European Commission

Seventh Framework programme

MODSafe Modular Urban Transport Safety and Security Analysis

Deliverable D5.1

Urban Guided Transport Object Safety Model

Contract No.	218606
Document type	DEL
Version	V1.1
Status	Final
Date	110228
WP	WP 5
Lead Author	Astrid Schindelhauer TUD
Contributors	M. Matousek TelSys
Description	Deliverable D5.1
Document ID	DEL_D5.1_TUD_WP5_110228 V1.1
Dissemination level	Public
Distribution	Consortium

Document History:

Version	Date	Author	Modification [very short description]
V0.1	25.01.2010	A. Schindelhauer	Draft of D5.1 to WP5 members
V0.2	08.09.2010	A. Schindelhauer	
V0.3	13.09.2010	M. Matousek	
V0.4	15.10.2010	M. Matousek	Comments from WP5
V0.5	8. 11. 2010	M. Matousek	Comments WP10
V1.0	29.11.2010	M. Matousek	Comments WP10
V1.1	22.02.2011	TUD / TRIT	Remaining comments WP10

Approval:

Authority	Name/Partner	Date
WP responsible	TUD	29.11.2010
EB members	WP10 Consensus	22.02.2011
Coordinator	TRIT	28.02.2011

Table of content

1. Summary of this Document 5
1.1 References 6
1.2 Terms and Abbreviations 7
1.2.1 Terms 7
1.2.2 Abbreviations 8
2. Introduction 9
2.1 Link to other MODSafe WPs 10
2.2 Purpose of Task 5.1 (Safety Object Model) 11
3. MODSafe Safety Object Model 15
3.1 Structure of the Safety Object Model 15
3.1.1 Objects, Realization Entities and UML-Modeling Constraints 15
3.1.2 Boundary, Classification, Organization of Realization Entities 15
3.2 MODSafe Safety Object Model Representation 19
3.2.1 Second Level of MODSafe Safety Object Model 19
3.2.2 Lower Levels of the Trainborne Entities Model 20
3.2.3 Lower Levels of the Wayside Entities Model 24
3.2.4 Lower Level of Central Equipments 27
4. Conclusion and Further Proceeding 28

List of figures

Figure 1 Overview over the MODSafe tasks, arranged into a V-Model like structure 9
Figure 2 MODSafe Safety Model elements split up into work packages.....11
Figure 3 Safety Integrity Influences as per D 4.1 12
Figure 4 Relation between SILs, Functions and Objects 13
Figure 5 MODURBAN system boundaries /5/ 16
Figure 6 First level grouping of Realization Entities 17
Figure 7 Colour-code of Safety Object elements 18
Figure 8 Second level classification of the Realization Entities.....19
Figure 9 Realization Entity Carborne Controller/HMI 20
Figure 10 Train Communication Object Classes.....21
Figure 11 Realization Entities of Train Doors.....21
Figure 12 Train Braking System Object Classes.....22
Figure 13 Realization Entities of Train Propulsion System and Train Power 22
Figure 14 Realization Entities of Speed and Position Measurement 23
Figure 15 Obstacle/Derailment Detection and Others.....23
Figure 16 Realization Entities of Interlocking Equipment incl. Switch Lock 24
Figure 17 Realization Entity Zone Controller.....25
Figure 18 Realization Entities of Track to Train communications 25
Figure 19 Realization Entities of Station Equipment 26
Figure 20 Realization Entities of Centralized Equipment 27
Figure 21 Preliminary Example Screenshot of Allocation Matrix.....28

1. Summary of this Document

The Work Packages WP2 (Hazards Analysis), WP4 (Safety Requirement Allocations to Functions) and WP5 are highly linked in the MODSafe project.

While WP2 analyses, what possible hazards must be mitigated in an Urban Guided Transport System, WP5 (together with WP3 and WP4) defines a set of functions that shall in fact warrant this mitigation. WP4 analyses, “how safe” a respective function shall be, by allocation of a Safety Integrity Requirement, e.g. a SIL (Safety Integrity Level), to each function. One representation of a Safety Integrity Level is, however, a maximum still acceptable rate of wrong behaviour.

Since in the real world, functions are realized, built up or supported by concrete equipments/entities, where several entities may be needed to realize a function but also several functions may share an individual entity, the questions occurs of how the “Functional” Safety Requirements may be allocated to real equipments/realization entities. The latter question shall be addressed further in task 5.3 of WP5.

To permit and support the above analysis, a typical generic model of the “Objects” - or better “Realization Entities”, which realize the functions - is required.

This deliverable consults therefore multiple detailed UML databases from urban and mainline guided transport systems and adapts the same to the scope, level of detail, Grades of Automation and functional compatibility with the other MODSafe Work Packages.

1.1 References

Reference-ID	Document title, identifier and version

/1/ DEL_D2.1_TUD_WP2_091021_V2

/2/ D2.1_Annex_Hazard_Analysis_091102_v3

/3/ D2.2_Annex_Hazard_ Analysis_100125_v4

/4/ DEL_MODSYSTEM_WP23_D127annex_TUD_080328

/5/ DEL_MODSYSTEM-D80_BVG_WP21_090317_V2-5

/6/ DEL_MODSYSTEM_WP23_D86_TUD_060914

/7/ DEL_MODURBAN-D129_RATP_WP20_090317_V27 MODURBAN GLOSSARY

/8/ COMITÉ EUROPÉEN DE NORMALISATION ÉLECTROTECHNIQUE: "EN 50126 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)", CENELEC 1999

/9/ COMITÉ EUROPÉEN DE NORMALISATION ÉLECTROTECHNIQUE: "EN 50129 Railway application – communication, signalling and processing systems – safety related electronic systems for signalling", CENELEC 2003

/10/ INTERNATIONAL ELECTROTECHNICAL COMMISSION: "IEC 62290-1 Railway applications - Urban guided transport management and command/control systems (UGTMS) - Part 1 System principles and fundamental concepts", IEC 2009

/11/ INTERNATIONAL ELECTROTECHNICAL COMMISSION: "IEC 62267 Railway Applications - Automated Urban Guided Transport (AUGT) - Safety Requirements", IEC 2006

/12/ DEL_D10.5_RATP_WP10_101005_V3, MODSafe Glossary

/13/ DEL_MODSYSTEM_D85 – MODURBAN architecture, identification of key interfaces and some preliminary FIS

/14/ INTERNATIONAL ELECTROTECHNICAL COMMISSION: "IEC 62290-2 Railway applications - Urban guided transport management and command/control systems (UGTMS) - Part 2 Functional requirement specification", IEC 2010

1.2 Terms and Abbreviations

1.2.1 Terms

Term	Description	Source
Automatic Train Protection (ATP)	The functionality which maintains the safety of train movement.	MODURBAN D85, UGTMS
Grade of Automation (GOA)	Automation level of train operation, in which Urban guided Transport (UGT) can be operated, resulting from sharing responsibility for given basic functions of train operation between operations staff and system	IEC62290-1
Operations Control Centre (OCC)	Refers to the Centre from which the traffic (and optionally additional functions) of one or several lines is supervised and managed.	MODURBAN
Realization Entity	(Physical) Objects, software components, work procedures or regulations that perform a function.	new for MODSafe
Urban Guided Transport (UGT)	Urban Guided Transport (UGT) is defined as a public transportation system in an urban environment with self-propelled vehicles operated on a guideway.	MODURBAN

1.2.2 Abbreviations

Abbreviation	Explanation
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATS	Automatic Train Supervision
CCTV	Closed Circuit Television
DoW	Description of Work
FMECA	Failure Mode and Effects and Criticality Analysis
GOA	Grade of Automation
HMI	Human Machine Interface
HW	Hardware
HVAC	Heating, Ventilation, Air Condition
I/O	Input/Output
ID	Identification
OCC	Operations Control Centre
SCADA	Supervision, Control And Data Acquisition
SIL	Safety Integrity Level
SPMU	Speed and Position Measurement Unit
SW	Software
UGT	Urban Guided Transport
UGTMS	Urban Guided Transport Management System
UML	Unified Modeling Language

2. Introduction

The European Urban Guided Transport sector (Light rails, Metros, but also Tramways and Regional Commuter trains) is still characterized by a highly diversified landscape of Safety Requirements, Safety Models, Responsibilities and Roles and Safety Approval, Acceptance and Certification Schemes. The main aim of the MODSafe project is to enhance cross acceptance of once approved and certified urban rail technologies within one country or to another countries of the European Community.

In doing so, the project MODSafe is split into work packages, which are arranged into a V-Model. On the left the Safety Analysis and modelling tasks are arranged, tasks that relate to Verification, Testing, Validation, Approval, Acceptance, Certification procedures etc. are placed at the right. The project addresses the full Safety Life Cycle of an urban guided transport system.

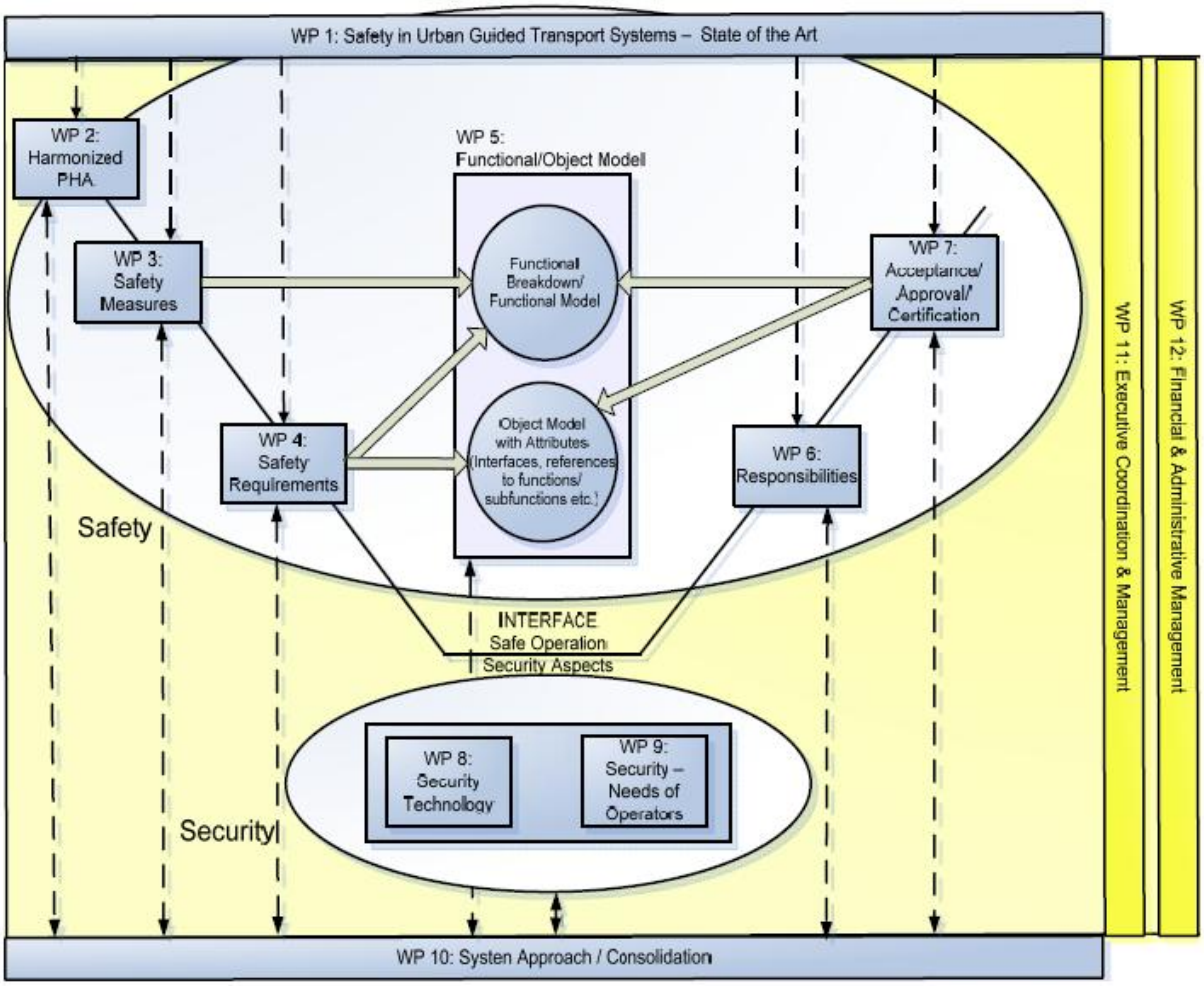


Figure 1 Overview over the MODSafe tasks, arranged into a V-Model like structure

The main purpose of the WP5 “Functional and Object Oriented Safety Model” is to combine for the first time beyond state-of-the-art not only potential Hazards, Safety Requirements and functions but link these elements to a generic functional and object structure of a Guided Transport System.

Therefore, the work package 5 is split into three tasks:

- Task 5.1: Safety Object Model
- Task 5.2: Safety Functional Model
- Task 5.3: Safety Attributes Allocation Matrix

The model develops generic objects and functions of a guided transport system. It includes elements of all major subsystems with particular focus on the control system, and within the control system on relevant objects (e.g. ATC, Interlocking).

These tasks result in three deliverables, of which the first one is presented with this document.

WP5 is highly linked to WP4 “Safety Requirements”, which results in a combined effort for the tasks 4.2 “Application of the Safety Requirement Allocation Process to MODSafe continuous Safety Measures and Functions” and 5.2 “Safety Functional Model”. According to the DoW, a separate Functional Model Document (D5.2) is created within WP5, being the same model as developed in D4.2.

2.1 Link to other MODSafe WPs

WP5 is linked to those work packages, which deal with allocation of safety measures to hazards in order to mitigate hazard evolutions. The final output “Safety Attribute Allocation Matrix” of WP5 is highly linked to the coverage of the WP2 Hazard List in order to perform the risk analysis and build the MODSafe Safety Model. Safety requirement allocation of WP4 is combined with the Functional Safety Model of Task 5.2, the Architectural Elements of WP3 and thus also associated with the Object Model.

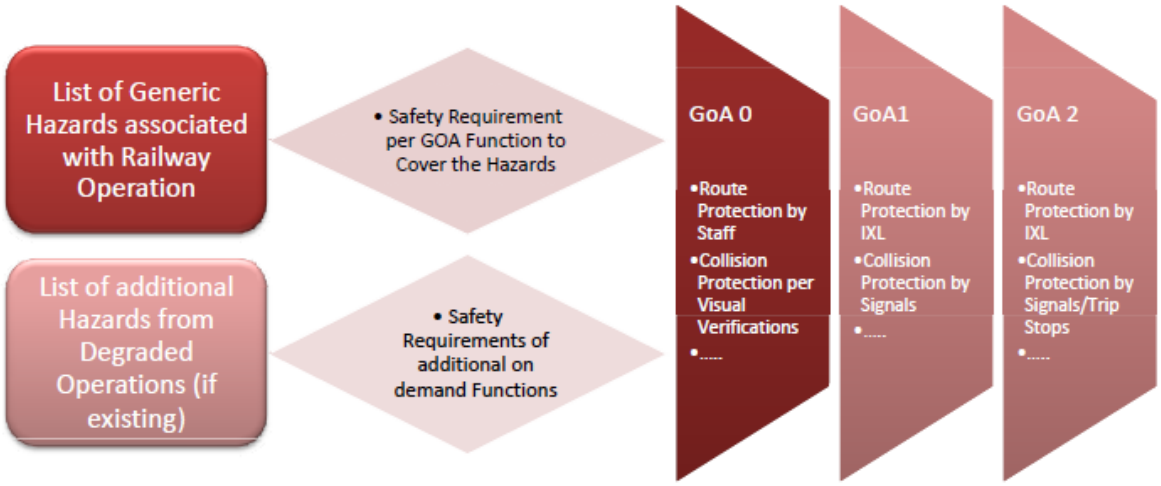


Figure 2 MODSafe Safety Model elements split up into work packages

2.2 Purpose of Task 5.1 (Safety Object Model)

Figure 2 indicates how the potential hazards identified in the analyses of WP2 are covered by safety related functions or measures. A complete set of functions had been identified jointly with WP4 and listed in the deliverable D4.2 "*Functional Model and Analysis of Safety Requirements for MODSafe Continuous Safety Measures and Functions".* The set of functions had been selected carefully in conformity with IEC 62290 Part 1 and Part 2 /10//11/.

Also in the task 4.2, the WP4 endeavors to allocate Safety Integrity Requirements to the respective functions, based on agreed risk analysis approaches.

While it is not in the scope of MODSafe to conduct a new debate about the nature and interpretation of Safety Integrity Levels as a characterization of Safety Integrity Requirements, it becomes obvious from the respective references (CENELEC EN 50126, 50129) that the notion of "Safety Integrity" includes limitations of (at least) systematic and random faults/failures as sources of wrong behaviour. The below figure indicates this relation graphically, for further discussion see *"D 4.1 State of the Art and Compilation of Results from Previous Projects".*

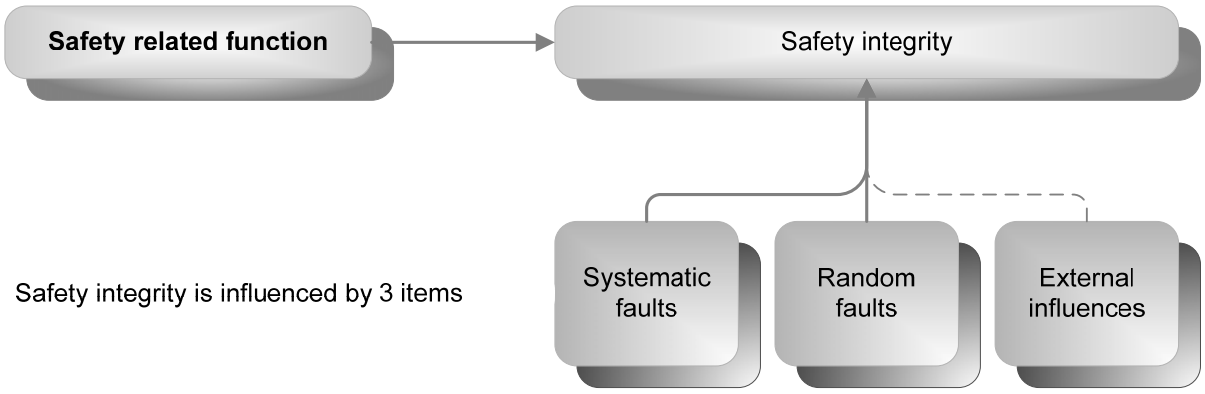


Figure 3 Safety Integrity Influences as per D 4.1

It shall be noted, that the SIL concept as one aspect of Safety Integrity associates especially with the Random Faults Categories (low) failure rates for possible wrong side failures of an entity or function that shall not be exceeded by the entity or function. Should “random” or “statistical” rates not describe plausibly the nature of a fault, then an equivalent level of safety shall be sought by alternative, equivalent systematic measures.

The most common safety requirement allocation process practised today in the European Union and also followed in this project (D4.2) consists in allocating a Safety Integrity Level to a “Function”, meaning that the safety capacity of this function shall not more often fail (and leading subsequently to unsafe system behaviour) than prescribed by the respective SIL/THR.

Consider now in particular the “rates”-based SIL (SIL-THR Table) concept, being implicitly based on the idea of statistically constant, independent rates of failure (often expressed as exponential density function over time).

Then, by inspection of a more complicated real ATP or Interlocking architecture three difficulties in further management of the Safety Requirements become obvious:

- Any of the “Functions” is in fact realized by multiple objects and/or sub-functions
- Vice versa, any of the constituents (objects) realizes in general not only one particular function but multiple functions.
- When thinking of “Constant” failure rates, it must be noted that in physical reality constant failure rates are a rather rarely observed “idealization” of more complicated density functions such as Weibull distributions. In any event, “failing” with a constant rate is an artefact of a physical entity (or object) rather than of any of the functions that may be realized (or not) by the entities. On the other hand it is clear, that in almost all cases a direct correlation between the wrong side failure of a function and

the wrong side failure of any of the object constituents of the function may be found. Other elements such as Software or Procedures are clearly insufficiently described by “constant rates”.

The figure below shall indicate graphically these observations.

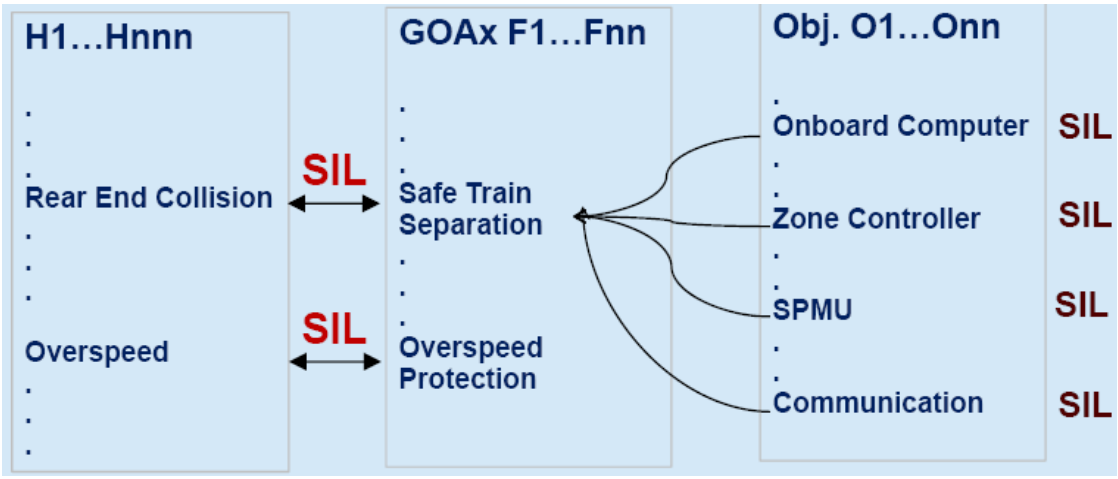


Figure 4 Relation between SILs, Functions and Objects

From above considerations, the question remains of how to break the higher architecture level functional SIL consistently down to the lower parts and/or into the objects/entities realizing the functions.

One way could consist in directly allocating Safety Requirements/SILs to the objects at intermediate level of complexity. This direct approach had not been followed in MODSafe due to the fact that Functional Safety Architectures are more common in Safety Requirement discussions and that it is more straightforward to verify, that a Functional Architecture “covers” completely the hazards identified in the Hazard Analysis.

A second approach could consist in directly analysing objects (or Realization Entities), estimating their wrong side failure behaviour statistics, build a function from these realization entities and verify that the result matches high level of safety requirements. As a supporting argument, it can be observed that Safety Cases produced today include often Generic Safety Cases of Safety Equipments such as a Controller or an Onboard Device, and these safety cases analyse often in fact through (reliability) Fault Trees and FMECAs aggregated wrong side failure rates. It shall be noted, however, that also in this process the designers must receive before concept a clear idea of how “safe” the equipments shall be. A systematic

coverage of all hazards identified during system hazard analysis cannot be demonstrated with this approach.

Therefore, within MODSafe a top down allocation of safety requirements from the functions to the objects is attempted and researched. The resulting model, the difficulties in allocation and the allocation itself will be subject of Deliverable D5.3.

Since the functions are taken from the model in D4.2 and D5.2 and the SIL inputs into the model are also taken from deliverable D4.2, only typical “objects” are missing at this time to continue the analysis.

Therefore, the task of this deliverable contains the analysis of a model of typical, generic objects that build the considered functions or generic architectures.

The selection of these “objects” is at first independent of the respective Grade of Automation, since certain objects may be used equally well in one or the other architecture or GOA, but of course not all found objects in this “overcomplete” model will be found in every GOA. A selection of what object may emerge in what GOA may be performed in the deliverable D5.3.

A second issue coming from discussions in the WP5 and WP4 teams concerns the question of the “nature” of the “objects”. While a resistor or a transponder may be clearly considered as the representative of an Object or a Class of Objects, this is less obvious for constituents like SW Modules for example (or systems of HW and SW).

Therefore, the more general notion of “Realization Entities” is utilized throughout the task as a synonym notion to “object”.

The challenge of this task is to define an appropriate level of Objects/Realization Entities that appears adequate for the later task of Safety Requirement Allocation, remains generic, are still typical for the respective architectures (MODURBAN D85) and does not get too complex (see chapter 3)

This deliverable yields a reduced, generic and typical Safety Object Model that may be used in further analysis.

3. MODSafe Safety Object Model

The Safety Object Model shall include typical elements that build up the safety functions during operation of the Urban Guided Transport System. Other elements (i.e. elements not building up safety functions) of a transport system had not been considered, since they do not further contribute to the methodology, are not in line with the D85 architecture or are not adequately characterized by SILs (eg. mechanical parts). The safety functions as such are however not sufficient to define the boundary for the Object Model (otherwise it would be redundant).

3.1 Structure of the Safety Object Model

3.1.1 Objects, Realization Entities and UML-Modeling Constraints

As observed in the previous chapter, the elements that shall be incorporated into the final allocation matrix of functions and objects are not confined exclusively to classic “objects” but are extended to other relevant entities, in summary called “Realization Entities” in this project, and as simplification further on simply “Objects”.

In stricter, semi-formal definitions such as UML (in computer science) “Objects” are commonly “Representatives” or “Instances” of “Classes” that may in turn be “associated” amongst each other by “links”.

“Classes” are related to each other by “Aggregations” (where the aggregated classes may also exist alone) or “Compositions” (where mostly class existences condition each other), and “Attributes” that may follow inheritance rules.

Furthermore, it has been found useful during the discussions of the project task to sometimes drop detailed differentiation between “Classes” and “Objects” and “Aggregations/Compositions” for better readability. It is however the intention to maintain formal characteristics of the investigated Objects as much as possible, such as “Identity”, “State”, “Attributes”, “Behavior”, etc.

3.1.2 Boundary, Classification, Organization of Realization Entities

To better find a possible Boundary Line and to stay consistent with other models in and before MODSafe for the Object Model, the task relates the analysis work to the MODURBAN D80 (‘*Comprehensive operational, functional and performance requirements*’ /5/) definitions and identifies accordingly major groups of equipments such as the traction power system, track, station equipment, passenger information system, communication system, control/command and supervision of train movement system.

During further refinement of the highest level (UGT) model, the focus had given mainly to those objects, that are likely to correspond to the functions of D4.2/D5.2 – which are in turn coming from the IEC 62290 definitions /10//11/– and therefore elaborate mainly transport management (control, command) functions (but not exclusively). Where adequate, the model follows the notations of the D85 entities.

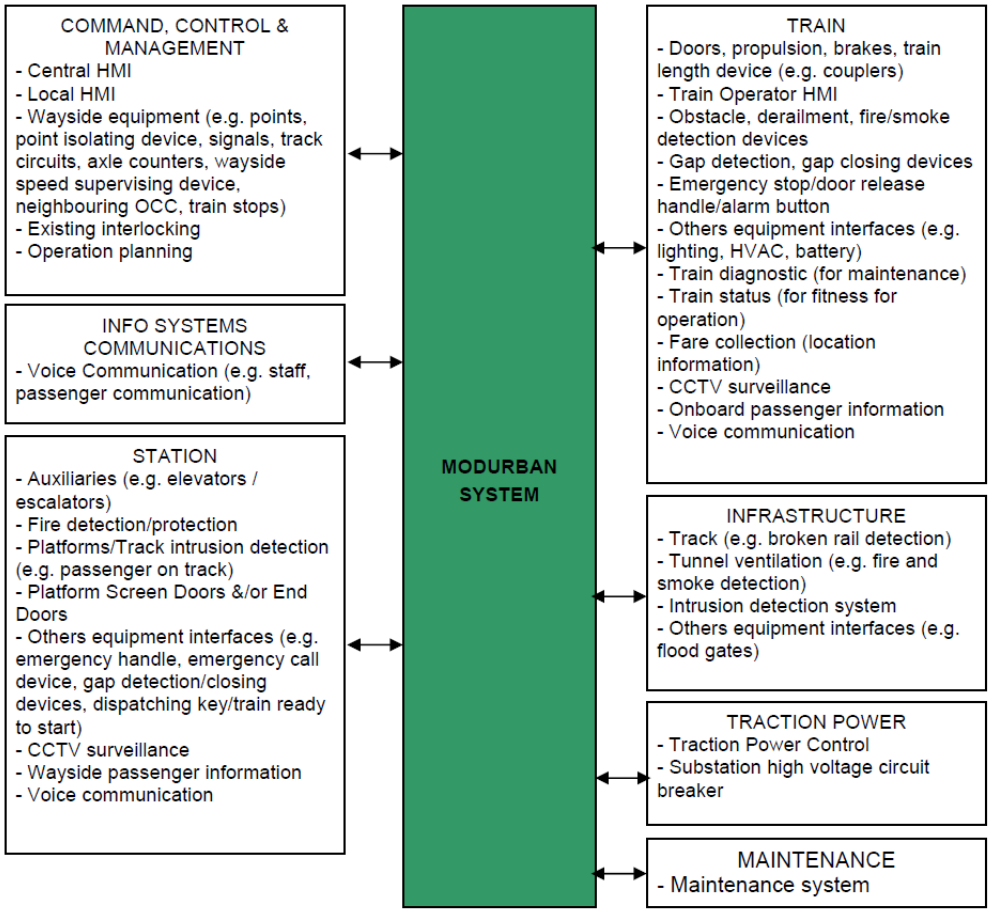


Figure 5 MODURBAN system boundaries /5/

The elements of the Safety Object Model are subsequently arranged at the highest level in a comprehensive “geographic” way that facilitates the user’s orientation. Figure 5 classifies system elements in seven clusters, motivated by either functional or local aspects.

At previous UML modeling work at TUD of Train Control Architectures it had been found that different categorization parameters may be selected.

- Entities could, for example, be organized according to typical Functional Procurement Lots, like ATO, ATP, ATS, Telecom, Trains, SCADA etc. Then, at lower levels, entities (like e.g. a Wayside Controller) may contribute to different Groups. Also, entities at lower levels may be distributed over several locations like wayside, onboard of trains, etc. The result of these hierarchies becomes therefore often rapidly a mixture of “location” where an object is installed, and “functional coherence” (logical architecture of Objects) of a component with other components. The above representation in figure 5 is a typical example of these mixtures, where the classes do not necessarily join fully the attributes but mix locations (“Stations”, which are not themselves objects but “locations” where our objects are placed), Lots (“Traction Power”, which comprises Objects at different locations), functions (“Command and Control” is an attribute common to the different equipments at different locations under this functional group).
- Alternatively, the location of where an object performs its functions can be selected. Disadvantage of this organization becomes also evident at levels of increasing detail, e.g. when a Train Separation System is distributed by its objects over the train (onboard controller), the wayside (wayside control unit) and the track-train communication in the track area. It appears, however, intuitively for most parties the “clearer” categorization (which is also observable from the above figure since most groups denote implicitly a geographic location).
- Also, lot wise grouping as for example used in implementation contracts may be used and represent often a mixture between functional coherence and location.

Derived from the debate and above input, the MODSafe Safety Object model defines at the first (highest) level three groups of Realization Entities,namely Trainborne Entities, Wayside Entities and Operations Control Centre (OCC) according to their location (Figure 6). The OC covers functions performed on both trainborne and wayside locations.

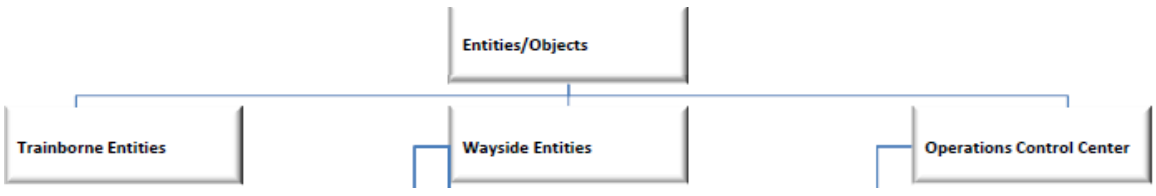


Figure 6 First level grouping of Realization Entities

While the class definition is not mandatory, it may be easily transferred into any other class definition, because the classes are not more than ordering parameters. Oriented on

locations, the differentiation into equipments associated with the trains, and equipments organized into some proximity to the track (wayside) appears convenient. Also for convenience, the central equipments normally organized around the Operations Control Center had been arbitrarily separated. The categories are then further refined into subclasses of increasing detail.

The resulting tree structure had been colour coded to differentiate two cases:

- When a class of objects (or: the object) reaches the final level of generic detail and is retained, then the Entity is considered a “Terminal Entity” and the colour code is “BLUE.”
- When an object class has not reached the terminal level of detail, or is not retained for further 5.3 analysis or is intended to only show possible other example entities (generic or not generic) to better situate the context, then the element is shown in “WHITE”. Note, that after internal MODSAFE review, the majority of levels of detail and examples had been suppressed, so only the minimum of white elements are retained that are necessary to clarify the links and context.

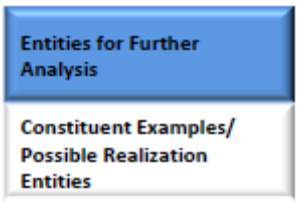


Figure 7 Colour-code of Safety Object elements

The discussion of what level of detail of the MODSafe Safety Object Model shall be used for further analysis examples remains in the discretion of every individual user. It shall be noted, however, that the degree of complexity is rapidly increasing with the considered level of detail. Should for example 20 functions be spread against 20 objects in two GOAs, then 800 individual combinations require adequate reflection. Should, instead, 80 functions are considered against 80 object classes for four GOA, then 19.200 individual combinations must be considered.

For the examples in task 5.3, only the Blue elements are kept.

3.2 MODSafe Safety Object Model Representation

3.2.1 Second Level of MODSafe Safety Object Model

In this chapter, the MODSafe Safety Object Model is described and given in a tree like aggregation structure representation according to the remarks in previous chapters.

After the first level location based classification into Trainborne Entities, Wayside Entities and Operations Control Center Entities, a next level of object classes is yielded by division into subgroups which will be further developed (see Figure 8).

At this second level of detail, the confinement to safety relevant entities is already clearly recognizable. While the Wayside Entities are broken down into the classic wayside subsystems (Wayside ATP, Interlocking) also other Object Classes are prepared for completeness like Traction Power, Station Equipments, Tunnel and Depot Equipments etc.

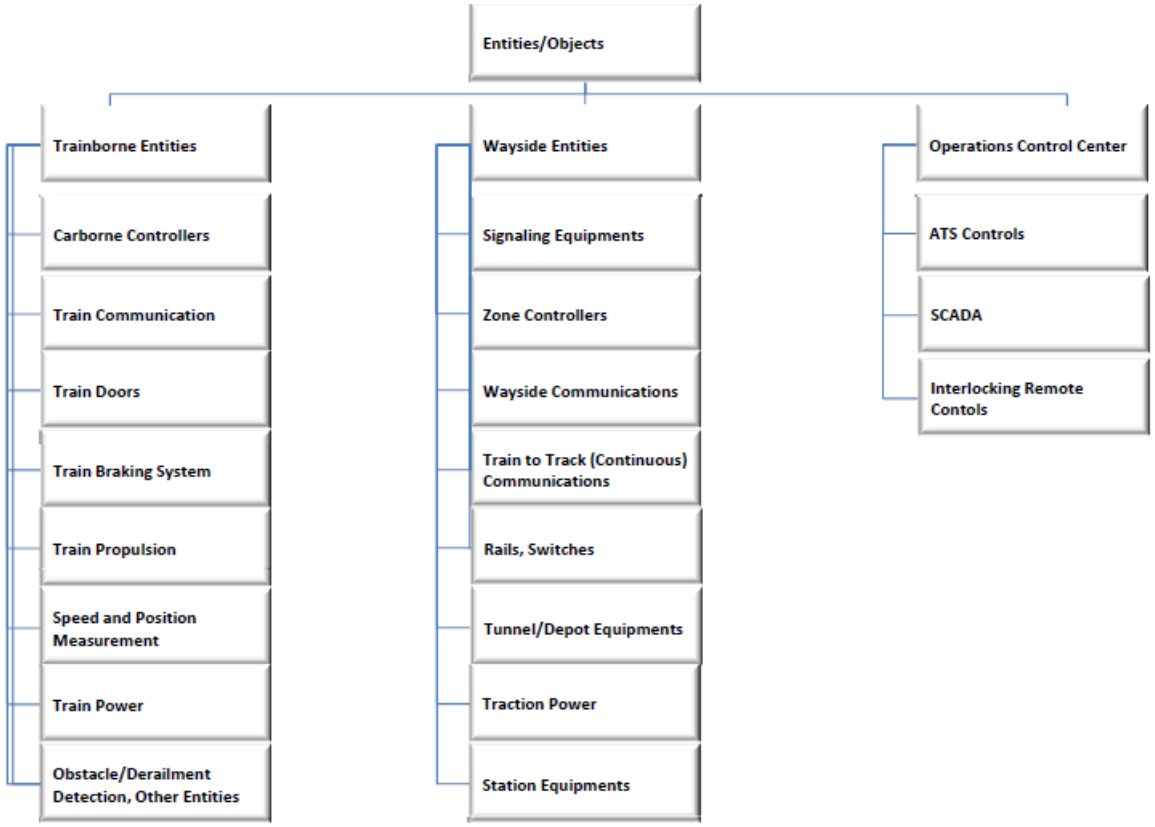


Figure 8 Second level classification of the Realization Entities

Similarly, the trainborne equipments contain the directly comprehensible safety subsystems as Carborne Controllers, Speed and Position Measurement or Obstacle Detection but also preparations of other classes like Doors, Train Power etc. that are likely to contain safety relevant entities at more detailed levels.

For Centralized Equipments, the Remote Control for Interlocking Equipments is kept, as well as (possibly “safe”) ATS equipments and the SCADA (for Traction Power Shut Down). CCTV equipments, Audio Control or Telephones etc. are organized under the ATS.

3.2.2 Lower Levels of the Trainborne Entities Model

The following tree structures represent a further break down of the trainborne entities (Figure 9 to Figure 20).

At the third level of detail, below the first sequential entity – Carborne Controller – several sub classes could be imagined, but after internal discussions only two where retained: the Carborne Controller without further breakdown and the driver HMI, also without further breakdown.

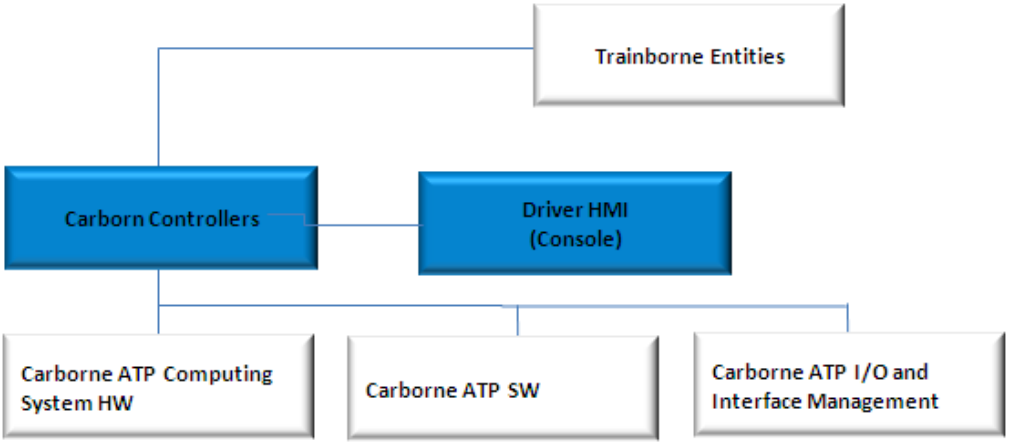


Figure 9 Realization Entity Carborne Controller/HMI

Although it is obvious that a possible SIL allocation to a Driver HMI as such would require further breakdown of this class to those elements that in fact pertain to safety, no further level of details found acceptance in the MODSafe project team.

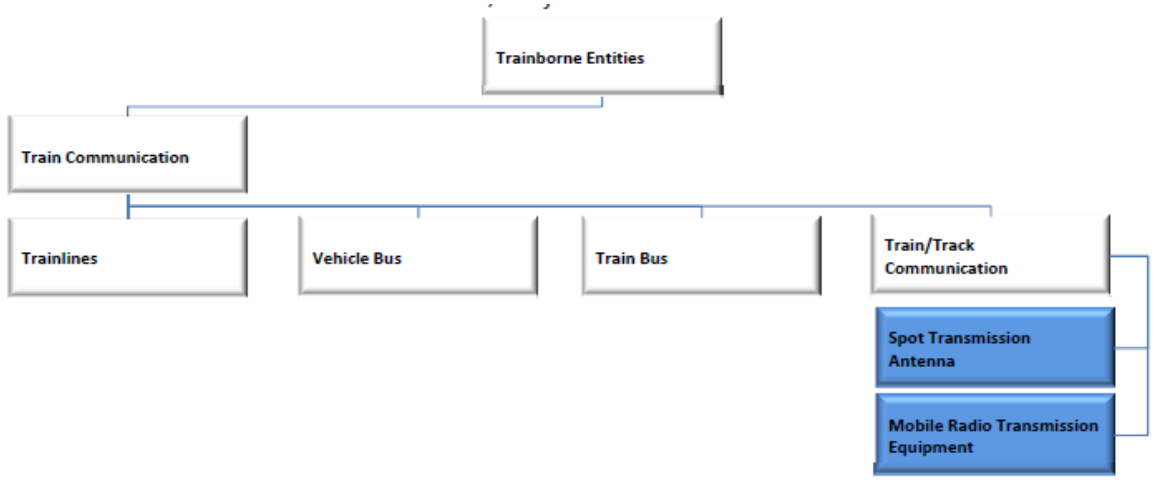


Figure 10 Train Communication Object Classes

For the refinement of the Object Class “Train Communication”, only the interfaces to the Track/Train communication - the Spot Transmission Antenna objects attached to the train for spotwise communication, and the Mobile Radio Transmission onboard equipments - had been kept for further analysis, other entities are just shown to remind of additional example objects that may be taken into account for specific analyses.

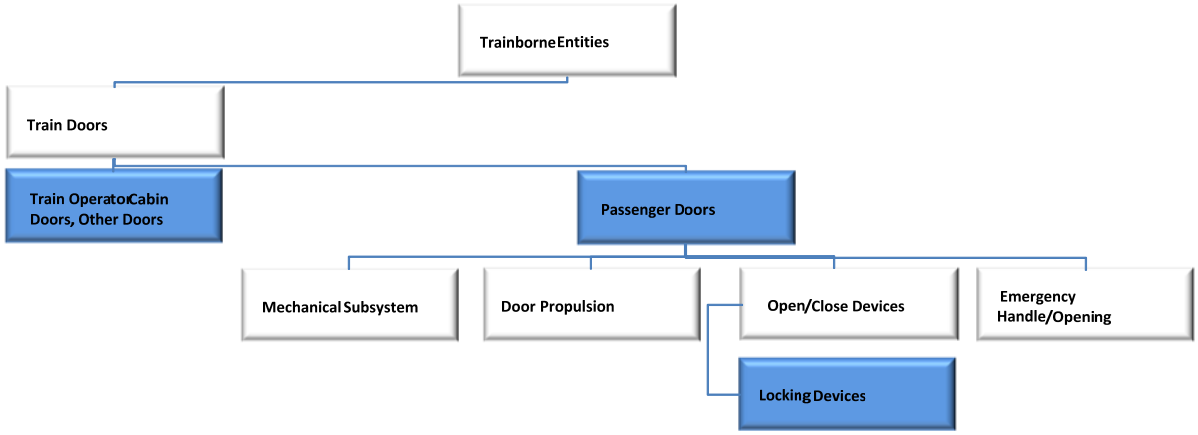


Figure 11 Realization Entities of Train Doors

On the door subsystem, the locking device of the passenger doors had been retained for further analysis as an important example of safety relevant elements associated with the doors.

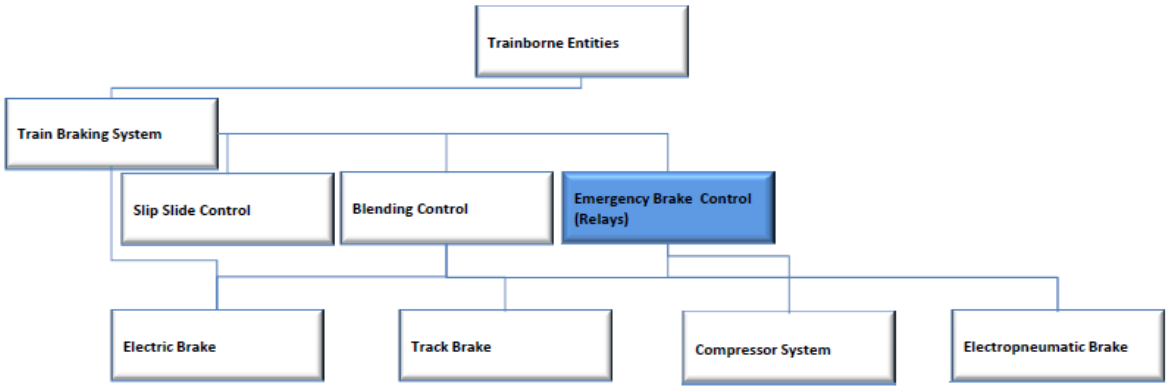


Figure 12 Train Braking System Object Classes

On the track braking system, only the interface to command/control was kept for further analysis since the examples of WP5.3 for methodology clarification avoids to open debates that are outside the scope of MODSafe, such as what a SIL for mechanical objects in the braking system could be.

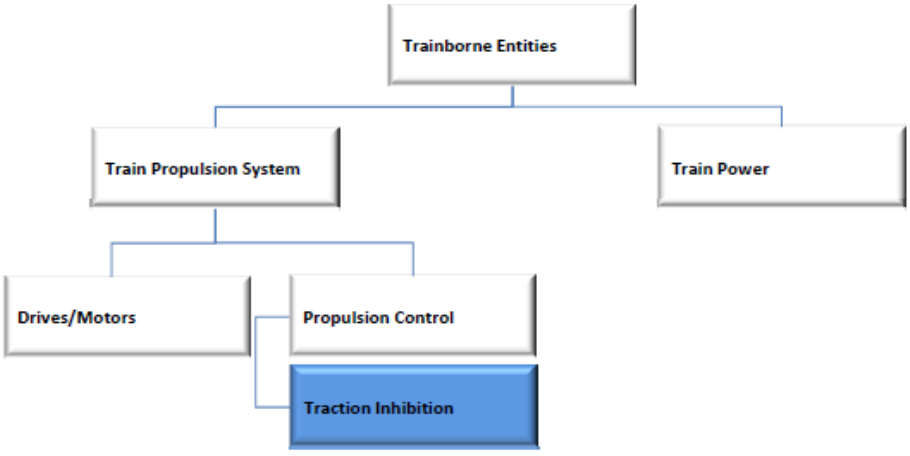


Figure 13 Realization Entities of Train Propulsion System and Train Power

Similar to the Train Braking System, also the Train Propulsion System (and Train Power) was reduced for further analysis to the (safe) inhibition of the train traction in case of Emergency Braking. Retaining other elements, such as the traction drives itself, would yield questions outside of the MODSafe scope, such as what a SIL for a motor could possibly be.

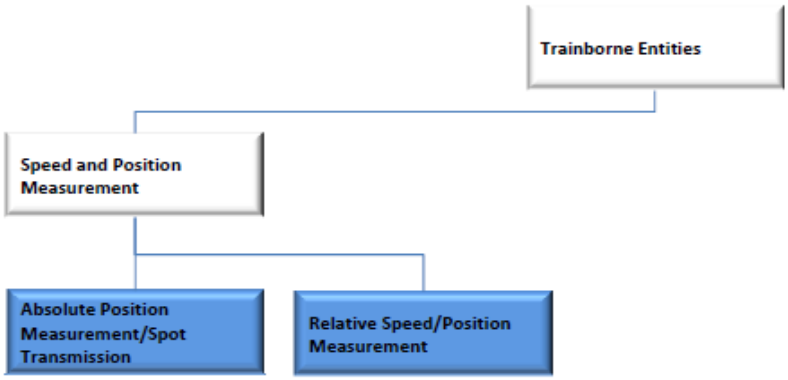


Figure 14 Realization Entities of Speed and Position Measurement

The speed and position measurement had been further developed into the two basic equipment classes for relative and for absolute position measurement. The absolute position measurement is associated with the D85 concept of spot transmission.

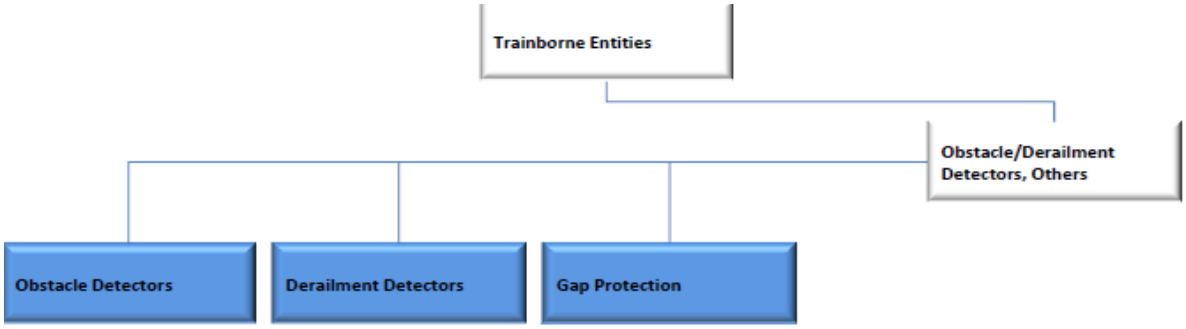


Figure 15 Obstacle/Derailment Detection and Others

A last Object Class for possible safety related onboard equipments aggregates realization entities that are in particular found in (but not be limited to) higher Grades of Automation.

Without going further into detail, the “Obstacle Detector”, “Derailment Detector”, “Gap Protection” (if part of train) are retained for further analysis.

3.2.3 Lower Levels of the Wayside Entities Model

At a generic level, the wayside safety architectures are constituted by wayside ATP entities (here Zone Controllers) and Signalling equipments including the Interlocking and the corresponding peripherals. It is therefore not surprising to find particularly on the Interlocking side larger aggregations of equipments. All lower level Object Class trees of the wayside equipments are shown and discussed throughout Figure 16 to Figure 19.

As for the Trainborne Equipments, the Object Classes are shown directly in the suggested reduced form.

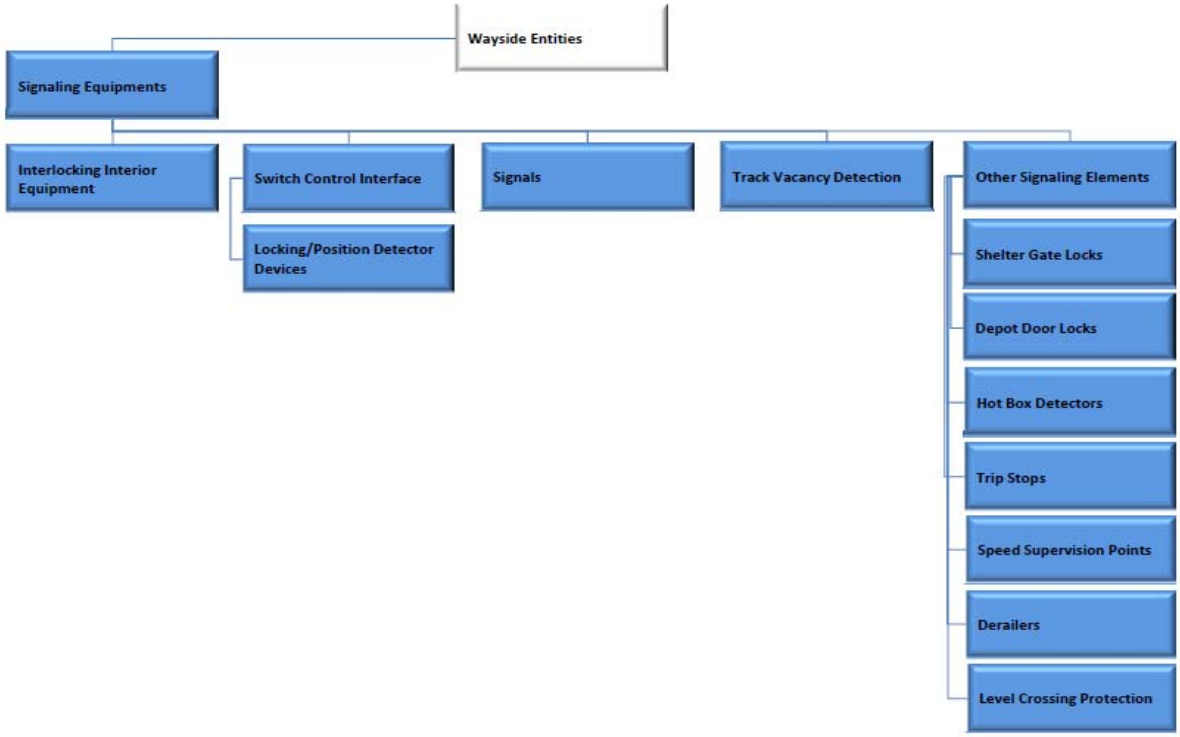


Figure 16 Realization Entities of Interlocking Equipment incl. Switch Lock

The Signalling Equipments/Interlocking contains or is associated with a larger number of clearly relevant entities, which are either part of the signalling or at least interfaced with the interlocking (like shelter gate locks). Within D5.1 all shown entities are kept since it is assumed that in particular lower GOAs are largely based on these; should simplifications be adequate, it will be performed in task 5.3.

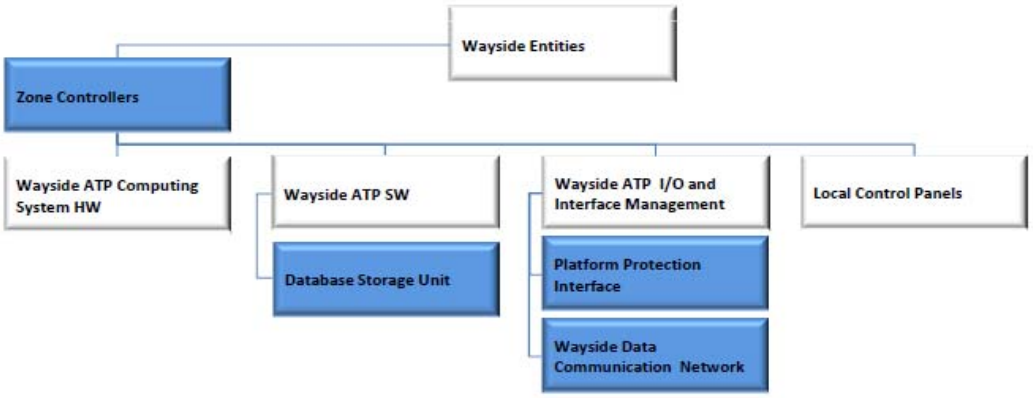


Figure 17 Realization Entity Zone Controller

The Zone Controller is kept as the major wayside safety element besides the interlocking, including some more detailed entities such as interfaces to other wayside elements. For task 5.3 allocation works, it may be sufficient to consider only the Zone Controller itself.

The Object Class refinement of “Track to Train Communications” (here the wayside perspective) contains essentially a spot transmission (transponder) class and a continuous track to train communication class. Besides the many possible technical implementations of the latter class (like inductive transmission), only the wayside radio transmission was kept upon advice of the MODSafe team. The Wayside Data Transmission interface has also been associated.

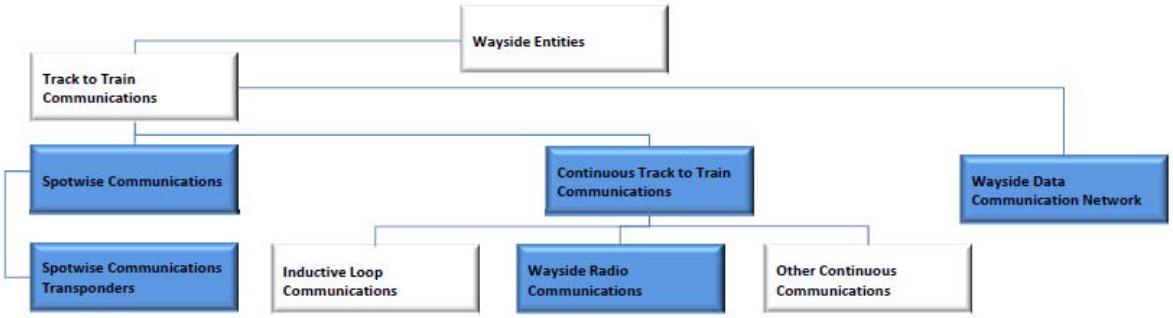


Figure 18 Realization Entities of Track to Train communications

Concerning other equipments along the track, two classes are shown in one tree structure together, other “Tunnel/Depot Equipments” and “Traction Power Equipments”.

While it could well be argued that e.g. inappropriate “Emergency Walkways” or wrongly closed “Depot Doors” may lead to potentially unsafe situations, the task kept in particular the Traction Segment Shutdown as a critical element to evacuation (and maybe other functions). Should further analysis show that the allocation process to other simultaneously active equipments is different from the power shutdown equipment or hazards appear that require other particular equipment combinations, then the selection will be extended as necessary (unproblematic).

On the Station Equipments, basic categories such as the platform track protection system in higher GOAs or the gap (between train and platform edge) protection (if implemented wayside) had been retained for further analysis. Since the MODSafe team insisted on generic character of the models wherever possible, no technical implementation such as Intrusion Detection Systems or Platform Screen Doors had been detailed but can be easily performed individually in the future.

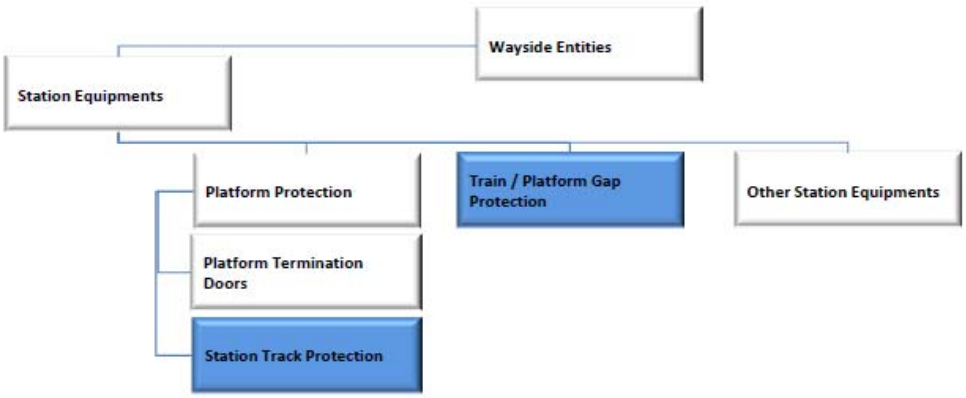


Figure 19 Realization Entities of Station Equipment

3.2.4 Lower Level of Central Equipments

The below indicated Operations Control Center Object Classes summarize all those installations that are typically installed in an OCC, from which traffic shall be monitored and from where fleet and traffic mode commands are issued, but also some command that pertain to objective safety.

While of course also Interphone Communications or Elevator Controls may have an impact on safe traffic management, and in particular in emergency situations, it is not common to assign a Safety Integrity Level to these entity classes, since mostly special risk analysis is performed, a high level of (functional) redundancy is given, and the safety related activities pertain to irregular situations (such as mass panic or evacuations).

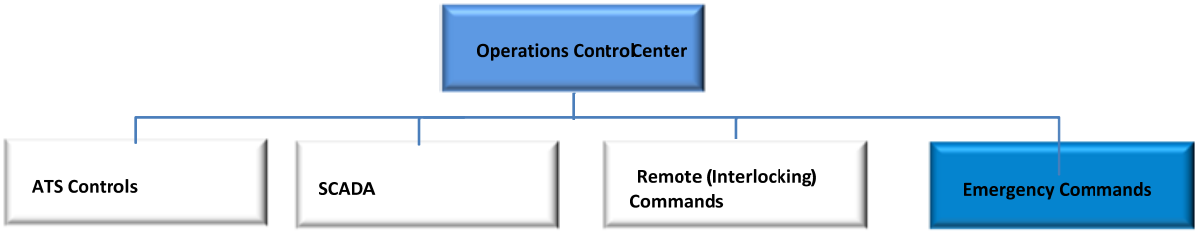


Figure 20 Realization Entities of Centralized Equipment

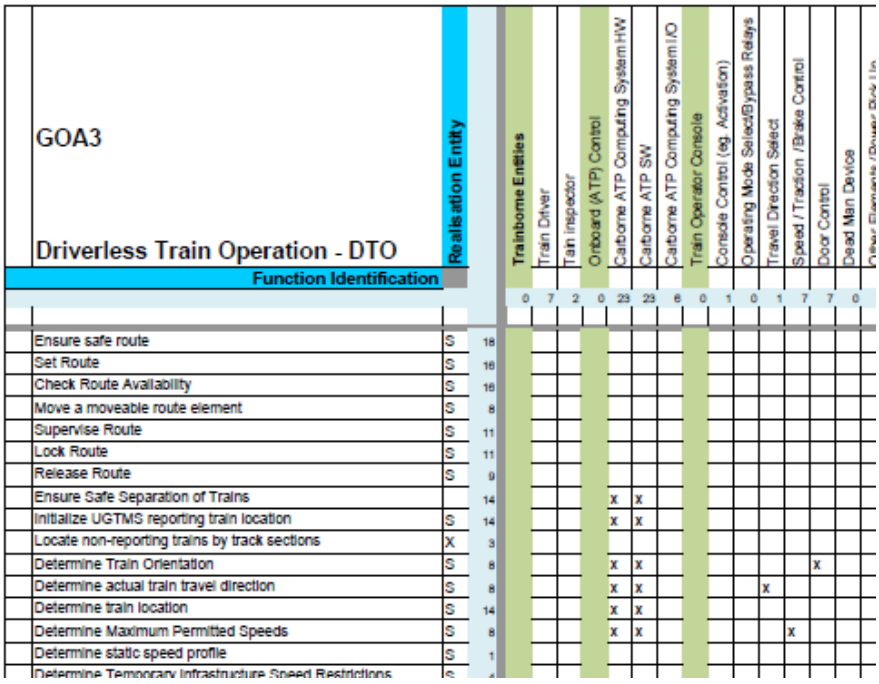
After advice of the MODSafe team to stay at higher levels of detail, the Operations Control Center level was not further broken down into partial equipments.

4. Conclusion and Further Proceeding

The deliverable shows, that it is possible by relatively straightforward considerations and analyses to derive a plausible Object Model for those entities that typically build up the Safety Functions analysed in D4.2/5.2.

For better readability some representation simplifications compared to the constraints of UML are advised and, in order to stay generic, only in rare and argued cases concrete implementations of the Object Classes where retained.

Since in a next step the Safety Objects are related to the Safety Functions (see example table part below) for Grades of Automation, it is recommended to keep the considered Object Classes at a manageable number, not using every level of detail. A possible selection is indicated by colour code in the deliverable.



GOA3 Driverless Train Operation - DTO Function Identification	Realisation Entity		Trainborne Entities	Train Driver	Train Inspector	Onboard (ATP) Control	Carborne ATP Computing System HW	Carborne ATP SW	Carborne ATP Computing System I/O	Train Operator Console	Console Control (eg. Activation)	Operating Mode Select/Bypass Relays	Travel Direction Select	Speed / Traction / Brake Control	Door Control	Dead Man Device
			0	7	2	0	23	29	6	0	1	0	1	7	7	0
Ensure safe route	S	18														
Set Route	S	16														
Check Route Availability	S	16														
Move a moveable route element	S	8														
Supervise Route	S	11														
Lock Route	S	11														
Release Route	S	9														
Ensure Safe Separation of Trains		14					x	x								
Initialize UGTMS reporting train location	S	14					x	x								
Locate non-reporting trains by track sections	X	3														
Determine Train Orientation	S	8					x	x						x		
Determine actual train travel direction	S	8					x	x					x			
Determine train location	S	14					x	x								
Determine Maximum Permitted Speeds	S	8					x	x						x		
Determine static speed profile	S	1														
Determine Temporary Infrastructure Speed Restrictions	S	4														

Figure 21 Preliminary Example Screenshot of Allocation Matrix