OC Concept

Subconcept OC TOPO

Version 1.1_published, 30.4.2018

1 Disclaimer

This document is a DRAFT version which is still under construction. Its content may change in the ongoing concept phase of SmartRail 4.0. The document is not completely verified and is not finalized by now. The document is published to enable an open discussion of the ongoing work of the SmartRail 4.0 program.

Links and references inside of this document may refer to other documents inside of the program SmartRail 4.0, that may not be published at this stage.

2 Content

3 List of Figures

4 Glossary

Term	Abbrev.	Description
Infrastructure Object Element	IOE	The logical representation in form of edges and/or vectors of elements of the track side assets. This logical representation is - among other things - used to describe the track network topology and for communication purposes between software components. Example: a single switch would consist of either two non-directional edges or four (directed) vectors, representing the trafficability possibilities 'through' and 'deflecting'.
Infrastructure Object Element State	IOES	The current state of an Infrastructure Object Element. Example: The logical representation of the point in reverse direction (= an IOE) is "trafficable"
Level crossing	LX	A level crossing is an intersection where a railway line crosses a road or path at the same level.
Occupancy level		Logical topology level for representing the track occupancy (or inversely, the vacancy) reported by Clear Track Signaling Installations.
Point		It is a mechanical installation composed of rails, blades and auxiliaries, certain of which are movable, which enables railway vehicles to tangentially branch from one track to another without interruption of movement. *Clarification: in the UK, the term point refers to the entire mechanism, whereas in North America the term refers only to the movable rails an the synonym "switch" is used instead.*
Positioning level		Logical topology level for linking railway infrastructure points to track edges.
Trackside Asset	TA	Trackside installations such as rail points, level crossing barriers, signals, etc.
Trafficability Level		Logical layer of the topology which Expresses the trafficability of something.

5 Introduction

The Object Controller (OC) forms the link between trackside assets and the new electronic ETCS interlocking (EI). All EI relevant actions that are either executed by the OC, or the conditions that are detected by it, are related to the trackside assets.

A key feature of this function logic is that the interlocking control of the trackside assets is not generally carried out using signal wires, or more precisely classical interfaces, but by using software logic and the implementation of bus systems and communications protocols. As a result, instead of digital switching logic, a logical language is used to transmit actions and to report states.

> Assigning commands and reporting states **for the correct trackside asset** is one of the most fundamental aspects of safe OC configuration!

The topological models currently used for operation are data constructs that have continuously grown over the years.

6 Setting Targets

The OC topology will be used as a central element in the representation of trackside asset configurations.

The design of the topological model must therefore form a sufficient basis for correctly assigning all data applications that involve actor commands and sensor information. This topological description will follow an abstracted form, that will be based on generic descriptions of the topology and its properties and capabilities, independent of any hardware considerations.

7 Input Variables (Inputs)

7.1 Data Building

Remark:
The sub-concept OC-TOPO was designed based on the premise that the trackside asset topological references used by the OC will be also registered via the OC.
Meanwhile, an evaluation of the process of creating and validating a safe topology (TOPO4) has shown that this process flow should be called into question. As the OC only keeps parts of the topology in its representations, it is questionable as to whether it can on the whole make a fitting contribution to creating a safe topology.

7.2 Data Model

The abstraction of the rail network topology means developing and applying a data model that allows the topology to be described in terms of generic properties and capabilities.

In order to support quality and continuity, the data model which encapsulates the railway topology must be constructed accordingly. All necessary entities and their dependencies must be representable.

Special care must be taken in regard to the change management processes. A current representation of the topology has the character of a snapshot. The data model must enable data changes by supporting versioning. Several states (current state, planned state, previous state) must be manageable at same time.

7.3 Database

The integrity of the topological data has a significant effect on the safety of processes related to the infrastructure elements. The quality and safety of the database can only be guaranteed if all life cycle stages, from creation to archiving, can be proven to be error free.

Existing databases taken from current topological models can be re-used as long as the quality can be guaranteed in relation with the new models.

8 Requirements

All requirements related to the OC-TOPO concept are inherited from the basic requirements laid out in the main OC concept.
The current valid OC requirements can be found in subconcept document Anforderungskatalog (V02).

9 General Function Description

The following sections describe the data modelling for the topological references for trackside assets and their elements, so that trafficability and related functionality can be modelled in an abstracted and generic form.

9.1 OC Topology Datamodel and Trackside Asset Control

The object controller OC acts as a connector between the already installed trackside assets (legacy infrastructure) and the new software-based ETCS Interlocking. All traffic management actions and states exchanged between EI and OC are related to the underlying railway network topology.

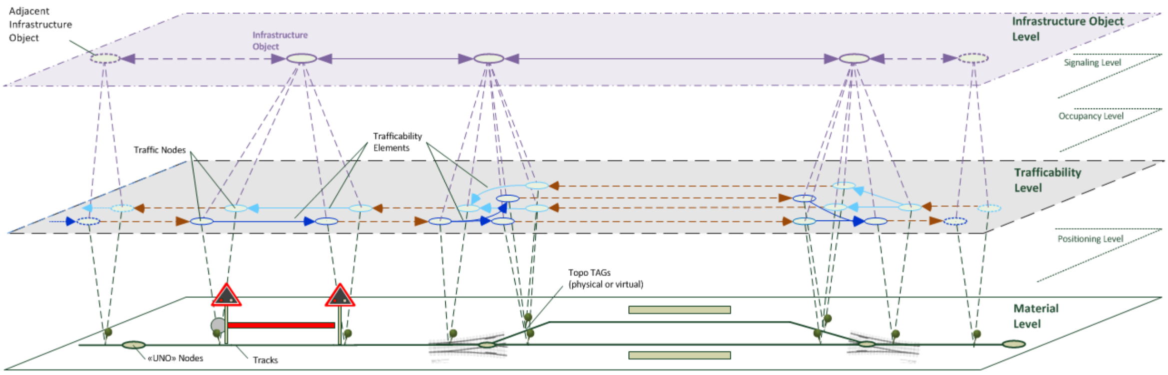


Figure 1 Layered model of railway network infrastructure

The whole railway network topology can be divided into six levels. The illustration above indicates all six, focusing on three of them: Material Level, Trafficability Level and Infrastructure Object Level. The additional levels Positioning Level, Occupancy Level and Signaling Level are described later in this document.

Since the OC sensor and actor functionalities concern the interactions between trains and railway network, the main functional level is called Trafficability Level. Graphs on this level have logical character. They are built up by interconnecting Traffic Nodes of adjacent infrastructure objects with connecting trafficability vectors.

The functionality used for controlling trackside assets is assigned to their trafficability elements. Trafficability elements are the subsets of infrastructure objects which safe states and offer capabilities. Connecting vectors are passive elements and therefore not managed by the OC.

Binding of logical nodes to their physical locations is done by another kind of nodes called *Positioning Nodes*.

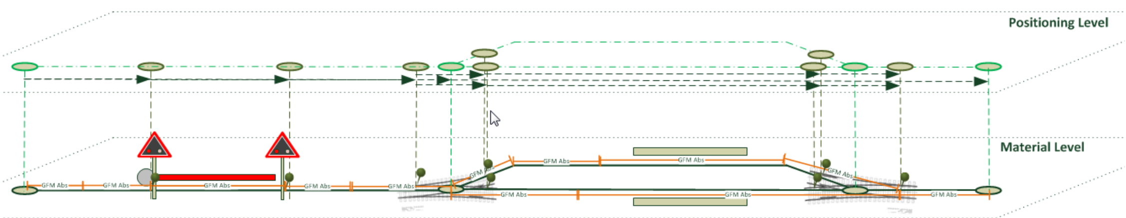


Figure 2 Positioning Level

Positioning nodes can be considered as pins which are attached to the tracks. Their Universal Unique Identifier (UUID) is used for linking any kind of logical nodes to correct and safe positions on the railway network.

On the trafficability level, several elements for movement control and monitoring exist.
The following list shows an extract of typical trackside assets and their assignment to different categories of trafficability:

Active elements (actors):

- Routing Control
  - Point-machine
  - Turntable
  - Derailer
- Object Protection
  - Level Crossing LX
  - Track-worker Safety System (TSS)
  - (Derailer)
- Movement Control
  - Signals
  - Automatic train protection systems

Passive elements (sensors)

- Track Occupancy
  - Clear Track Signaling Installation
  - Movement detection

Taking these different characteristics into account, the trafficability level must be divided into appropriate functional levels:

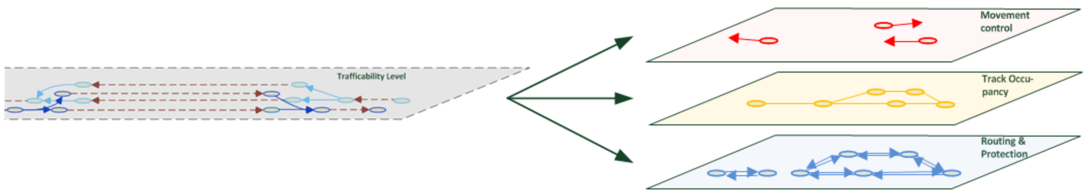


Figure 3 Division of trafficability layer into three sub layers

9.1.1 Routing Level

The EI routing functionality adjusts and secures routes on which railway vehicles may travel. Main elements of this level – next to common tracks - are points. **The traffic must be managed in a direction-dependent way**. Therefore, routing elements are modelled by logical nodes indicating the direction of travel. Such nodes are called *Inbound Traffic Node* and *Outbound Traffic Node*, respectively.

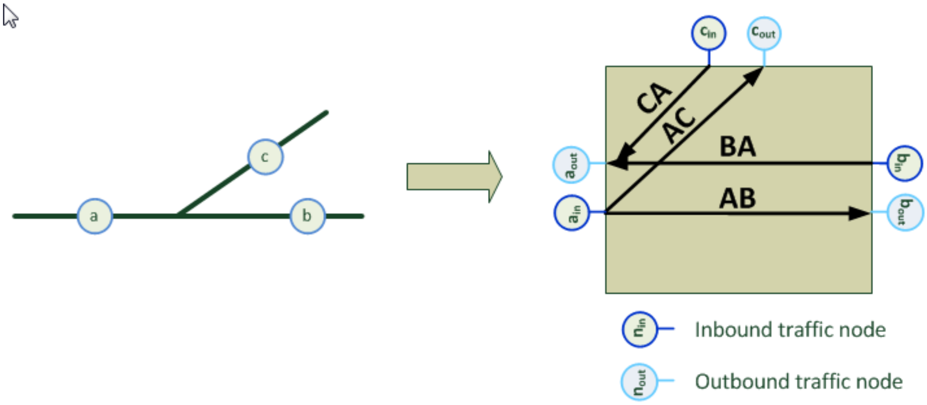


Figure 4 Vector abstraction of a two-way point

The picture above shows the OC modelling of a standard point. The three nodes a, b, c which define the track connections, are divided into sub nodes n_{in} and n_{out}, where n_{in} means inbound traffic and n_{out} means outbound traffic. The directed inner routes are represented as *Trafficability Vectors*.

A main characteristic of a point is that only one leg can be passed at a time. Therefore the OC has to manage the inner dependencies of the vector states correctly. The static presence of a vector means that passing is probably possible. The current state of an element is provided by the *Trafficability State* of the corresponding vector. A vector state dependency ruleset ensures that logical states always correspond to the physical behavior of the abstracted infrastructure object.

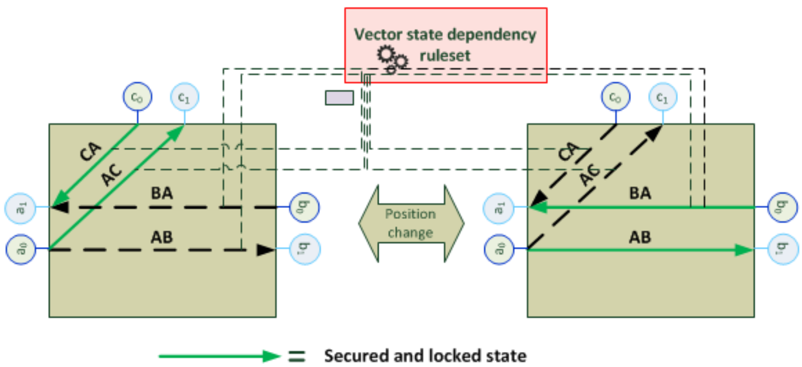


Figure 5 Vector state dependency ruleset

With this modelling concept, all kinds of trafficability variants for routing elements can be defined. Below, the modelling of a double slip point is presented as a further example:

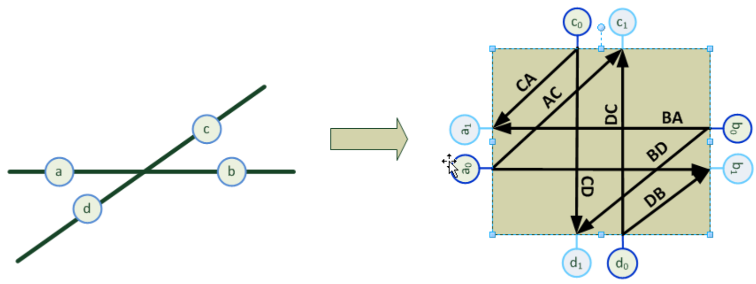


Figure 6 Vector abstarction of a diamond crossing

Special Routing Element Spring Points

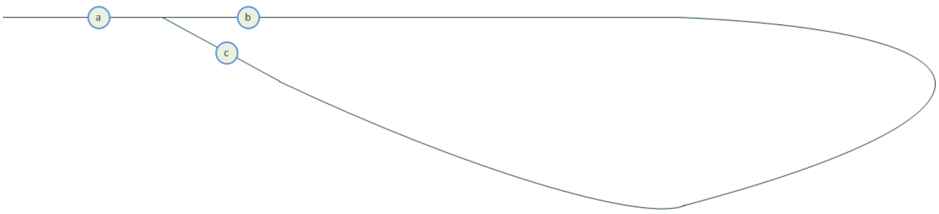


Figure 7 Track loop for turing trains

The above illustration shows a rail loop with spring points. The set-up can be used for turning trains around.

The spring points can not be controlled. The train activates them when it passes over and, once finished, a spring mechanism resets it to the default position (ahead only).

The corresponding vector model looks like this:

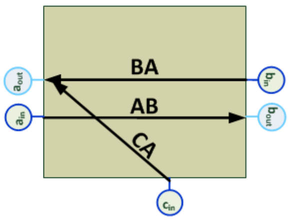


Figure 8 Vector abstraction of spring points

Thanks to the spring centring it never deviates from the default position. The vector model illustrates this.

The backup points have the following properties regarding the EI – OC interaction:

- A route cannot actively be set or locked. The point is virtually unmanaged. Points like these do not have the same capabilities as a normal point.
- The current state can only be detected if the point has the corresponding sensors.
- The point can be travelled over. However, restrictions such as slow speeds apply.

The following concept is proposed for handling such elements:
If the point is going to be used for a movement permission then it must be, as it were, 'prepared' so that its vectors can display a state in the operations representation, which makes them suitable for a movement permission.

This preparation can be made using a special capability. In using this capability, the OC would be set to a corresponding (virtual) state *SecuredByUse* (applied to all vectors).

There would also be a capability for locking and unlocking this state. Unlocking would clear the virtual state *SecuredByUse* again, meaning that the initial conditions *Secured* for AB BA and *NotSecured* for CA would be set.

This physically non-applicable virtual state would signal the intention of using the point for traffic routing only and that the current state would only be set DURING the passage of a train.

Using such a state would have the advantage of never having to use *NotSecured* vectors for movement permissions.

9.1.2 Protection Level

Level crossings (LX) and warning systems (= trackworker safety systems TSS) are main protection systems. The protection acts in similar way for both LX and TSS i.e. level crossings protect tracks and therefore trains from other objects and vice versa. Warning systems protect tracks and therefore trains from personnel and vice versa.

Protection areas are configured in relation to a section alongside one or multiple tracks.

Example A) Modelling of level crossing with two tracks:

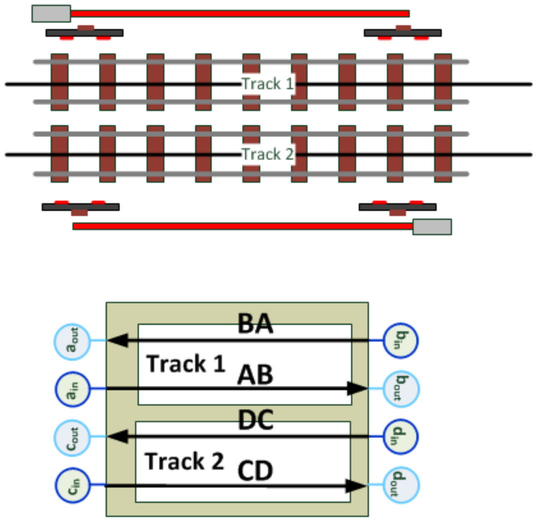


Figure 9 Vector abstraction of a two-track level crossing

Similar to the modeling of points, every track protected by the level crossing is abstracted with two vectors

Example B) Modelling of OC managed warning system

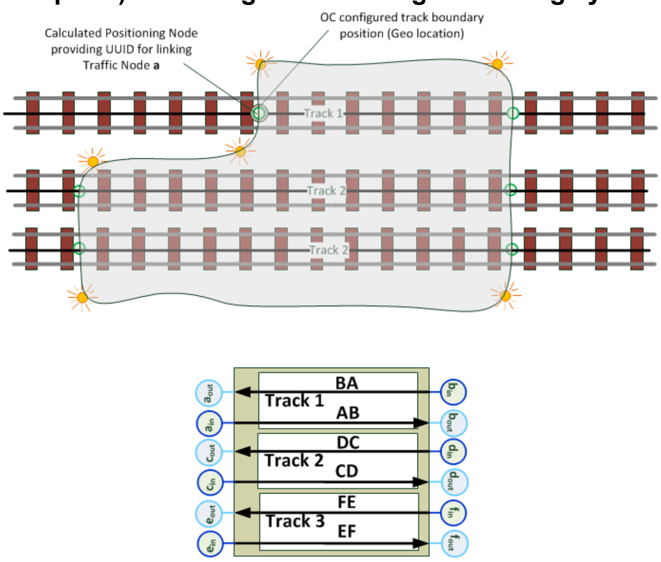


Figure 10 Vector abstraction of a protected area with three tracks

Remark:

One of the reasons why protection is modelled in direction dependent way is the fact that visibility of protected objects can be dependent from which side the train drives. This is relevant, for example, when the train is traveling with on-sight driving restriction. This means that infrastructure objects on the protection level are modelled in same way as infrastructure objects on routing level.

9.1.3 Track Occupancy Level

The object controller must be able to interact with Clear Track Signaling Installations. Infrastructure objects of this type are either axle counters, track circuits or rail contacts. On OC, train detection sections are modeled as *Trafficability Sections*. Trafficability sections are undirected connections between two traffic nodes. As no direction exists, the distinction between logical inbound and outbound traffic nodes is not necessary.

9.1.4 Movement Control Level

Movement control managed by an OC is treated either with help of traditional (legacy) trackside signals or with the help of automatic train protection systems, mainly track antennas. Both, signals and track antennas are modelled as point-shaped infrastructure objects. Modelling of signals is more complex because the visibility has to be taken into account. The following section illustrates the modelling of signals:

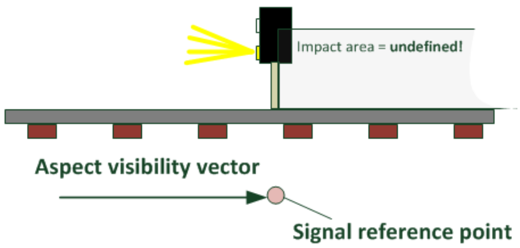


Figure 11 Modelling of a signal

The geo-location of the signal reference point is configured on OC. The signal positioning node, representing the start of the signal impact area, must also be provided by the OC configuration. Additionally, an *Aspect Visibility Vector* has to be configured. The instance that combines and validates Topo information provided by different subsystems must be able to manage the signaling direction correctly.

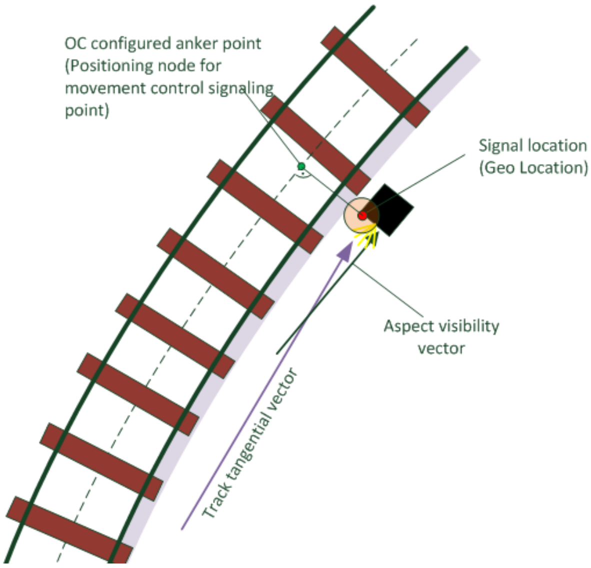


Figure 12 Topological reference of a signal

OC managed signals support a fixed set of aspects. Different aspects are made available by providing corresponding capabilities in the capability profile (refer to sub-concept Subconcept Modes of Operation and Configuration).

9.1.5 Connecting Vectors

For building up the complete trafficability level, logical nodes of OC managed infrastructure objects must be connected with the connecting vectors. *Outbound Traffic Nodes* are always bound to *Inbound Traffic Nodes* and vice versa. The result must be a vector chain without any gaps. Connecting vectors are constructed by instances outside the OC and are not known by it.

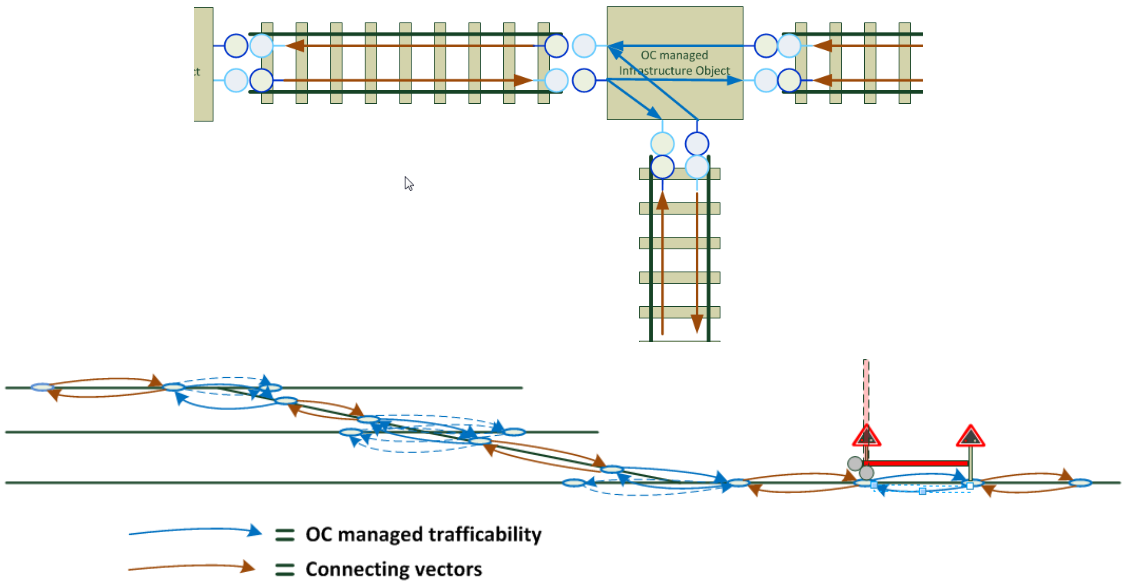


Figure 13 Connecting vectors

Remarks

An OC is only accepted by the EI as valid if the OC TOPO corresponds to the EI TOPO.

The binding element between the physical and logical world is the positioning level. Positioning nodes place logical nodes (e.g. trafficability nodes) on physically existing tracks, represented in the material level.

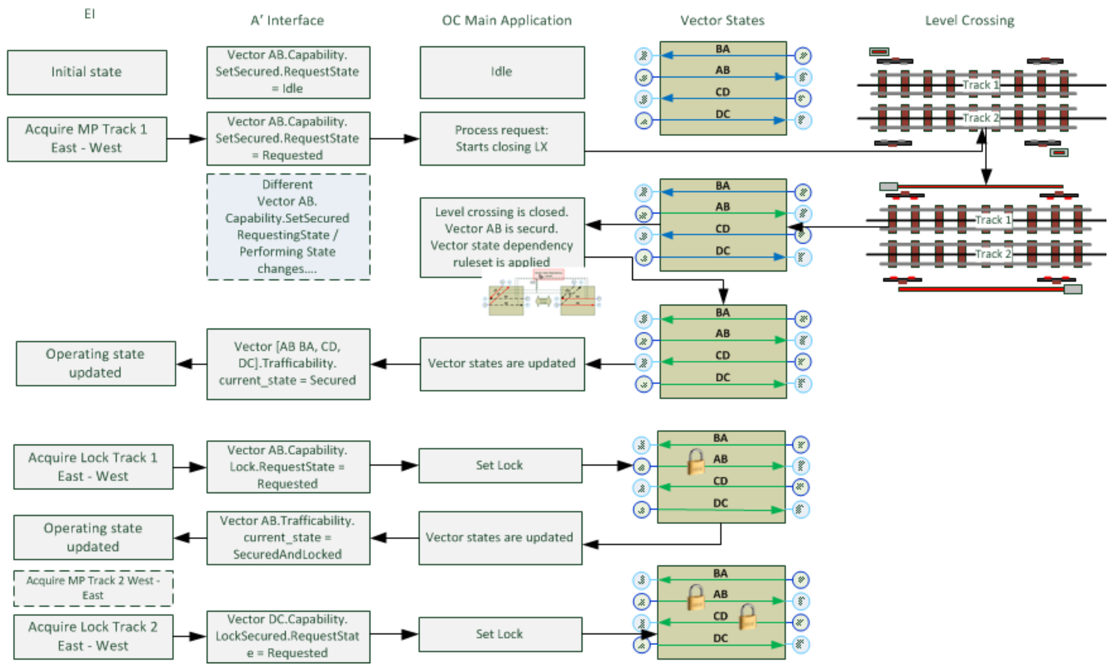
9.1.6 Capabilities and States

As a project requirement, the interface logic between EI and OC must be generic and as simple as possible (see “open safety”). Therefore the following rules are applied.
Every *Infrastructure Object Trafficability Element*, either *Trafficability Vector*, *Trafficability Edge* or *Traffic Node*, supports a fixed set of states. In addition, every trafficability element supports a set of capabilities. Capabilities enables state changes.

9.1.7 Locking states and cleanup procedures

States bound to trafficability elements support a locking mechanism. This locking mechanism serves two purposes. First, it provides a higher level of safety by ensuring that the OC knows that the current state may not change under any circumstances. Second, it is part of the cleanup procedure. As soon as the lock is released, the OC may change to its default state. It is up to the OC to decide if this is necessary or not. This means that any states of vectors, edges and nodes used in a movement permission have to be locked before the movement permission (MP) is requested. The EI will check the locks as part of the safety conditions to grant a movement permission. When the MP is removed (or shortened), the locks have to be released to, either by the EI or the TMS.

Example: Level crossing protecting multiple tracks:



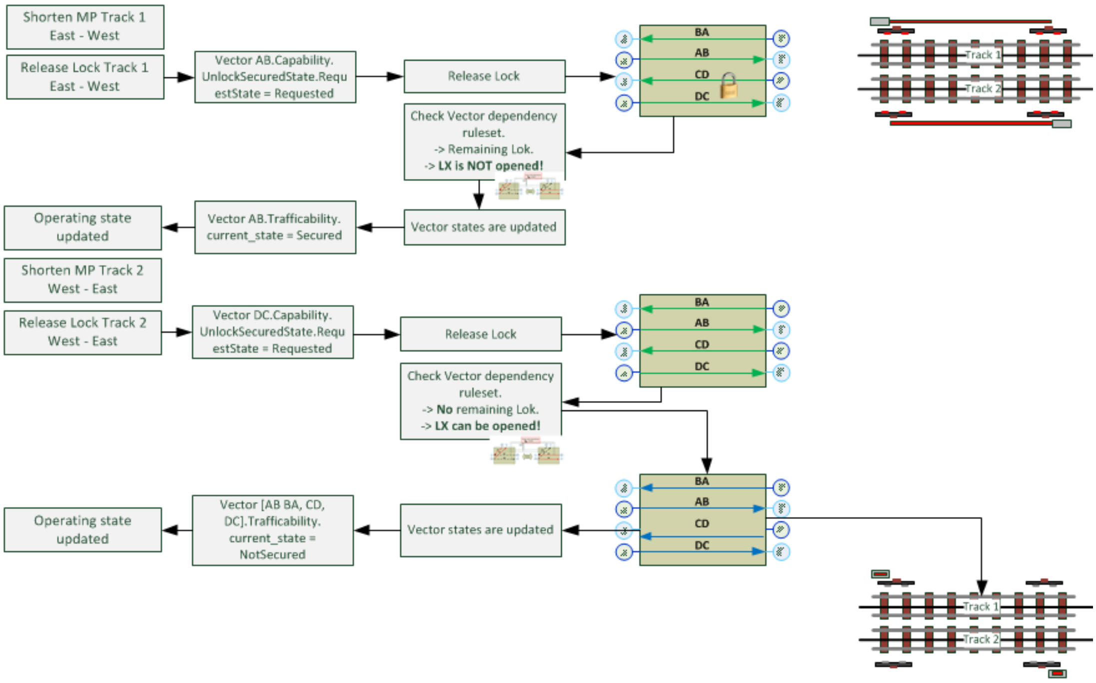


Figure 14 Process of securing a two-track level crossing which is represented by trafficability vectors

9.1.8 OC Data Model

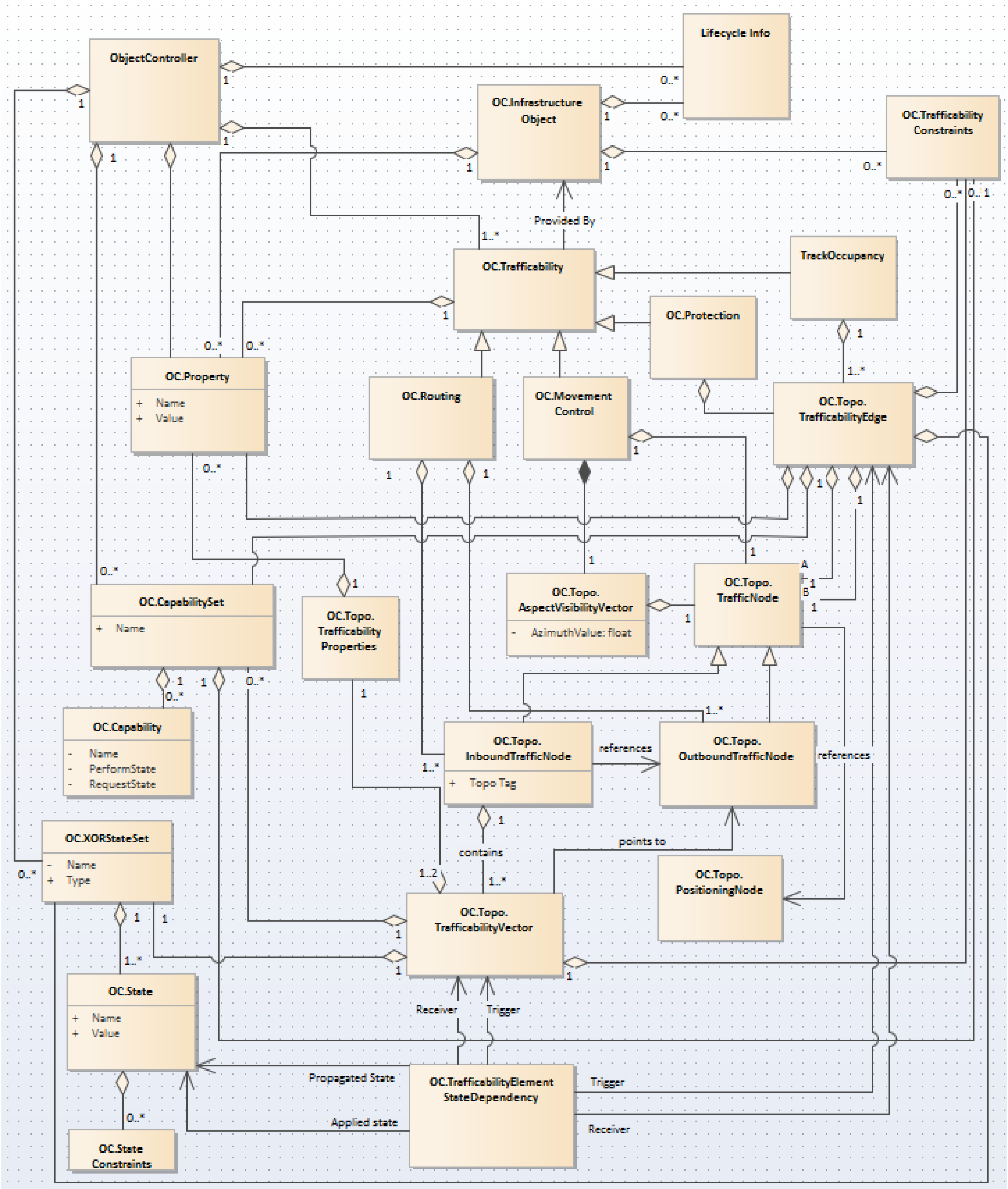


Figure 15 Possible semi generic C data model

Informal Description

One OC can manage one or multiple infrastructure objects. Infrastructure objects are trackside elements such as points, level crossings, etc.

One Infrastructure Object represents one or multiple trafficability elements. Trafficability elements are *TrafficabilityVectors*, *TrafficabilityEdges* and *TrafficNodes*. Every one of these elements contains properties, states and capabilities.

9.1.8.1 Class Description

Class	***ObjectController***	**Namespace**	***root***
Description	The Object Controller is the root element and represents the OC device (Hardware and Software).		
Data elements / examples			
Properties	Model, Type, SerialNo, MaxPowerUsage, ….		
States	CurrentRunLevel, CurrentSafetyLevel, …		
Capabilities	Reboot, Reinitialize, ChangeToRunLevelX, BackupConfig, RestoreConfig		
LivecycleInfo	InstallationDate, HWRevision, SWRevision, Uptime, PlannedEndOfLiveDate, ….		

Class	***InfrastructureObject***	**Namespace**	***OC***
Description	Logical representation of trackside assets such as points, level crossings, etc.		
Data elements / examples			
Properties	Model, Type, SerialNo, MaxPowerUsage, ….		
States	Ready, OutOfWork, Damaged, …		
Capabilities	Reset (taking initial position if available)		
LivecycleInfo	InstallationDate, ProprietaryID, SerialNo, SwitchCount, LastLublicationDate, ….		

Class	***TrafficabilityCategory***	**Namespace**	***OC***
Description	Abstract class that generalizes dedicated trafficability categories.		

Class	***Routing***	**Namespace**	***OC***
Description	Abstraction for all trackside routing elements.		
Data elements / examples			
InboundTrafficNodeList	List of Inbound Traffic Nodes		

Class	***InboundTrafficNode***	**Namespace**	***OC-Topo***
Description	Connector node with indication of the direction of travel. Describes a logical point where the train drives to the trackside element.		
Data elements / examples			
TrafficabilityVectorList	List of Trafficability Vectors		

Class	***TrafficabilityVector***	**Namespace**	***OC-Topo***
Description	Active element for managing trafficabiliy. Offers states and capabilities		
Data elements / examples			
OutboundTrafficNode	Outbound Traffic Node served by the Vector (destination node)		
TrafficabilityProperties	Set of properties without direction of travel dependency		
States	Free, Secured, SecuredAndLocked, n/a		
Capabilities	Secure, Lock, Release		

Class	***TrafficabilityProperties***	**Namespace**	***OC-Topo***
Description	Special kind of properties which is designed for saving direction independent		

	attributes. In normal cases, two vectors for both traffic directions between two nodes points to one instance of this class.
Data elements / examples	
Properties	physicalLength, VMaxEisen, ….

Class	***OutboundTrafficNode***	**Namespace**	***OC-Topo***
Description	Connector node with indication of direction of travel. Describes a logical point where the train leaves the trackside element (from a logical perspective).		

Class	***Protection***	**Namespace**	***OC***
Description	Abstraction for all trackside elements which have protective character		

Class	***TrackOccupancy***	**Namespace**	***OC***
Description	Abstraction for all trackside elements with capability to detect track occupation.		

Class	***TrafficabilityEdge***	**Namespace**	***OC-Topo***
Description	A track section which can influence the trafficability, such as a track occupation segment.		
Data elements / examples			
ANode	TrafficNode marking section start/end point		
BNode	TrafficNode marking section end/start point		
Properties			
States	Secured, Free, Occupied, Vacant, Failure		
Capabilities	Secure, Lock, Release		

Class	***TrafficabilityConstraints***	**Namespace**	***OC***
Description	Encapsulates temporary constraints concerning trafficability elements. Used for handling special operation modes (degradations due to temporary limitations of trackside assets).		

Class	***MovementControl***	**Namespace**	***OC***
Description	Abstraction for all trackside elements with capability to influence train movements, typically signals.		
Data elements / examples			
TrafficNode	TrafficNode marking a signal reference point. The geo-location of this point is used for representing the start point of the signal impact area.		
AspectVector	Logical vector indicating aspect visibility direction. Vector has to be configured by capturing an azimuth value.		

Class	***PositioningNode***	**Namespace**	***OC-Topo***
Description	Declares a unique position on a track. Positioning nodes are calculated with help of configured or measured geo-locations and combined with positioning information of the tracks. The UUID of positioning nodes are the interface for connecting logical nodes to the iron track network.		

Class	*Property*	Namespace	*OC*
Description	Property name value pair		
Data elements / examples			
Name	SWRevision, Type, VMaxEisen, …		
Value	1.1.3, OC-0815, 80, …		

Class	*Capability*	Namespace	*OC*
Description	Describes Capabilities of OCs, infrastructure objects and trafficability elements		
Data elements / examples			
Name	SecureTrafficability, LockSecuredTrafficability, ReleaseLockedTrafficability, Aspect1, Aspect2, Aspect3, …		
ApplicationState	Requested, Transient, Applied, n/a		

Class	*XORStateSet*	Namespace	*OC*
Description	A group of states having XOR characteristic among each other		
Data elements / examples			
Name	TrafficabilitySecurityStates, SignalAspectStates, ….		
ApplicationState	Application state. Used in cases where the capability profile would be used as active protocol for information exchange		
StateList	List of states having XOR characteristic among each other		

Class	*State*	Namespace	*OC*
Description	A state of the OC, Infrastructure Object or Trafficability Element		
Data elements / examples			
Name	Secured, SecuredAndLocked, Freed, …		
Value	Enum Value		

Class	*StateConstraint*	Namespace	*OC*
Description	Used if a state is namely applied, but with restrictions. *Remark: Level of attributes have to be worked out!*		

Class	*TrafficabilityElement StateDependendy*	Namespace	*OC*
Description	Used for applying dependency rules among trafficability elements.		

Datamodel Domains

The OC data model can be divided into a few parts that cover different logical domains.

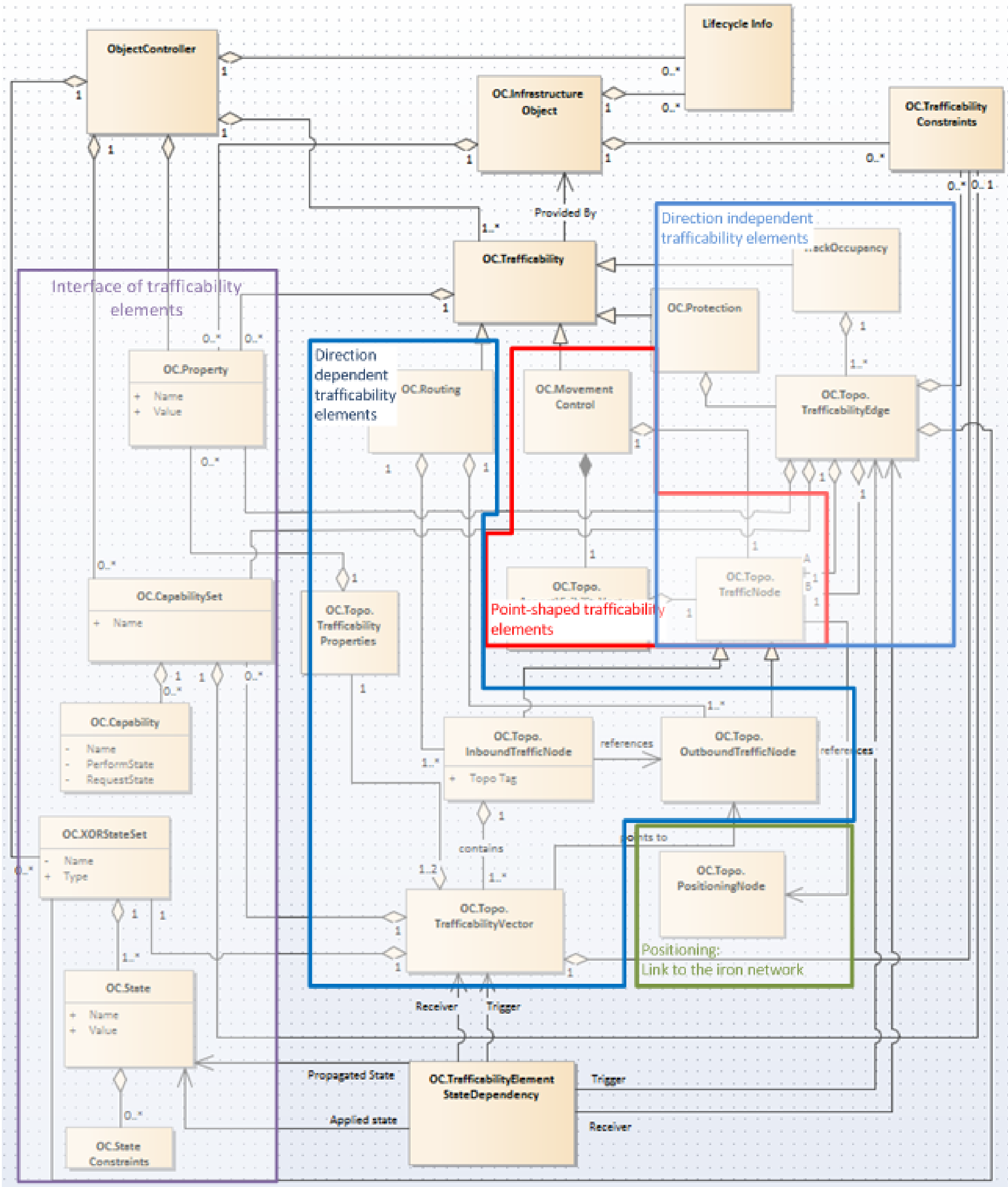


Figure 16 Data model domains

9.2 Operating Concept

The use of topological modelling in configuration is important for the operation. The configuration aspects as well as the other technical aspects of the operational concept are described in the umbrella document.

9.3 Hazards that could affect the system

Incorrect data. Any loss of integrity can have safety-critical consequences.

Incorrect data management. Incorrect data management can by implication lead to data of dubious integrity. Especially critical is the way in which changes are handled. The existence of several different, yet valid, recognised versions of the topology would pose an enormous threat to safety.

10 Sources / References

Document
OC Concept Umbrella Document
Subconcept OC TOPO
Subconcept Interlocking Switchover
Subconcept Transfer System
Subconcept Transfer System Connector
Subconcept Transfer System Module
Subconcept Configuration Profile Synchronization
Subconcept Modes of Operation and Configuration
Subconcept CP-to-L Translation
Subconcept Clear Track Signalling Installation
Subconcept Block
Subconcept Level Crossing
Subconcept Point Controller
Subconcept Signal Controller
Transitions under EI
Subconcept M-D-I-Interface
OCs in ELEKTRA_SimisW
Monitoring Concept
Subconcept - SBB W Interface OC-TA
Anforderungskatalog (V02)
OC_Hazards.xlsx
M5 Migrationsprinzip und Übergänge
M6 Bauverfahren, Gebäude, Überlagerung