y,z	< must comply			
	Not suitable for driving MOB types a,b,c	< must comply			
	Not suitable for driving all MOB types	< must comply			
	Unknown				
	Occupied				

Not occupied

The concept foresees that authorised safety-actors can only change the utilization conditions within the "safe range". For example, the maximum speed allowed within a construction area can only be changed to less than (or set equal to) the maximum speed in this area, or the range of MOB types allowed can be reduced to exclude commercial traffic but cannot be extended to allow traffic which was prohibited in normal usage.

9.3.5 Safe Distance

9.3.5.1 Risk Path

Between each newly requested utilization permission (UP) and the existing UPs there may exist a path making it possible to move from one to the other. This path can only be interrupted by elements that are in the corresponding state and are locked. These elements cannot be changed as long as the UP to be protected exists. Any possible path allowing a movement between UPs is called a risk path.

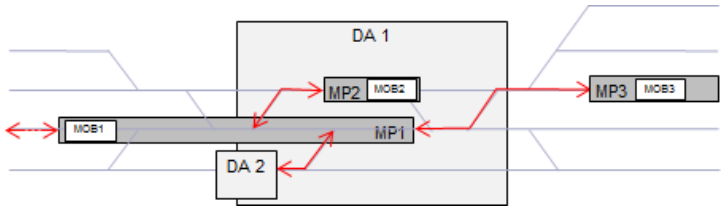


Figure 6 Risk paths between utilisation permissions

In the case of geometrical overlap (negative distance) between a MP and a DA, the risk distance between the two is not checked, but instead the risk path outlined to all other secured geographic areas (Utilisation Permissions), as shown in Fig. 10 (MP1 is checked). If no other secured geographic area is found within a parameterized geometric distance, the navigation to determine a risk path is aborted. In case of geometrical overlap, further checks are required. For example, to ensure that the utilization conditions of the overlapping section of MP 1 comply with those of DA 1.

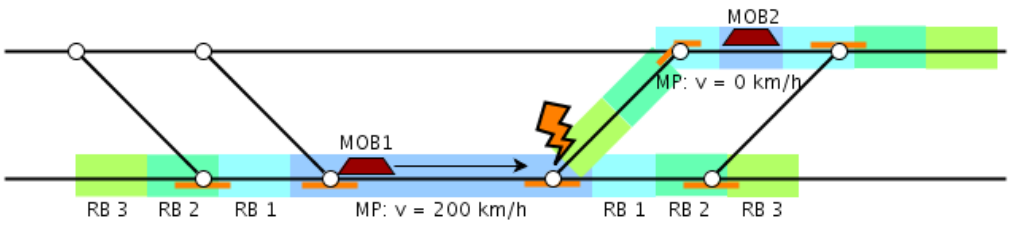
9.3.5.2 Risk Buffer

A Risk Buffer (RB) is a specific topology fragment with the minimal safe distance and goes in every trafficable direction along the topology at all sides, that are threatened by a movement (not reverse to it), around the UP, that are or could be made passable by changing unlocked IO. The length of the RB at a side of a topology fragment depends also on speed and direction of the movement, so that it could be zero behind a moving MOB.

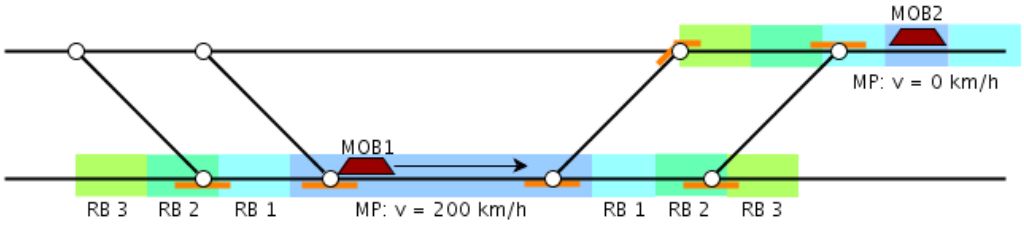
9.3.5.2.1 Application of a Risk Buffer

Each UP protects other UPs from itself - Risk Buffers spread along paths that can be reached by track bound MOBs in the UP.

Example 1: high speed train - MOB1's flank is endangered by a MOB2 at standstill, since a switch is violating flank protection - MP shall be rejected



Example 2: high speed train - a switch is violating flank protection, but no MOB is close enough to endanger MOB1; MOB2 is in safe distance - MP can be accepted



9.3.5.2.2 Length of the Risk Buffer

The length of the RB shall be the maximum safety distance possible for the related UP. Since the safety distance is always calculated for 2 MOBs and the second MOB is not known at the time the RB is calculated, worst case assumptions for the second MOB shall be made. The worst case assumption is a parameter (or derived from parameters) in EI application data set.

9.3.6 Safeguard

The EI also has a safeguard application. This application must monitor the occurrence of dangerous situations (hazard monitoring of hazard patterns). When they occur, a safety reaction has to be executed, that reduces the danger as much as possible and useful. The following pattern has to be monitored:

Unsafe Occupation

A MOB in/on/near a track occupies or threatens the track without UP.

Unsafe UC violation

A MOB in/on/near the track moves without MP or moves in a way, that it will not stay inside of its UP.

Not localizable MOB

A MOB is not or not correctly locatable (occupation, speed, ID, safety relevant properties) , for example because the communication to him is not available any more.

Unsafe change of UC

The safety relevant UC of an UP change in a dangerous direction without assurance and execution by the EI.

If one of the hazard pattern is detected by the safeguard, a emergency safety reaction (e.g. request emergency stop, request danger area) has to be triggered by the safeguard application.

The hazard pattern check is triggered by every change of the operating state.

9.4 Requesting and reserving a movement permission

The following example illustrates the operating principle from requesting a MP until it is written to the EI operating state. In the example, two planned train journeys from station A, lower track, to station B, lower track and from station B, upper track to station A, upper track, respectively, are shown:

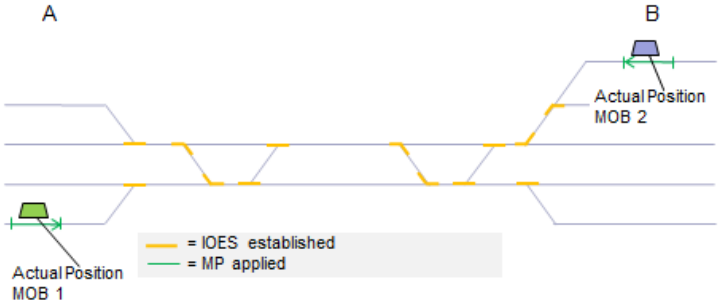


Figure 7 Operating principle MOB, MP – Start position

Start position: MOB1 and MOB2 are trains which have been moved to their current position with valid MPs. Their respective MPs were shortened to the minimum length at the end of their prior movements. Further movement from the current location is carried out by means of an extension (update) of the existing MP as described below.

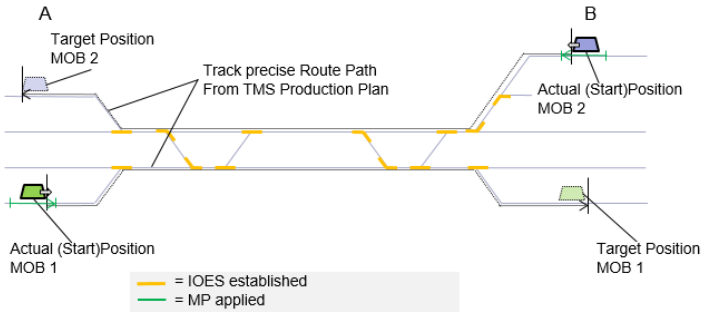


Figure 8 Operating principle MOB, MP – TMS operational disposition

The TMS wants to move MOB1 from A to B and MOB2 from B to A. Furthermore, the TMS possesses a track-selective positioning for both MOBs.

Before a MP can be requested for MOB1, the necessary infrastructure object element state (IOES) must be appropriately set. Before accepting the request, the EI shall ensure that any change of an element state does not violate any existing utilization conditions. Points and any other protective elements (IOE) may not alter their state as long as they lie in or belong to an existing MP (protective elements). The following locking mechanism shall thus be implemented:

Actor A generates the necessary requests for changing all the required element states for a MP to the required states - only if a change is necessary. Later in the process, when the EI accepts the requested MP, the EI ensures that all element states used by that MP are locked.

Note: The sequence of requests described above cannot be compressed, for example, into one request that includes the request for the IOES changes and the MP request. Since the EI does not consider time evolution and only checks the current operating state, the MP request will always fail because the IOES state does not match the MP conditions and it takes time to change the state (unless all states are already set as needed).

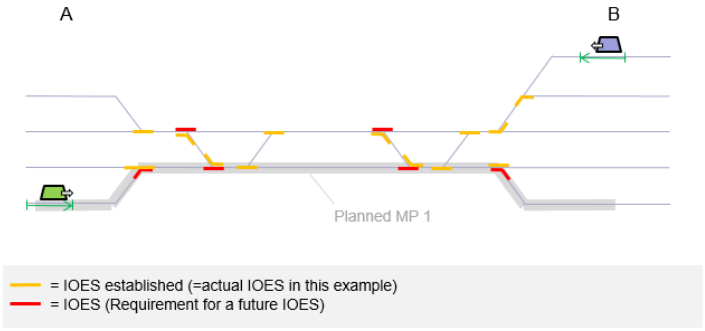


Figure 9 Operating principle MOB, MP – MP is first issued when all IEs meet the required states

For those infrastructure object elements that do not yet have the required element state, the IOES needs to be requested by the TMS.

Note: All IOES need to be requested by the TMS, prior to any MP requests.

If an IOES cannot be set (defect, error), the TMS must respond accordingly.

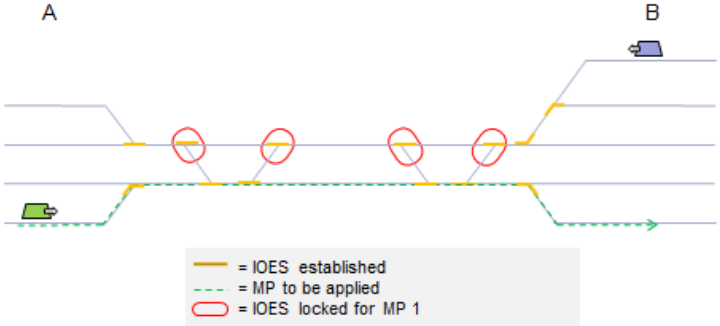


Figure 10 Operating principle MOB, MP – Locked elements offering protection against other MOBs

Once all IOESs meet the required state for MP1, the TMS can issue a MP request to the EI. Apart from a geometric extension, a MP request includes, among other things, a speed profile (v, location). The speed profile is necessary for the safety function to determine the risks (comparison between the risk path and the risk distance). The requested properties and utilization conditions are checked for feasibility and safety according to the known IOES.

Note: The required safety can be ensured by varying the speed, changing points (traditional: flank protection) and keeping distance between MOBs. If the TMS attempts to drive constantly at full speed, the safety function will eventually reject the MP request, because the requested MP or an already issued MP defines a speed which is too high for the current situation. For example, two trains travelling as shown below:

Figure 11 Safety distances by adjusting speeds

When train 123 approaches, depending on the speed and distance, train 456 will not be able to approach at the same time, because the distance between them is too small (traditional: slip distance). If the TMS now allows train 123 to travel at full speed, the MP for train 456 will be rejected. But if the TMS reduces the speed for train 123, both trains can approach at the same time because the safety distance changes depending on the speed profile.

For example: In Switzerland, the often used interlocking "Simis W" has a special operating mode regarding flank protection. When shunted, trains which have no flank protection may only drive at 80 km/h, otherwise faster. If this requirement is transferred to the EI' logic, for shunting movements, only a MP with a lower speed is permitted. If a MP with a higher speed is required for a passing train, then the MP will be rejected and the train must stop. No special operating mode is necessary, because the EI evaluates for each situation what is permissible.

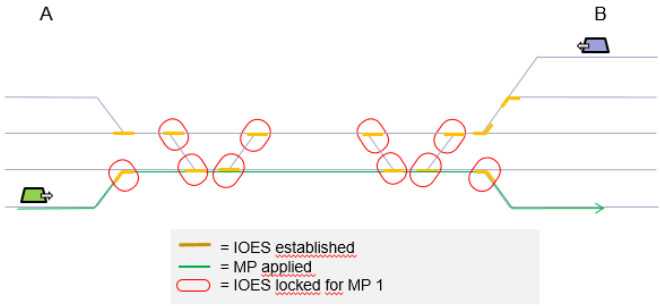


Figure 12 Operating principle MOB, DA, MP – MP issued

After passing the check of the risk distance, the MP is stored in the operating state and - in case of utilising ETCS - a corresponding Movement Authority (MA) is issued.

The scenario described above is shown below as an interaction diagram. Key findings from this study are:

- Synchronisation: a MP can only be issued if the necessary IOES' exist
- The operating state and the current actual state of trackside asset object do not always have to be identical (asynchronous)
    - On the operating state, the IOES must display the status "switching/changing, demand created" immediately after the request has been granted, and not only after the IO has reported its status "switching/changing".
    - There must be a function which actively manages the IOES. For example, the desired IOES is A, the trackside asset installation object state reports B, or IOES remains too long in "switching/changing" mode.

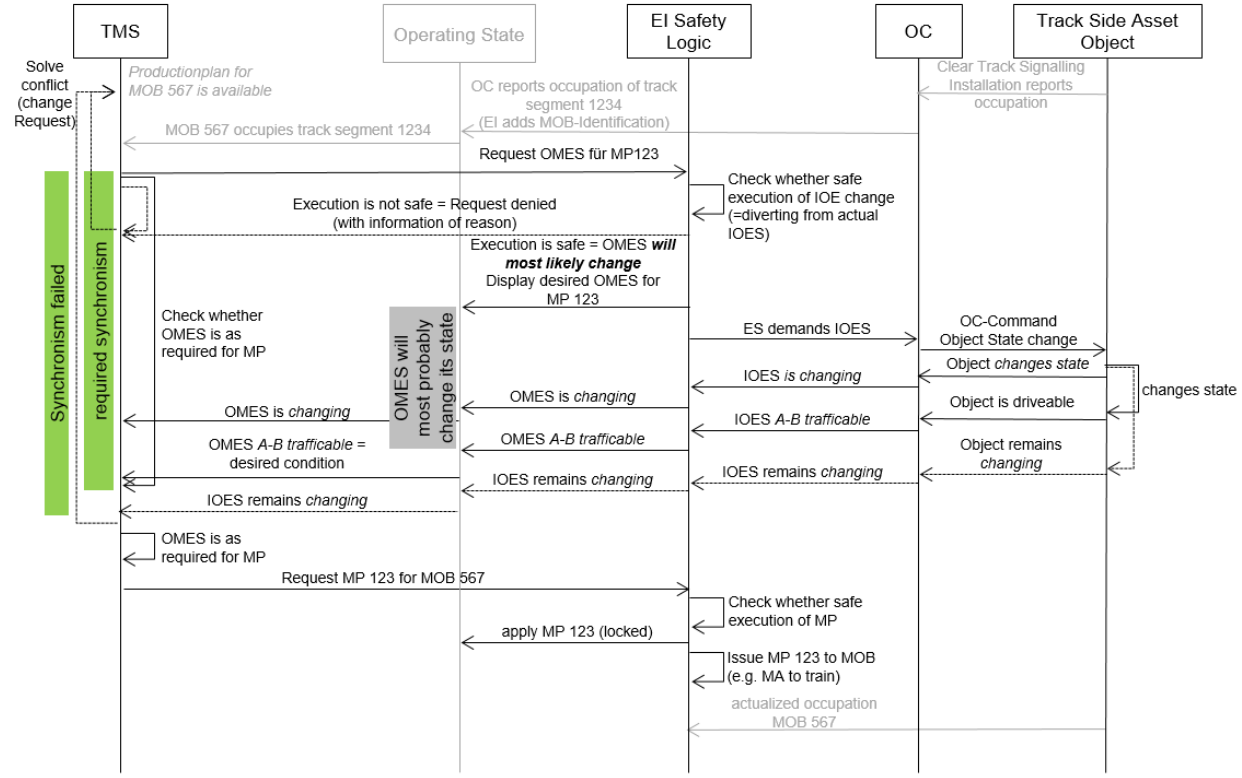


Figure 13 Interaction diagram - Creating a MP

The same procedure takes place if a MP is to be created for MOB2 (purple filled in circles indicate change in IOES for MP2).

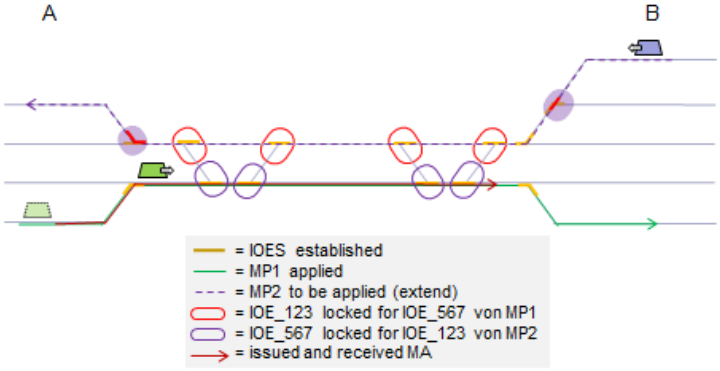


Figure 14 Operating principle MOB, MP - IOESs with reservation and lock protection within an external MP

In this example protective IOES, which are located in the MP of MOB1 are requested.

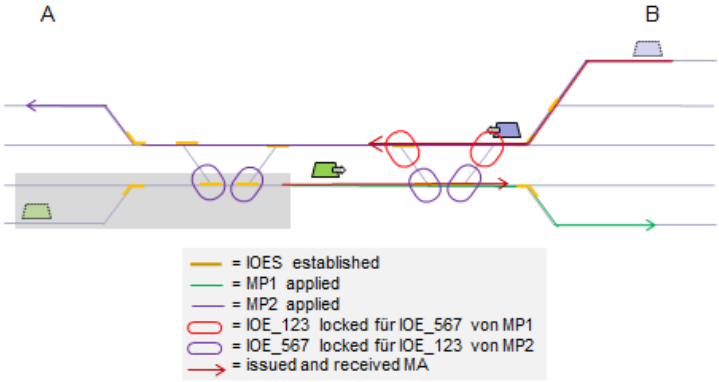


Figure 15 Operating principle MOB, MP - driving and cancellation of protective IOEs

Topology sections which have been cleared by the MOB within its MP are released by the TMS by means of MP update requests. The MP update request shortens the MP at the tail. Removing the MP from the IOES effectively unlocks them. As always, this safe release is checked by the EI.

9.5 Localisation of objects

One of the most important but also most challenging part is the precise localisation of the objects (e.g. trains). There are many different systems possible to send localisation information of the objects as clear track signalling installations (e.g. axle counters), train control systems (e.g. ETCS position reports), GPS, fibre optic, etc..

All localisation data of the object is sent to the EI over a defined interface. The duty of the EI is to analyse all this data and to merge it to an object which will be presented in the operating state. The EI will always choose the most precise localisation data set to represent the objects.
Example: The ETCS of a train sends its safe train front end position but not the safe train rear end position (no train integrity and safe train length is available). The clear track signalling system sends an occupation report of the corresponding track segment. EI will then take the ETCS train front position data to represent the train front end and the clear track signal installation information to represent the train rear end.

9.5.1 Effects of localization inaccuracies in the steering and the MP protection

Any localization technology inherently has inaccuracies, whether today's axle-counters are considered or GPS-assisted inertial technologies in the future. This implies that the safe algorithm of the object identification in the EI core must consider the MOBs to be larger/longer (“virtual length” or “safe track reservation”) than they in fact are.

In the case of rail-guided MOBs, it can be assumed that they do not leave the rails during movement (exceptions: road-rail vehicles, track laying machines). This means that the path on which a rail-guided MOB moves is known. A non-rail-guided MOB, however, can change its direction and speed at any time during a movement. Non-rail-guided objects can also move “outside” the rail topology (e.g. worker runs crosswise over rail tracks, car follows road), implying that their path is only poorly predictable, if predictable at all.

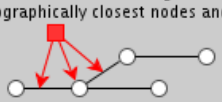
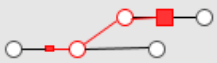
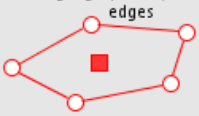
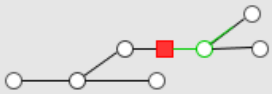
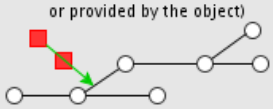
	Object Track-Guided	Object not Track-Guided
Position (P)	Point on Topology 	Point as LV95 coordinates with calculated references to the Node-Edge model via the geographically closest nodes and edges 
Occupation (O)	Consecutive sequence of track elements and section on track element 	Point with calculated references to the Node-Edge model via the geographically closest nodes and edges 
Speed (v, V)	According to technological equipment - if only position data is available,for example, calculation is done by EI or GLAT - is provided by the object itself	
Heading Vector	Along the path. Defined by current IOES. 	Free in space. (calculated by EI or GLAT based on the position data or provided by the object) 
Observations	All movements are bound to the track. Its current state determines what is possible and the direction of movement.	It has to be verified, that the mix between node-edge coordinates and free positioning yields good results in the detail specifications.

Figure 16 Overview of MOB position, occupation and speed

Every MOB has a physical length. However, the (geometrical) occupation of the MOB depends on the localization technology used. If “only” clear track signalling (CTS) information for a topology segment is available, the exact geometrical position of a MOB on that section cannot be determined. This means that the occupation will be equal to the length(s) of the section(s) occupied by the MOB.

Example: A locomotive with a physical length of 18 meters stands on a 50 meter long track section, where only a CTS system is available (e.g. track circuit, axle counter). The locomotive will thus be seen through its position extension as being 50 meter long, since the localization technology offers no additional information other than that the locomotive lies (somewhere) inside the track section.

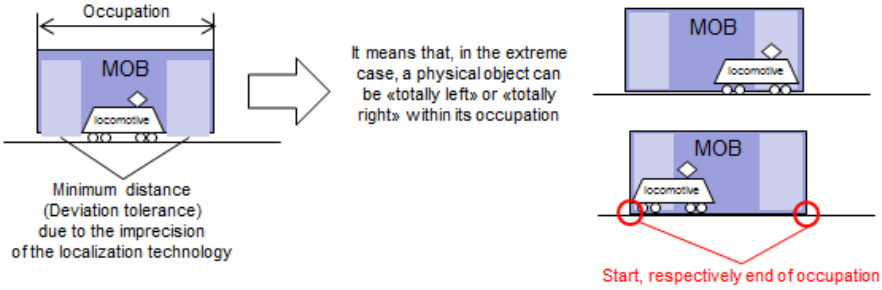


Figure 17 Principle of MOB occupation

Thus, the occupation of a MOB can be seen as the MOB's "virtual length", i.e. it *expands* the "real length" of the MOB by including the necessary safety tolerance inherited from the localization technology used.

Even if more accurate localization technologies are available and the MOB position could be identified, for example within +/- 5 meters accuracy, there are still situations where the remaining inaccuracy can be problematic. Namely, in the event of a planned approach, where two MOBs are to be coupled to each other, as outlined below.

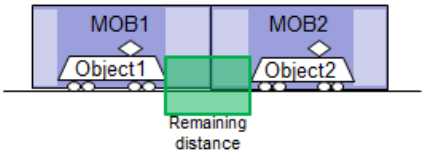


Figure 18 Remaining distance between physical MOB lengths

The presented safe distance is the smallest possible distance between two MOBs, which the EI can safely guarantee.

The EI only perceives MOBs, not the physical objects 1 and 2 as in Figure 5. Therefore, from the EI point of view, when coupling MOBs or during shunting movements, the MOBs occupation must overlap. This occupation overlap shall be allowed, however, only under certain conditions.

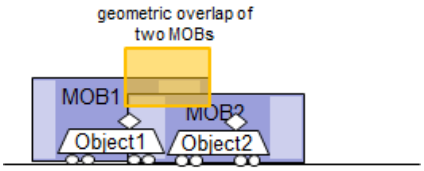


Figure 19 Intended overlap of MOBs (geometrical) occupation

On the other hand, two MOBs could be performing independent shunting movements (Figure 7, the driver has insufficient knowledge). In that case, an approach with occupation overlap is safety critical and shall trigger an automatic safety reaction. The MOBs should be warned or automatically stopped, and/or have their movement permission shortened, in order to avoid collision.

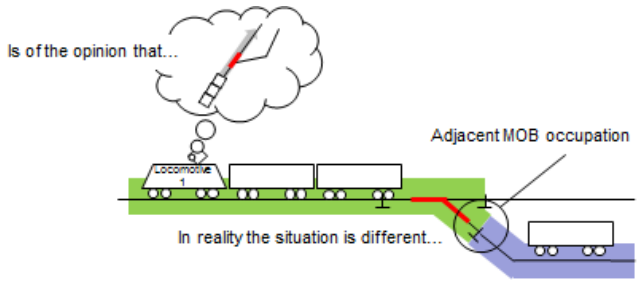


Figure 20 Unintended overlap of occupation

If only section occupancy information is available, the examples in figures 6 and 7 would be identically interpreted by the EI and would trigger an automatic safety reaction. From an operational point of view, however, it shall be possible to differentiate between an intended and an unintended occupation overlap.

Consequences of localization inaccuracy:

1. The EI cannot setup safe MPs when physical objects approach at a distance of 0 meters (e.g. unification).
2. The safety responsibility for compliance with the safety conditions 'free track' and 'risk distance ensured' may be transferable from the EI to another safety-actor (an entitled person, or another system). This other safety-actor shall operate as safely as possible until the physical zero distance is achieved. The EI shall thus implement a safe process in order to transfer the safety responsibility of a Utilisation Condition to another safety actor, as well as to resume the safety responsibility.
3. The localization inaccuracy (“tolerance”) must be considered while issuing a movement permission (MP) as it influences at which point the EI should transfer the safety responsibility to another safety-actor e.g. during approach movements. If the safety responsibility is not transferred in time, a safety reaction shall be triggered.

9.6 Geometric overlaps of MPs and DAs

From a technical perspective (but not from a physical perspective) there may occur geometrical overlaps of MOBs due to the fact that physical objects cannot be located accurately (see chapter above). Even if a millimeter-precise localisation (and control) were possible, there will still be cases where the EI considers a geometric overlap of MOBs operationally necessary (e.g. dipping the buffers during coupling).
Since the concept ensures that every MOB movement always takes place within a MP, and a MOB that does not move (stationary: shall not move) may be covered by a MP, the EI must allow geometric overlap of MPs with other MPs (i.e. two potentially moving MOBs) under defined conditions. Furthermore, geometric overlaps of MPs with DAs shall be possible under defined conditions (example: train that delivers building materials enters a construction site, enclosed by a DA).

Verification: In case of a MP request, the EI may allow a geometric overlap with an existing UP only if:

- the UPs to be overlapped allow the overlap in the requested segment.
- the utilisation conditions of the UPs are respected in the geometrically overlapping section of the movement permission.
- a non-EI safety-actor takes the safety responsibility for the utilization conditions "track free" and "compliance with distance between MOBs" (not to be confused with the "compliance with risk distance").

The safety-actors, to which EI can transfer the safety responsibilities (hierarchically), can be parameterized

Compliance: For a continuous monitoring of compliance within the geometric range of utilization conditions, in which safety responsibilities are assumed by a Non_EI safety actor, the EI shall verify that these safety responsibilities are transferred to the relevant safety-actor. The following example illustrates this:

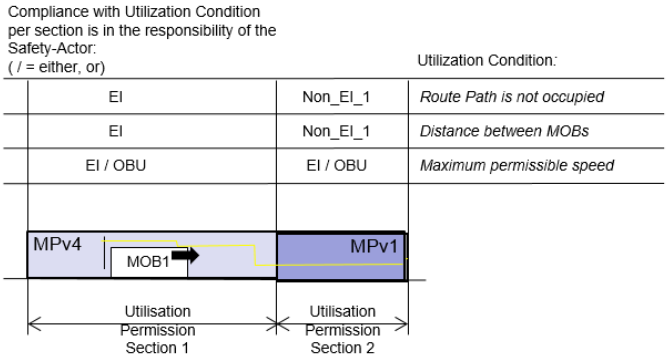


Figure 21 Example of different safety-actors due to geometrical overlap of utilization conditions

Hard limit: If the safety actor Non_EI_1 is not active when the MOB reaches the point where an emergency brake would stop it just before entering section 2, the EI will prevent the MOB movement as a safety measure. As a consequence, the Non_EI_1 safety actor must report the take over of the required safety responsibility for section 2 within section 1, i.e. a section transition without interruption of movement is desired.

Whether a MP is marginally or significantly overlapping a DA, is dependent on the operational requirements: for example, if a MOB "gravel train" is granted a complete and safe movement permission path by the EI to drive to the middle of a construction area, then the MP should be issued to the middle of the DA under the condition that the movement permission path is free. If the safety chief wants to take over the responsibility for the MOB "gravel train" from the construction site boundary on, one MP section would end at the construction site boundary and another MP section would begin within the geometric DA area with other utilization conditions.

Danger areas can also overlap geometrically. In case of overlapping, the most restrictive value must be considered for each safety condition. For the maximum permissible speed, for example, it means that the smallest speed of the overlapping DAs is valid within the overlapping area, as illustrated below.

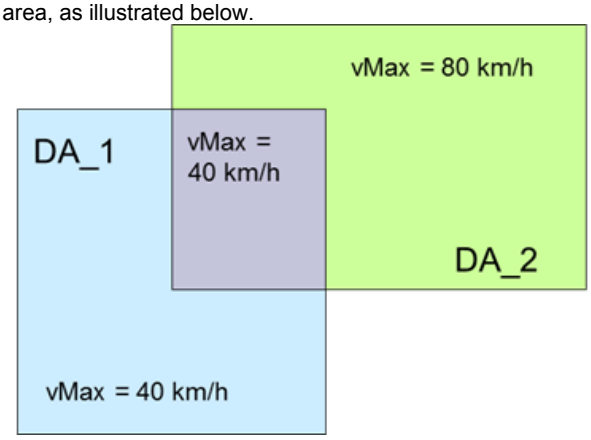


Figure 22 Overlapping danger areas

9.7 Conventional and extended safety aspects

9.7.1 Conventional safety aspects

The error-free detection and identification of movable objects, their properties, capabilities and states is an essential prerequisite for the EI. For example, the EI must be able to reliably determine if a movable objects is allowed to drive with the requested velocity and thus complies with a requested movement permission. Alternatively, the EI must be able to check whether there is a conflict or violation between the movable objects properties and states (e.g. structure gauge, axle load, cargo content) and the properties and states of the topology (utilization conditions).

The EI system receives the information on *conventional safety aspects* (such as the correct speed, secured closed path, isolated movements) from the underlying safety systems such as ETCS or the localization system. These information loops

are already closed and secured and can, therefore, be deemed reliable and safe. New localization systems shall be analogously designed, operate equally safe, and shall also allow safe movable object detection and identification. Today's architectural principles for the *conventional safety aspects* are adopted by the EI as a standard.

9.7.2 Extended safety aspects

9.7.2.1 Todays situation

Current interlocking systems do not receive any information on *extended safety aspects* (such as the structure gauge, hazardous goods, axle loads, untypical measured braking behaviour) which would allow extended safety checks. Checks are carried out by isolated systems such as train control devices. Currently there are no systems for checking *extended safety aspects* with a level of information reliability comparable to the interlocking systems.

In current higher-level IT systems (2017), the knowledge about a movable object is based on planned values in combination with manual inputs. For example:
1. A train is set up at a given location "A".
2. The driver manually inserts the train number into the control system at the reserved-section occupied by his train.
3. Based on the train number, the automatic route setting equipment retrieves the corresponding train records.
4. The connected interlocking station(s) are then activated according to the selected train data records.

In the event of an incorrect input, a "wrong" train data record would be retrieved and this may set up track paths which are not permissible for this train (e.g. too high axle load, inadequate structure gauge, etc). Additionally, production systems such as RCS-D (Rail Control System-Dispo) use the operational train number (including the additional train number and traffic day) to extract planned values from systems such as NeTS (Netzweites Trassen-System), CIS (Cargo Information System), and FOS (Formationsservice) as well as other information and properties. Based on this extracted information, the technical driving schedules are calculated and properties such as rolling stock type, load, etc. are displayed. By today's standards, if any of this data is incorrectly entered, no safety reactions are triggered i.e. the effects are not operationally intercepted.

9.7.2.2 Extended safety in EI logic

To incorporate the *extended safety aspects* in the EI logic, several prerequisites must be met. Following are the conditions for comparing movable object characteristics against track characteristics:

1. Recorded movable object properties shall be assigned a unique identification that can be reliably recognized and/or received by the EI.
2. Movable object properties and identification shall be reliably matched.
3. The EI shall be able to detect, at any time, all changes of safety relevant properties of a movable object.

Additionally, there are alternative approaches that may be employed in order to incorporate the *extended safety aspects* in the EI logic:

1. The extended safety aspects are tested in the higher-level TMS, based on unsafe information, e.g. from unsafe IT systems or unsafe sensors such as ZKE (Zug Kontroll Einrichtung). The movable object identification is performed by the TMS based on manual and/or unsafe processes. If the data is incorrect, the TMS will incorrectly verify the extended safety aspects, and thus possibly handle them incorrectly in individual cases. Only the conventional safety aspects are safely controlled by the EI.
2. A *safe MOB data system* is set up to secure both the identification and retrieval of movable object properties. This system would reliably keep the movable object records and safely manage any property changes. It would then become a new safe data supplier for the EI, and can uniquely assign properties to the localized movable objects. This approach allows the extended safety aspects to be included in the safety control of the EI.

The approach described at 1. provides a big improvement on the safety level, with comparatively low effort, even if it does not always operate fault-free. It cannot cause any deterioration in safety when compared to current systems. The logic described

in 2. also excludes the logic errors described in 1., however, it is comparatively more expensive. The 1st and 2nd models can be implemented at a gradually higher or lower cost.
The EI shall enable the implementation of both 1. and 2. logic models.

9.7.3 Continuous monitoring of movement

The safety logic requires knowledge of the point-dependent maximum speed of a MOB. The EI supports only the operation mode in which all MOBs movements can be continuously monitored e.g. ETCS "Full supervision" mode (analogous to CBTC). All other modes for movements are excluded or supplemented by additional technologies (such as GLAT) in such a way that the continuous monitoring of all movements is possible at all times. In the event that a continuous monitoring is temporarily not possible, it must be technically possible to either force the MOB to a standstill or to a defined foreseeable dynamic behaviour (direction, within a reserved range).

10 Processes and operations

In this chapter processes and operations for the use in a railway system will be treated. The processes and operations are possible with each CBTC system. Nevertheless, for a better understanding the description below is partly based on the use of ETCS L2/L3.

10.1 Processes

10.1.1 Initialization of the system

The initialization of the system (ETCS Interlocking) or a subsystem (e.g. Object Controller) bases on above described safety concept.

The process foresees that only if all safety responsibilities of an object are fully controlled by safety actors which are able to guarantee a safe use, the object can be used unlimited by the system. If the safety responsibilities are not controlled by a safety actor which is able to guarantee safety, the use of the object is not possible or is only allowed under certain conditions.

When for example an object controller of an element (e.g. point) is initialized, the safety responsibilities are allocated to a safety actor with limited rights (e.g. human being). The initialization process of the objects foresees that the safety responsibilities can be handed over to a safety actor with more rights. To achieve this, a process has to be followed by a system/application or by trained workers to achieve the required safety level.

10.1.2 Start up process of a movable object

Also in the future we have to expect (no GLAT available) that a movable object (e.g. locomotive) will start up on a track section where the location is not safely known by the ETCS Interlocking (e.g. after maintenance work). In this case, the System (RBC) may not send a Full Supervision movement authority for safety reasons.

In this case the safety responsibility of the distance monitoring would be attributed to the engine driver. The ETCS Interlocking would so only accept a movement permission (MP) if the requested speed of the train is low (e.g. 40 km/h). The engine driver is responsible to stay inside the MP. Moving over the first track side ETCS balise group the locomotive sends a safe position report to the ETCS Interlocking. Based on this position report ETCS Interlocking has the safe position of the locomotive and the safety actor of the safety responsibility (distance monitoring) can be set to a higher level (e.g. ETCS OBU).

10.1.3 Topology Updates

Since the network topology may change over time (e.g. new points), the topology data needs to change as well. For safety reasons, all safety relevant functionalities and/or components (e.g. EI, RBC, OC, ...) as well as the planning and steering elements (e.g. TMS) that are not safety critical, shall utilize an identical topology version in order to be able to communicate among each other. For availability reasons, an operation interruption for topology update is not possible. Therefore a functionality has been designed which allows updating topology versions without the need to stop and restart safety critical functions or components. For a topological/configuration change within the SR40 operation area, the topology to be changed will be embraced by a danger area, prior to preloading. Each topology version has been safely verified prior to the preloading action. Preloading ensures that all safety relevant components are able to utilize this topology version. If all components have successfully preloaded this topology version, an activation can be triggered. From this moment, the safety relevant components will utilize this topology version for production. It is possible, that during the preloading stage, certain verification of this topology version will take place. A new topology version can not be activated when verification did not occur or components could not successfully preload this topology version. Prior und during activation, no MOB movement in this area will be allowed.

10.2 Operations

In the following the concepts how railway operation will be executed are described. The operations described below shall cover all possible operations requested by railway infrastructures.

10.2.1 Basic running

To move a train, the Traffic Management System (TMS) must send a MP request to the ETCS Interlocking. The ETCS Interlocking itself checks if the train is able to fulfill the conditions and if the requested MP doesn't violate other safety restrictions (e.g. overlap with other MP). The ETCS Interlocking sends a MP demand to the RBC which translates the MP in a Movement Authority (MA). The MA will the be sent to the train.

The length of the MP and the maximum speed is defined only by the TMS. TMS is also responsible that the MP is requested in due time and all line side objects are in the correct state (e.g. level crossing is safe).

The train itself sends ETCS messages (e.g. acknowledgement) to the RBC. The RBC sends them to the EI OA which updates the operating state. The operating state shows the actual state of the train. Therefore, the TMS has the information about the MP executed by the train.

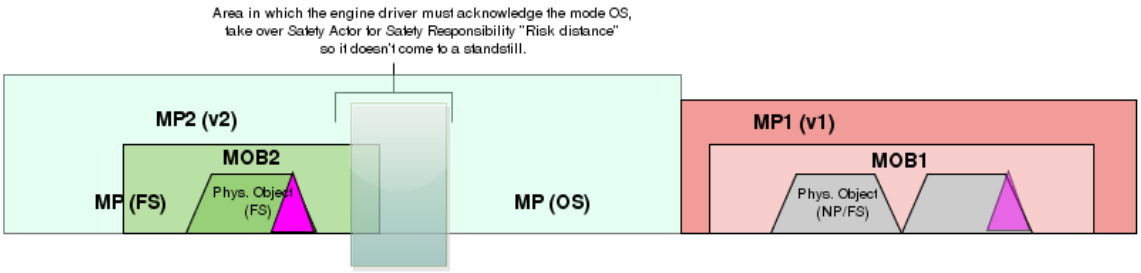
10.2.2 Joining

The following diagram sketches the procedure to join two movable objects (MOB) where each MOB has its own MP.

1) Initial situation: MOB2 in mode "Full Supervision" and MOB1 in mode "Non Powered", "Sleeping" or "Full Supervision". MOB1 is in standstill. MOB2 is travelling in direction to MOB1 and has to join with it.

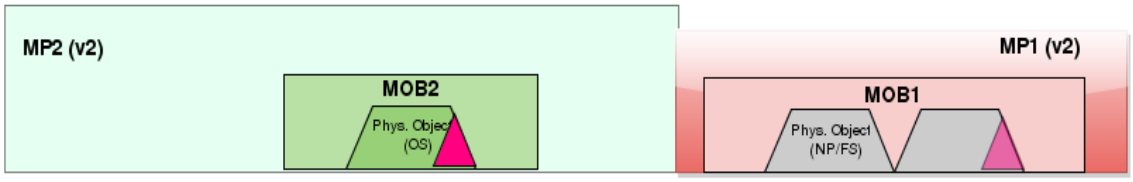
2.) TMS updates MP2 to touch MP1. Since the two MPs have to touch no risk buffer should be set. This is only allowed by the ETCS interlocking when the train driver takes over the responsibility "Risk distance" to prevent a collision with MOB1. Therefore the ETCS of MOB2 has to change in "On Sight" mode before the end of MP2.

3) MOB2 driver acknowledges within the acknowledgement window the change to the mode "On Sight" and assumes the safety responsibility for "Risk distance".

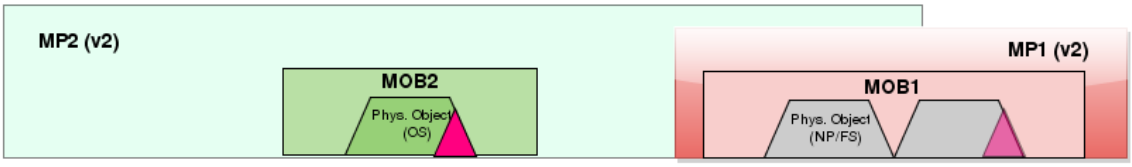


After the hand over of the safety responsibility is successfully performed, the actual joining can be initiated.

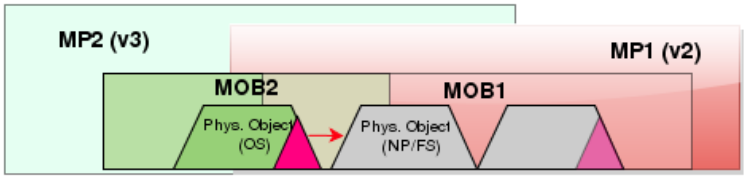
5) The joining is planned and the conditions are prepared by TMS to notify the EI of this planned joining.
TMS requests an update for MP1 to allow the overlap with MP2;
Train driver of MOB2 is now responsible for the safe approach.



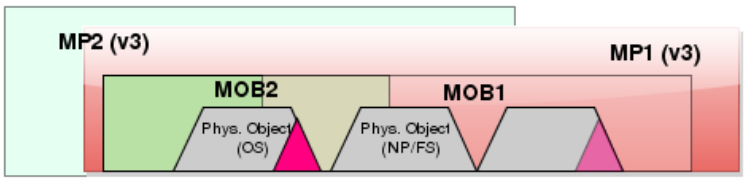
6) TMS requests update for MP2 with sections which allow overlap with MP1



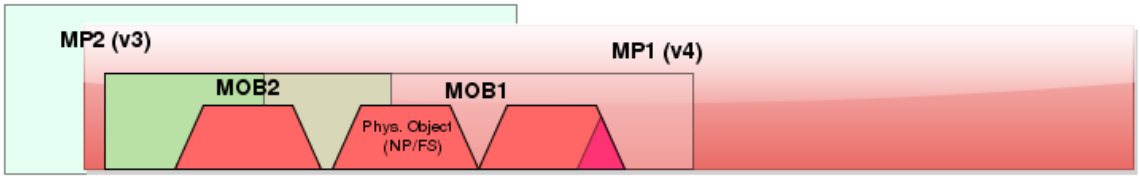
7) MOB2 and MOB1 couple, MP2 can be shortened



8) MOB2 logs off and shuts down. TMS request an update of MP1 to cover both trains. Physically, MOB2 doesn't exist anymore since it coupled with MOB1.

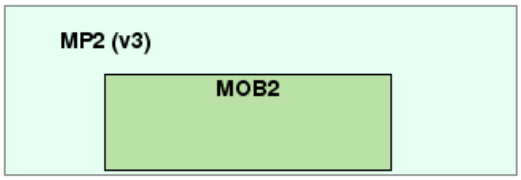


9a) MOB1 logs on again, updates its train data.
9b) TMS requests an update for MP1



10) MOB1 leaves the track. TMS request the shortening of MP1.

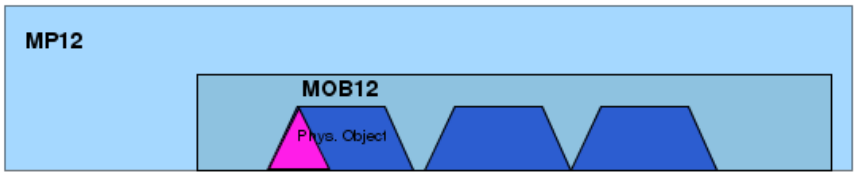
A clear section report is sent to EI. EI will demand the deletion of the MP2 and the position of MOB2.



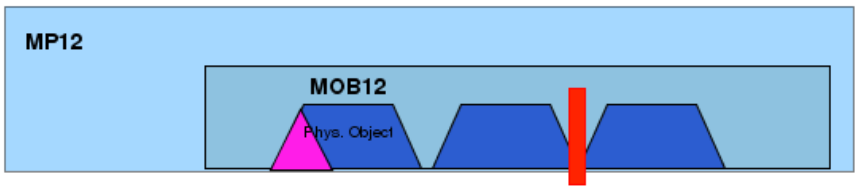
10.2.3 Splitting

Here the following example is shown: A train enters a track, stops, splits and continues the journey in the same direction.

1.) MOB12 entered the track and is in standstill..



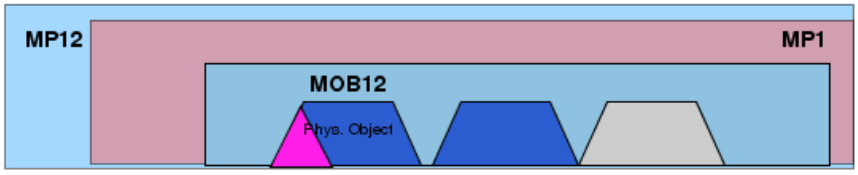
2.) The actual Splitting is performed



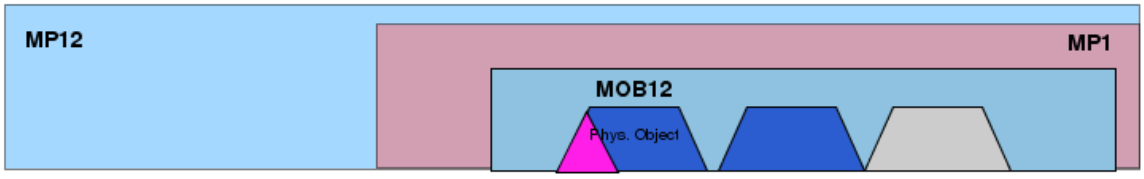
3.)

3a) TMS updates MP12 to allow overlap with MPs.

3b) If no safe splitting signal is available, EI does not know about the two parts of the train and TMS has to request a MP in advance. If a safe splitting signal is available, EI will create a new MOB and could automatically create the MP for the MOB.



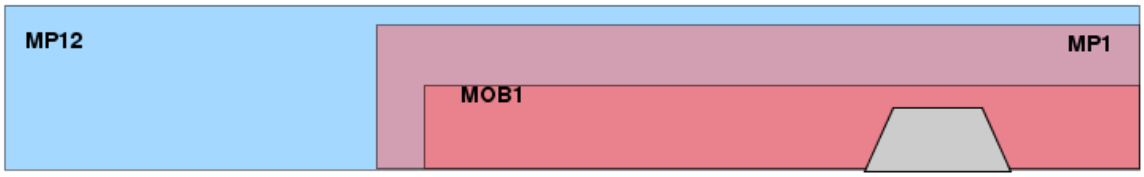
4.) TMS requests an update of MP12.



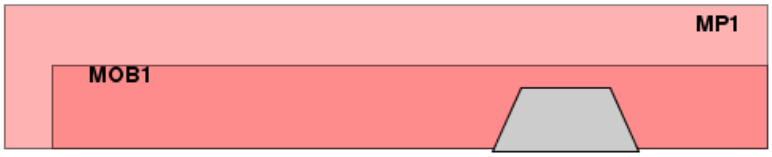
5.)

5.a) MOB12 continues the Journey and leaves the track.

5.b) Since the track is still occupied EI creates a new MOB. The safety manager does not react if the MP requested in advance fits to the MOB. If TMS would not have requested the MP in advance, SM would have to intervene and check which measures must be applied.



6.) TMS requests an update for MP12. Only MOB1 in MP1 is left on the track.



10.2.4 Change of running direction

Here it is shown how a train will change the running direction. It is assumed, that the train composition remains unchanged (no splitting or joining).

Note: The joining and splitting scenarios can also be adapted if the train changes the running direction.

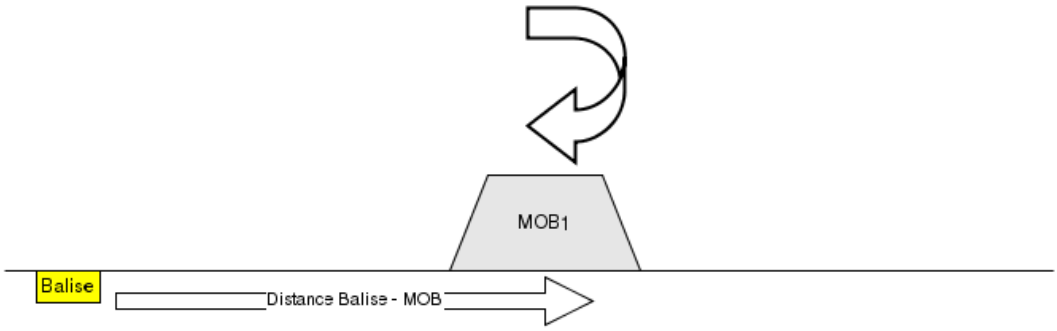
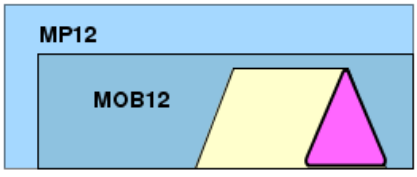


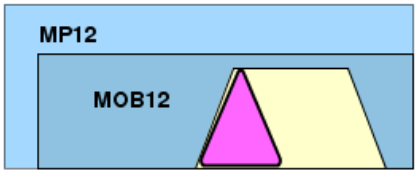
Figure 23 Change of running direction. The last read balise group is the reference for the new movement authority.

1) A train (MOB12) is running versus a track in which it has to change the running direction.

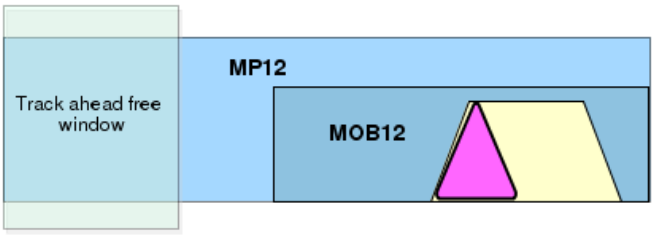
2) The train stops and the driver shuts down the desk (ETCS changes to "Sleeping Mode"). TMS requests the shortening of MP12.



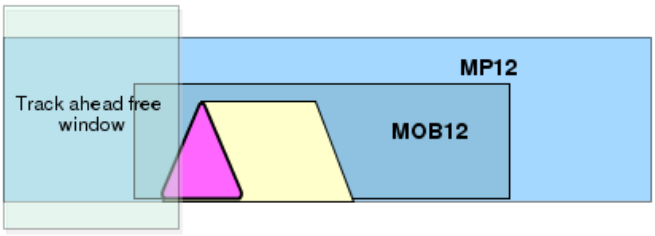
3) The train driver starts up the desk at the other side of the train. The ETCS connects with the RBC and sends a train position report. Based on the train position report, the RBC knows the train running direction and new position of the train front end. Since there is no guarantee that there is no wagon (with the assumption all vehicles are equipped with a GLAT tag) in the front of the new train front end the responsibility for "track ahead free" can't be taken by the system but by the engine driver.



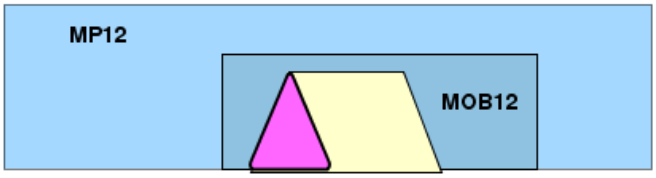
4) TMS requests an update of MP12 in the opposite direction. Since "Track ahead free" can't be granted by EI a movement permission with only reduced speed may be allowed. The RBC will then send a "On Sight" Movement Authority according to the new train running direction and will define a "Track ahead free" window where the train driver may acknowledge "Track ahead free



5) The train departs in "On Sight" mode. As soon as the train front end reaches the track ahead free window the train driver has to acknowledge the information on the desk. The acknowledgement will be sent to the EI. EI changes the state of the MOB ("Track ahead free" is granted by the EI) and updates the operating state.



6) Since the "Track ahead free" is safe, the train may now travel with maximum speed in mode "Full Supervision". Therefore, TMS sends the request of an MP update to the EI without this limitations. After the safety check by the EI the RBC sends a "Full Supervision" movement authority to the engine. The engine changes the mode to "Full Supervision" and is fully supervised by ETCS.



10.2.5 Shunting

The goal of the smartrail 4.0 project is, that in the future the system can do without line side shunting signals. Shunting movements without shunting signals will be executed in the same way as train movements. The information of the MP length must then be delivered by an other application or be integrated in ETCS system (change request).

Since there is no guarantee that the shunting signals can be replaced when the migration of EI starts, shunting signals must be supported by the EI.

However, for EI there is no difference between a MP for a train or for a shunting movement. The TMS requests a movement permission, EI checks if the execution is safe and sends a MP demand to a dedicated system.

Here it is shown how shunting movement will be executed when shunting signals are still in use.

If the MP is a shunting demand (on sight or track free) the EI shall trigger state change demands for OCs of dwarf signals.

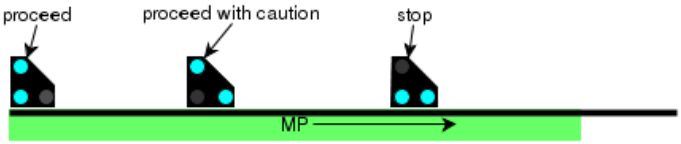
Dwarf signals shall only be set for the driving direction of the MP.

The last dwarf signal aspect within the MP (in driving direction) shall indicate 'stop'.

The second last dwarf signal aspect shall indicate 'proceed with caution'.

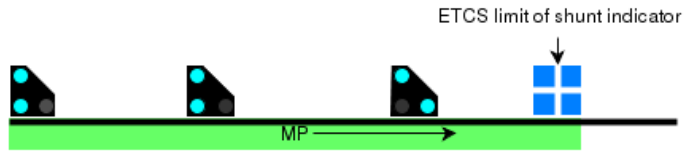
The section between the last dwarf signal and the end of the MP will not be used.

It is not EI's responsibility to match MP planning with signal locations.



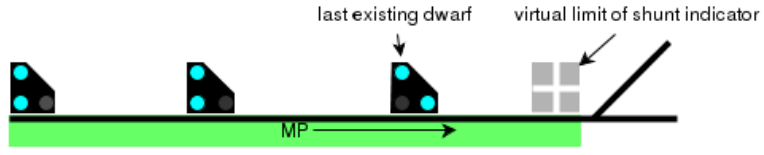
ETCS limit of shunt indicators (dt: ETCS Rangierhalttafel) shall be represented in the topology in the same way as operating dwarf signals. No OCs are linked. Its state is always stop.

For EI logic such ETCS limit of shunt indicator satisfies the rule that the last dwarf signal shall show stop. Thus, the last operating dwarf signal aspect may indicate 'proceed with caution', if it is followed by an ETCS limit of shunt indicator within the MP.



For areas outside the scope of EI (e.g. shunting areas), for which the last dwarf signal in EI's scope shall indicate 'proceed with caution', a virtual limit of shunt indicator shall be used to satisfy EI logic.

Such virtual limit of shunt indicator do not exist in the real world. But in smartrail 4.0, it is the same data object as a real limit of shunt indicator.



The last dwarf signal aspect before a not EI controlled area shall indicate 'proceed with caution'

All other dwarf signal aspects in a section with shunting shall indicate 'proceed'

10.2.6 Reversing

Reversing is a specific ETCS application with is used for evacuating trains out of danger zones (e.g. tunnel fire). The following picture shows, which parameters have to be defined, to be able to make use of this specific application:

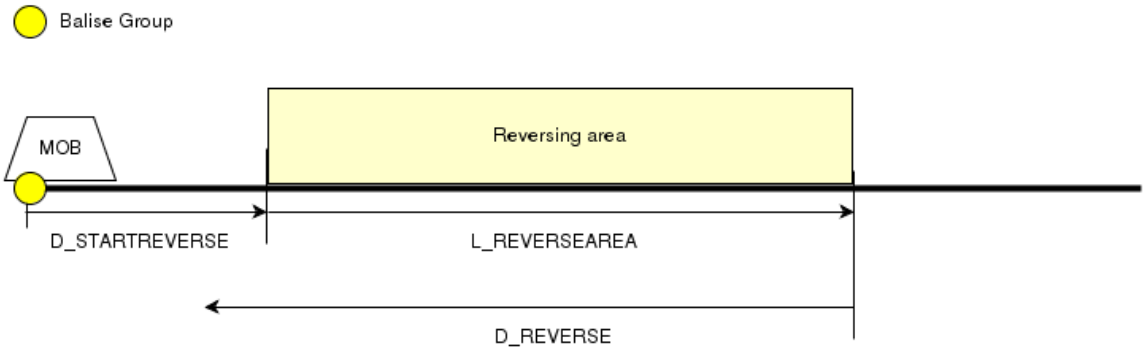
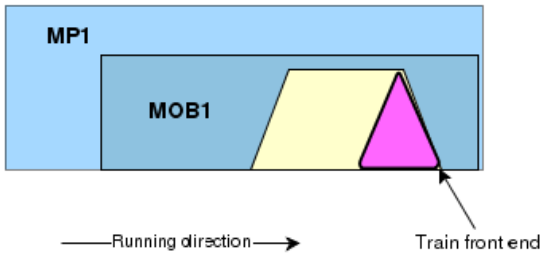


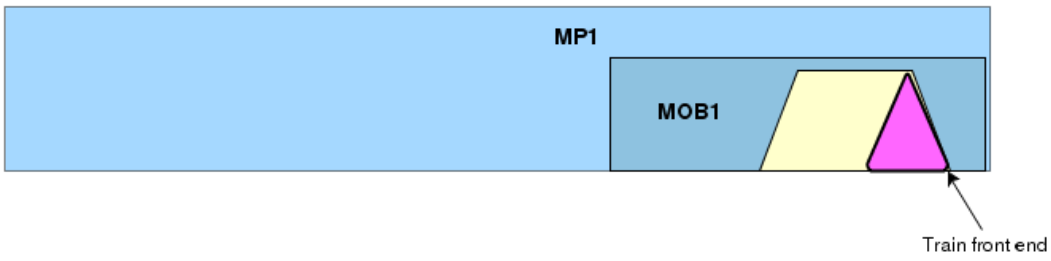
Figure 24 ETCS parameters for reversing.

If a train has to reverse, TMS sends a dedicated MP request to the EI. Receiving the MP demand from the EI, the RBC sends the needed ETCS packets to the train. It is in the responsibility of the RBC that the train will remain inside the MP. In the following the reversing process is described in more detail.

1) Train is tripped (emergency brake) because of a dangerous event. For protection reasons the train shall run backwards out of the dangerous zone.

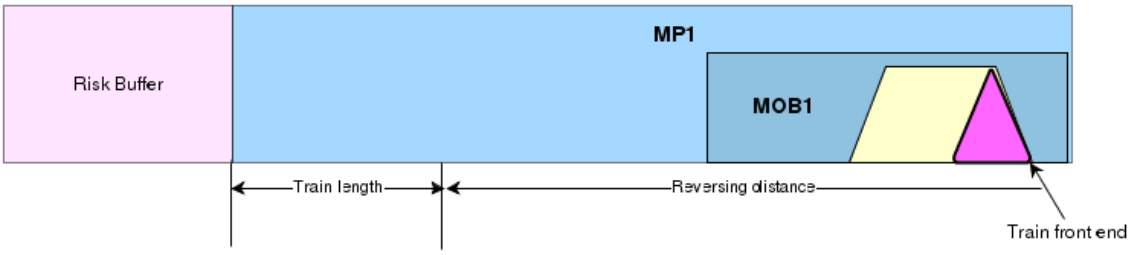


2) TMS sends a dedicated MP request to the EI. The EI checks the MP request and sends a MP demand to the RBC.



3) The RBC sends the ETCS packets to the train. The RBC itself is responsible, that the train rear end does not leave the MP. Since the reversing distance refers to the train front end the RBC has to guarantee, that the train rear end will remain inside the MP.

Note: It is possible that because of the lack of train end localisation system MOB1 leaves its MP. Since the ETCS system will guarantee that the train does not leave the MP the train shouldn't leave the MP. Nevertheless, EI sets in this case a big enough risk buffer at the end of the MP.



10.2.7 Transitions

Several transitions have to be handled by EI. Since EI will be migrated in several steps, borders to legacy interlocking have to be managed. These transitions can also contain RBC - RBC handovers. Moreover, the EI network can be divided in several EI areas. Transitions from one EI area to another EI area (e.g. neighbor infrastructure) must be handled too.

In any case, interfaces or specific Object Controllers have to be developed to manage the transitions in a safe way.

10.2.7.1 Transitions between EI and a legacy interlocking

Transitions from a legacy interlocking area to an EI area

A train running in direction of an EI area reads an announcement balise group and connects to the EI RBC. If the connection is established, the EI will create a new MOB with unknown position. Also the TMS is informed about the train running in direction of the EI because TMS knows the planning and is connected to the "old" automatic route setting equipment. Before the train reaches the border, TMS requests a MP for this MOB, to enter in the EI area. The EI RBC will then send a Movement Authority when it is sure about the exact train position. Therefore, some balises in no EI area must be known by the EI too.
If the legacy interlocking area uses ETCS L2/L3, a RBC - RBC handover has to be managed too. Therefore an interface between the two RBCs is foreseen in EI system architecture.

Transitions from EI area to a legacy interlocking area

The legacy interlocking area is informed about a incoming train through the TMS. The train running in direction of the EI will receive a Movement Authority until the first signal of the legacy interlocking. Depending of the border signalization the EI has to know the signal aspects of this border signal. Therefore, the Object Controller of the interface (legacy interlocking - EI) will present the signal aspect in the operating state. Based on this information a MP with a release speed will be requested by the TMS.

10.2.7.2 Transitions between two EI areas

In the following a EI - EI transition is described:

1. MOB1 is travelling in EI 1 area and wants to enter in EI 2 area.
2. MOB 1 approaches the EI 1 - EI 2 border.
3. TMS requests an MP for MOB 1 which extends over the EI-EI border.
4. EI 1 requests EI 2 to set a MP which starts at the EI - EI border.
5. EI 2 sets a reservation for a MP for MOB 1 and informs EI 1 that the MP is set.
6. EI 1 sets a MP over the EI - EI border and sends a MA to MOB 1

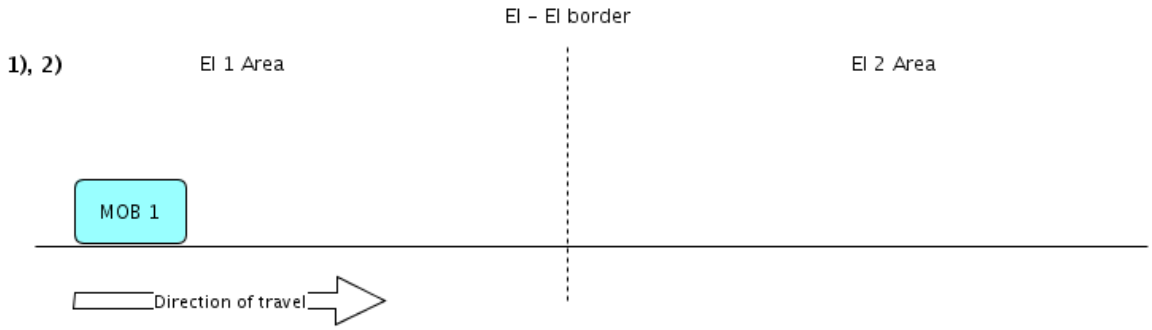


Figure 25 MOB 1 wants to travel into El 2 area.

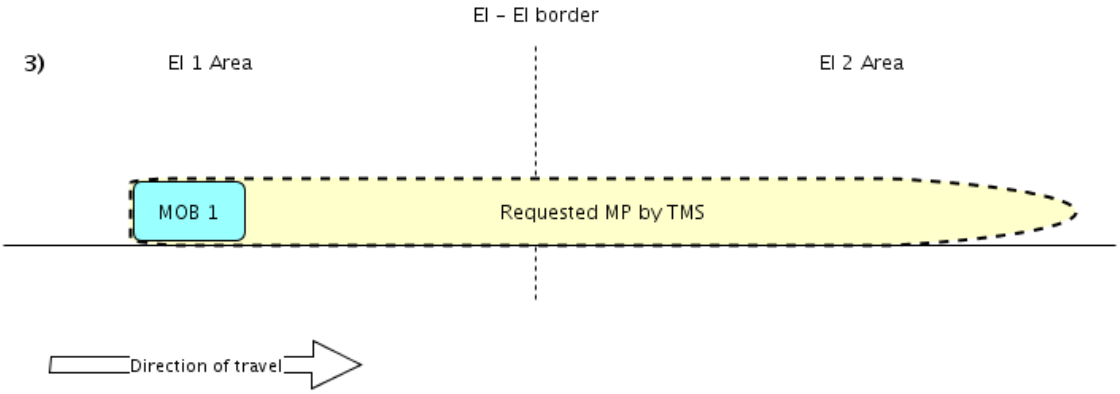


Figure 26 TMS requests MP for MOB 1

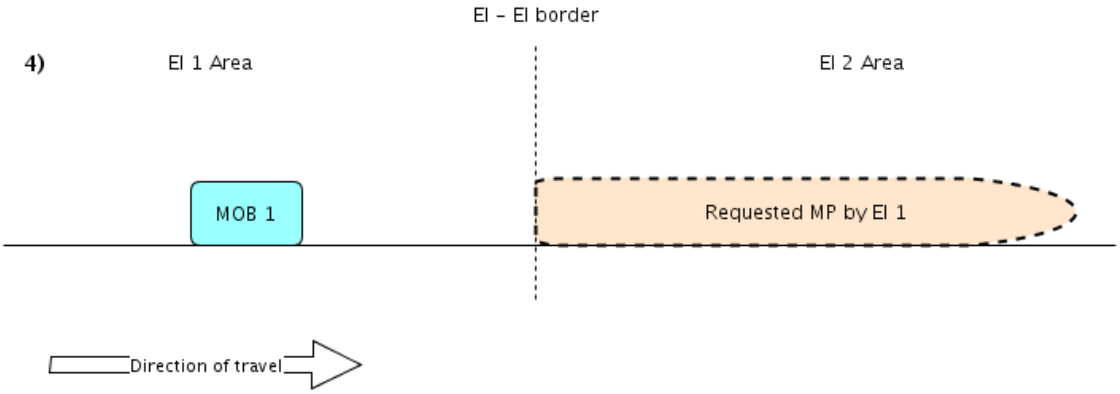


Figure 27 El 1 request MP for El 2 section.

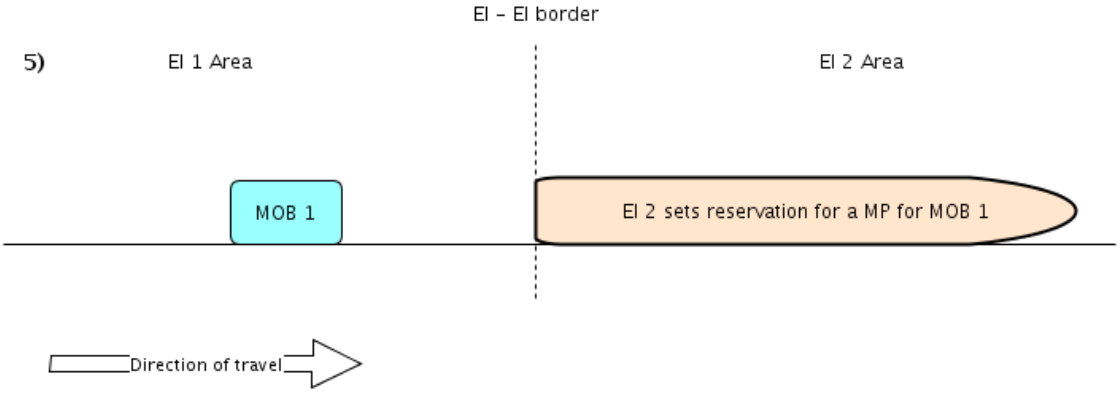


Figure 28 EI 2 sets a reservation for a MP for MOB 1 and informs EI 1 about.

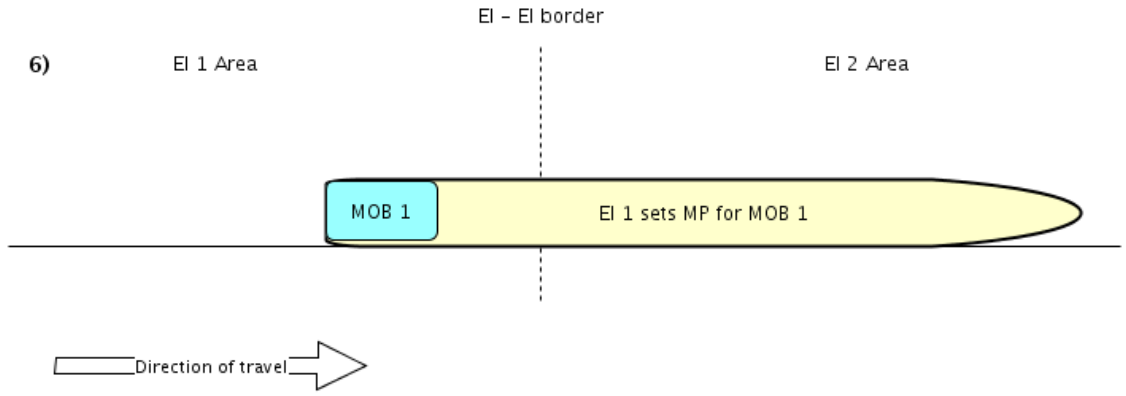


Figure 29 EI 1 sets the by TMS requested MP for MOB 1.

10.2.8 Track Conditions

Also under EI it will be possible to send ETCS track condition (e.g. lower pantograph) information to the train. This information can be sent in a safe or unsafe way. If the information has to be sent in a safe way, the state of the specific track condition area (e.g. powerless section) must be represented in the operating state. Therefore, an Object Controller has to be developed. If the information is not required to be safe another detection system can inform the TMS. TMS will then request a MP with the track condition information. This information will then not be checked by the EI. For time related track conditions (e.g. lower pantograph) a trigger point will be set on the topology. In this way it's guaranteed that the train receives the MP demand (incl. track condition) in due time.

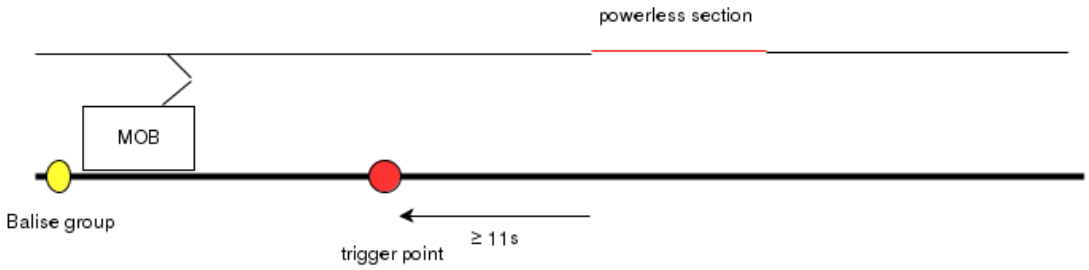


Figure 30 Schematic figure of a powerless section "Switch off main power switch". TMS may not request a MA which ends between the trigger point and the end of the powerless section (note: since the train may not stop inside the powerless section an MP shouldn't end close to the rear of this section).