SEVENTH FRAMEWORK PROGRAMME

MODSafe

European Commission
Seventh Framework programme
MODSafe Modular Urban Transport
Safety and Security Analysis

Functional Model and Combined Object/Functional Guided Transport Model

Deliverable No. D5.2

Contract No.	218606
Document type	DEL
Version	V2.1
Status	Final
Date	26. April 2011
WP	WP 5
Lead Author	WP 5
Contributors	WP 5 partners
Description	Safety Functional Model, Object Linking UML
Document ID	DEL_D5.2_TUD_WP5_110426_V2.1
Dissemination level	PU (not annex)
Distribution	MODSafe Consortium

Document History:

Version	Date	Author	Modification
V1.0	24. January 2011	WP 5	New document
V2.0	18. February 2011	WP5	Accounting for WP10 comments
V2.1	14. March 2011	WP10	Accounting for additional WP10 comments

Approval:

Authority	Name/Partner	Date
WP responsible	TUD	14. March 2011
EB members	WP10	15. March 2011
Coordinator	TRIT	17. March 2011

Table of contents

1 Summary of the document

This document contains the MODSafe safety functional model. The safety functions are taken primarily from the IEC 62290 part 2.

This functional model of the safety functions is used in the MODSafe deliverables D2.3, D3.2, D4.2, D4.3 and D5.3.

2 Bibliography

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

Note 1: For the compilation of MODSafe deliverable 5.2 the CDV (committee draft for vote) of IEC 62290-2 was available only.

Note 2: IEC 62290 is a draft European standard (prEN).

[2] MODULAR URBAN TRANSPORT SAFETY AND SECURITY ANALYSIS: "Deliverable 2.3 MODSafe Risk Analysis", MODSafe WP2 (not yet published)

[3] MODULAR URBAN TRANSPORT SAFETY AND SECURITY ANALYSIS: "Deliverable 3.2 Final Hazard Control and Safety Measures Analysis", MODSafe WP3 (not yet published, planned 2011)

[4] MODULAR URBAN TRANSPORT SAFETY AND SECURITY ANALYSIS: "Deliverable 4.2 – Analysis of Safety Requirements for MODSafe Continuous Safety Measures and Functions", MODSafe WP4 2011

[5] MODULAR URBAN TRANSPORT SAFETY AND SECURITY ANALYSIS: "Deliverable 4.3 – Analysis of on demand functions and systematic failures", MODSafe WP4 (not yet published)

[6] MODULAR URBAN TRANSPORT SAFETY AND SECURITY ANALYSIS: "Deliverable 5.1 – Safety Object Model", MODSafe WP5 2010

[7] MODULAR URBAN TRANSPORT SAFETY AND SECURITY ANALYSIS: "Deliverable 5.3 – Safety Attributes Allocation Matrix", MODSafe WP5 (not yet published, planned 2011)

3 Terms and abbreviations

3.1 Terms

Term	Definition	Reference
Driving mode	A driving mode describes how a train should be driven in a defined situation and can be performed either by an acting driver or automatically	UGTMS
Movement authority	Permission for a train to run, within the constraints of the infrastructure, up to a specific location.	IEC 62290-2
Non-operative UGTMS trains	Non UGTMS equipped trains and trains with inoperative UGTMS equipment.	IEC 62290-2
Operations control centre	Centre from which operation of the line or the network is supervised and managed	IEC 62290-1
Reporting train	UGTMS equipped trains able to report its location and other relevant information.	IEC 62290-2
Safety function	Function to be implemented by an E/E/PE safety-related system or other risk reduction measures that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.	IEC 61508-4
Safety measure	Means a set of actions either reducing the rate of occurrence of a hazard or mitigating its consequences in order to achieve and/or maintain an acceptable level of risk.	Commission regulation (EC) No 352/2009
Zone of protection	A zone where no train is allowed to run as a response to various kinds of incidents.	IEC 62290-2

3.2 Abbreviations

Abbreviation	Definition
AC/DC	Alternating current/direct current
D	Deliverable
IEC	International electrotechnical commission
OCC	Operations control centre
MODSafe	Modular urban transport safety and security analysis
Nr	Number
UGTMS	Urban guided transport management and command/control systems
UML	Unified modelling language
WP	Work package
XMI	XML (extensible markup language) metadata interchange

4 The MODSafe safety functional model

The origin for the majority of the MODSafe safety functions is the international standard IEC 62290 part 2 [1]. The functional model itself, however, is developed within MODSafe WP 4 for the purpose of the deliverable 4.2 [4] and upcoming MODSafe deliverables. For MODSafe purposes the IEC 62290-2 functions are amended and adjusted.

This MODSafe safety functional model is used in MODSafe deliverables:

- D2.3: MODSafe risk analysis [2]
- D3.2: Final hazard control and safety measure analysis [3]
- D4.2: Analysis of safety requirements for MODSafe continuous safety measures and functions [4]
- D4.3: Analysis of on demand functions and systematic failures [5] and
- D5.3: Safety attributes allocation matrix [7].

Note: the cross linking between objects model (cf. [6]) and functional model will be part of MODSafe deliverable 5.3 [7].

5 List of functions

5.1 Ensure safe movement of trains

5.1.1 Ensure safe route

Nr.	Name of safety function	Description	Reference
1	Check route availability	For the route to be set, the conflict free availability of all determined route elements shall be checked.	IEC 62290-2 5.1.1.1.1-3
2	Set route	This function is intended to set a route by command provided by operation control HMI or by the function set routes automatically.	IEC 62290-2 5.1.1.1.1
3	Supervise route	This function is intended to supervise that all conditions for the route are still in place.	IEC 62290-2 5.1.1.1.2
4	Supervise level crossing as secured	This function is intended to supervise that a level crossing is secured and locked in order to forbid its conflicting use by general road and pedestrian traffic.	New for MODSafe
5	Lock route	This function is intended to lock the route against route release by operator command if a train is approaching and the movement authority allows entry into route, or a train is within the route.	IEC 62290-2 5.1.1.1.3
6	Release route	This function is intended to release a route and its elements.	IEC 62290-2 5.1.1.2

5.1.2 Ensure safe separation of trains

Nr.	Name of safety function	Description	Reference
7	Initialise UGTMS reporting trains location	This function is intended to initialise the location of reporting trains which are: • stationary in stabling locations • entering UGTMS territory • recovering from localisation failures	IEC 62290-2 5.1.2.1
8	Determine train orientation	This function is intended to determine the physical orientation of the train relative to the defined orientation of the track.	IEC 62290-2 5.1.2.2.1
9	Determine actual train travel direction	This function determines the travel direction of trains.	IEC 62290-2 5.1.2.2.2
10	Determine train location	This function is intended to determine the location of all UGTMS equipped trains according to the train orientation and train length.	IEC 62290-2 5.1.2.2.3
11	Locate non reporting trains by track sections	This function is intended to determine the location of non reporting trains using external devices.	IEC 62290-2 5.1.2.3

5.1.3 Determine permitted speed

Nr.	Name of safety function	Description	Reference
12	Determine static speed profile	This function determines the static speed profiles, which are based on infrastructure data such as track geometry and quality, infrastructure constraints (tunnels, bridges, platforms, etc.).	IEC 62290-2 5.1.3.1.1
13	Determine temporary infrastructure speed restrictions	This function is intended to set and remove temporary speed restrictions for selected areas by operational commands or as result of system reactions.	IEC 62290-2 5.1.3.1.2
14	Determine permanent rolling stock speed restrictions	This function is intended to determine the maximum permitted speed for each type of rolling stock.	IEC 62290-2 5.1.3.1.3
15	Determine temporary rolling stock speed restrictions	This function is intended to determine temporary rolling stock speed restrictions due to train failures and to driving modes.	IEC 62290-2 5.1.3.1.4

5.1.4 Authorise train movement

Nr.	Name of safety function	Description	Reference
16	Determine movement authority limit	To ensure safe train movement, this function determines for each train its limit of the movement authority, corresponding to the first danger point ahead of the train.	IEC 62290-2 5.1.4.1
17	Determine train protection profile	This function determines the train protection profile for all trains to ensure their limits of movement authority and authorised speeds are never exceeded. The train protection profile terminates at a target point. The train protection profile shall be determined by the applicable safe braking model.	IEC 62290-2 5.1.4.2
18	Authorise train movement by wayside signals	This function is intended to authorise train movement by wayside signals for non UGTMS-operated trains if conditions of safe route and safe separation are fulfilled. Wayside signals are used to allow mixed traffic or, as one possibility, for degraded operation.	IEC 62290-2 5.1.4.3
19	Determine a zone of protection	This function is intended to set and remove zones of protection for selected areas by operational command or as result of system reactions.	IEC 62290-2 5.1.4.4
20	Stopping a train en route	This function is intended to stop a train immediately in case of emergency.	IEC 62290-2 5.1.4.5
21	Authorise the entry of non-operative UGTMS trains into UGTMS territory	This function is intended to authorise the entry of non-operative UGTMS trains into the UGTMS territory.	IEC 62290-2 5.1.4.6

5.1.5 Supervise train movement

Nr.	Name of safety function	Description	Reference
22	Determine actual train speed	This function is intended to determine the actual train speed.	IEC 62290-2 5.1.5.1
23	Supervise safe train speed	This function is intended to supervise actual speed against the permitted speed of UGTMS-equipped trains with respect to the train protection profile.	IEC 62290-2 5.1.5.2
24	Inhibit train stops	This function is intended to avoid UGTMS operating trains to be tripped by train stops.	IEC 62290-2 5.1.5.3
25	Monitor speed limit at discrete location	This function is intended to monitor external wayside equipment detecting predefined overspeed.	IEC 62290-2 5.1.5.4
26	Supervise train rollaway	This function is intended to supervise the train in case of rollaway.	IEC 62290-2 5.1.5.5
27	Immobilisation of train	This function is intended to constrain the train against motion during station stop for passenger exchange.	New for MODSafe
28	Detect unauthorised movement of non-operative trains	This function is intended to detect unauthorised movements of non-equipped or non-reporting trains.	New for MODSafe
29	React to unauthorised movement of non-operative trains	This function is intended to react to unauthorised movements of non-operative trains in order to prevent collisions.	IEC 62290-2 5.1.5.6
30	Detect intruding unequipped train	This function is intended to detect an intrusion of an unequipped train into UGTMS territory.	New for MODSafe

5.2 Provide interface with external interlocking

Nr.	Name of safety function	Description	Reference
31	Provide interface with external interlocking	This function is intended to provide an interface to an external interlocking if the basic function ensure safe route and other functions (e.g. authorise train movement by wayside signals, locate non reporting trains by track sections) are not realised inside UGTMS.	IEC 62290-2 5.1.6

5.3 Supervise guideway

5.3.1 Prevent collision with obstacles

Nr.	Name of safety function	Description	Reference
32	Supervise wayside obstacle detection device	This function is intended to supervise external devices in charge of detecting obstacles on the track.	IEC 62290-2 5.3.1.1
33	Supervise onboard obstacle detection device	This function is intended to supervise the actions of an external onboard obstacle detection device to stop the train in case of collision with obstacle.	IEC 62290-2 5.3.1.2

5.3.2 Prevent collision with persons on tracks

Nr.	Name of safety function	Description	Reference
34	Warn passenger to stay away from the platform edge	This function is intended to warn passenger to stay away from platform edge if a train is in approach to the platform track.	IEC 62290-2 5.3.2.1
35	React on emergency stop request from platforms	This function is intended to react to emergency stop request from platforms initiated by passengers or staff	IEC 62290-2 5.3.2.2
36	Supervise platform doors	This function is intended to supervise the closed and locked status of the platform doors if they are not required to be open.	IEC 62290-2 5.3.2.3
37	Supervise platform tracks	This function is intended to supervise the actions of an external platform track detection device to stop the train in case of intrusion of person.	IEC 62290-2 5.3.2.4
38	Supervise border between platform tracks and other tracks	This function is intended to supervise the actions of an external device which supervises both borders of platform tracks detecting persons which are intruding the adjacent track areas.	IEC 62290-2 5.3.2.5
39	Supervise platform end doors	This function is intended to supervise the actions of an external device which supervises doors on both ends of platforms detecting not permitted opening of doors and intrusion of persons to tracks between stations via that way.	IEC 62290-2 5.3.2.6

5.4 Protect staff on track

Nr.	Name of safety function	Description	Reference
40	Protect staff on track	This function is intended to establish and subsequently remove work zones in order to protect staff on the track. A work zone is set as long as the protection is required.	IEC 62290-2 5.3.3

5.5 Supervise passenger transfer

5.5.1 Control passenger doors

Nr.	Name of safety function	Description	Reference
41	Authorise train doors opening	This function is intended to authorise train doors opening regarding all conditions which are required to ensure a safe passenger transfer.	IEC 62290-2 5.4.1.1
42	Command doors opening	This function is intended to command train doors and platform doors (if installed) opening when opening authorisation conditions are met.	IEC 62290-2 5.4.1.2
43	Request doors closing	This function is intended to request the train door and platform doors (if installed) closing at stations.	IEC 62290-2 5.4.1.3
44	Supervise doors closing	This function is intended to supervise the train door and platform door (if installed) closing at stations.	IEC 62290-2 5.4.1.4
45	Supervise closed and locked status of train doors	This function is intended to supervise the closed and locked status provided by the rolling stock.	IEC 62290-2 5.6.6

5.5.2 Prevent person injuries between platform and train

Nr.	Name of safety function	Description	Reference
46	Prevent person injuries between platform and train	This function is intended to detect persons between platform and train. (Prevented hazard include falling or trapping between platform and train.)	New for MODSafe
47	Prevent person being trapped between platform screen doors and train	This function is intended to detect persons being trapped between platform screen doors (if installed) and train doors, when they are closing.	New for MODSafe

5.5.3 Prevent person injuries between train cars

Nr.	Name of safety function	Description	Reference
48	Prevent person injuries between train cars	This function is intended to detect persons between train cars. (Prevented hazard include falling or trapping between train cars.)	New for MODSafe

5.5.4 Ensure safe starting conditions

Nr.	Name of safety function	Description	Reference
49	Authorise station departure (safety related conditions)	This function is intended to verify all prerequisites necessary for safe station departure.	IEC 62290-2 5.4.3.1
50	Authorise station departure (operational conditions)	This function is intended to verify all prerequisites necessary due to operational constraints in order to authorise station departure.	IEC 62290-2 5.4.3.2
51	Command station departure	This function is intended to command a train to leave the station when the required operational and safety conditions are met.	IEC 62290-2 5.4.3.3

5.6 Operate a train

5.6.1 Put in or take out of operation

Nr.	Name of safety function	Description	Reference
52	Awake trains	This function is intended to awake trains which are in stabling locations (in workshop, sidings or in the line) before they enter service by the action of the driver, or by remote action from the OCC.	IEC 62290-2 5.5.1.1
53	Set trains to sleep	This function is intended to set the train to sleep in stabling locations (in workshop, sidings or in the line) after they leave service by the action of the driver, or by remote action from the OCC:	IEC 62290-2 5.5.1.2

5.6.2 Manage driving modes

Nr.	Name of safety function	Description	Reference
54	Manage driving modes	This function is intended to manage the driving modes of the train.	IEC 62290-2 5.5.2

5.6.3 Manage movement of trains between two operational stops

Nr.	Name of safety function	Description	Reference
55	Manage movement of trains between two operational stops	This function is intended to manage the movement of trains on the guideway between stations taken into account different operational disturbances leading to stops outside stations.	IEC 62290-2 5.5.3

5.6.4 Manage depot and stabling areas

Nr.	Name of safety function	Description	Reference
56	Manage depot and stabling areas	This function is intended to manage train movement in depots and stabling areas.	IEC 62290-2 5.5.4

5.6.5 Manage UGTMS transition areas

Nr.	Name of safety function	Description	Reference
57	Manage UGTMS transition areas	This function is intended to manage the train movement from or to UGTMS transition areas.	IEC 62290-2 5.5.5

5.6.6 Restrict train entry to station

Nr.	Name of safety function	Description	Reference
58	Restrict train entry to station	This function is intended to prevent entry of a train into station when the required operational conditions are not met.	IEC 62290-2 5.5.6

5.6.7 Manage the platform or siding stopping position of the train

Nr.	Name of safety function	Description	Reference
59	Manage the platform or siding stopping position of the train	This function is intended to manage different stopping positions of trains per platform or siding due to operational reasons.	IEC 62290-2 5.5.7

5.6.8 Change the travel direction

Nr.	Name of safety function	Description	Reference
60	Change the travel direction	This function is intended to define the conditions and process in order to change the travel direction of a train.	IEC 62290-2 5.5.8

5.6.9 Couple and split a train

Nr.	Name of safety function	Description	Reference
61	Couple trains automatically	This function is intended to automatically join two separate trains operated independently, in designated coupling area, to be operated as a single train consist.	IEC 62290-2 5.5.9.1
62	Split trains – untimely train uncoupling	This function is intended to split a train consisting of two or more trains sets into two separate trains to be operated independently.	IEC 62290-2 5.5.9.2

5.6.10 Supervise the status of the train

Nr.	Name of safety function	Description	Reference
63	Supervise UGTMS onboard equipment status prior to entering service	This function is intended to perform all necessary tests on vital equipment during the power on process or prior to entering UGTMS territory. Generally this function includes only those self tests that deal with the safety of UGTMS and the inputs and outputs necessary for a vital operation. Self tests that are necessary to achieve the safety features of vital processors (computing unit including operating system) are not included here.	IEC 62290-2 5.5.10.1
64	Supervise UGTMS onboard equipment status during operation	This function is intended to perform all necessary tests during operation of the system. Generally this function includes only those self tests that deal with the safety of the UGTMS application and the inputs and outputs necessary for a vital operation. Self tests that are necessary to achieve the safety features of vital processors are not included here.	IEC 62290-2 5.5.10.2
65	Test emergency braking performance	This function is intended to perform a dynamic emergency braking test by commanding emergency braking during motion.	IEC 62290-2 5.5.10.3
66	React to detected train equipment failure	This function is intended to react to train equipment failures reported by the rolling stock impacting operation.	IEC 62290-2 5.5.10.4
67	Manage traction power supply on train	This function is intended to manage traction power supply during train operation (e.g. selection of current collector, AC/DC selection, voltage selection, automatic raising and lowering of pantographs and collector shoes, automatic opening/closing of circuit breakers). This function is for instance applicable if several power systems are fitted for a given line.	IEC 62290-2 5.5.11

5.7 Ensure detection and management of emergency situations

Nr.	Name of safety function	Description	Reference
68	Detect fire and smoke	This function is intended to detect fire or smoke onboard of train.	New for MODSafe
69	React to detected fire/smoke	This function is intended to supervise an external onboard fire/smoke detection device in order to report corresponding emergency conditions to OCC and to hold train at next station or optionally at the next evacuation point.	IEC 62290-2 5.6.1
70	React to detected or suspected broken rail	This function is intended to react to detected broken rail by external devices. This function describes as well the reaction of UGTMS for suspected broken rails when no broken rail detectors are implemented, but track circuits are used as train detection devices.	IEC 62290-2 5.6.3
71	Monitor emergency calls	This function is intended to monitor external emergency calls.	IEC 62290-2 5.6.4.1
72	React to passenger alarm device activation	This function is intended to react to the activation of an external onboard passenger alarm device.	IEC 62290-2 5.6.4.2
73	React to emergency release of train doors	This function is intended to manage the actions following the emergency release request of train doors. Such request is triggered by activating an onboard device if fitted.	IEC 62290-2 5.6.4.3
74	Detect loss of train integrity	The UGTMS system shall detect when a train of two or more cars has parted.	New for MODSafe
75	React to loss of train integrity	This function is intended to react to the loss of the train integrity provided by the rolling stock.	IEC 62290-2 5.6.5
76	Detect derailment	This function is intended to detect derailment by an external onboard derailment detection device.	New for MODSafe
77	Trigger emergency brake	This function is intended to initiate application of emergency brake e.g. due to detected overspeed or passing signals at danger.	New for MODSafe

6 Preliminary Combination of Functions and Objects

In order to prepare the allocation of Safety Requirements between Functions and Objects in D5.3, a preliminary UML model links the Functions of this deliverable with the Objects identified in D5.1.

Since UML is a modeling language supported by a number of tools with continuing updates, a versatile and generic modeling has been selected. Functions, as well as Objects, are represented by “Classes” to permit later users further detailing (introduction of inherited classes, addition of further meta-classes, definition of representatives of a class etc.).

An example for a Functions Class could be “Determine Train Location”, examples for Object Classes could be “Carborne Controller”, “Spot Transmission Antenna” (onboard), “Onboard Continuous Transmission Equipment”, “Absolute Speed/Position Measurement”, “Relative Speed/Position Measurement”, “Track Vacancy Detection”, “Zone Controllers”, “Database Storage Unit”, “Spotwise Communication” (wayside), “Continuous Communication” (wayside), “Wayside Data Communication Network”.

Three typical UML-Relationships between classes may be considered: “Generalization”, “Aggregation” or “Association”.

A Generalization-Relationship, sometimes called “Abstraction”, relates a number of entities to an abstract form that covers all entities in a generic sense. Example: “Season” is the abstraction of “Summer”, “Spring”, “Winter”. For our purposes, this relation is not adequate, since we want to relate Objects to Functions that have a priori no abstract commonality.

An Aggregation--Relationship expresses, that one Class consists of representatives of other Classes. Example: “Year” consists of “Summer”, “Spring”, “Winter” and “Autumn”. Aggregations are adequate for our purpose to model the structure of objects (object tree) and functions (function tree), respectively. For example, the object class “Zone Controllers” aggregates in our model from the three object classes “Zone Controller”, “Database Storage Unit” and “Wayside Data Communication Network”. However, for a linking of objects and functions the aggregation relationship is not adequate for two reasons: Functions and Objects are different in nature, so a Function may consist of Sub-Functions and Objects may consist of Sub-Objects, but an Object does not “consist” of Functions.

More importantly: Objects that are involved in the relation of a function shall respect the safety requirements of this fonction or shall demonstrate to be free from any dangerous fault regarding safety requirements of this function. The purpose of the link is NOT, to prescribe what objects shall be mandatorily used to realize a function.

An Association-Relationship is suitable to link entities that are different in nature. An example is the Association of “Sunshine” and “Summer”. This relation is considered adequate for our purpose, since we can associate Objects with Functions in a generic form and without further constraints (as for the other relations).

Procedure of the Association:

Starting point for the Association are the Functions. For every Function (in a certain GOA), all Objects are screened. If it appears plausible, that an Object may interfere in the realization of a Function, then it is linked (“associated”). As an example, the Object Classes “Carborne Controller”, “Spot Transmission Antenna” (onboard), “Onboard Continuous Transmission Equipment”, “Absolute Speed/Position Measurement”, “Relative Speed/Position Measurement”, “Track Vacancy Detection”, “Zone Controllers”, “Database Storage Unit”, “Spotwise Communication” (wayside), “Continuous Communication” (wayside) and “Wayside Data Communication Network” may be associated with the Function “Determine Train Location” in GOA4 (see Fig. 1).

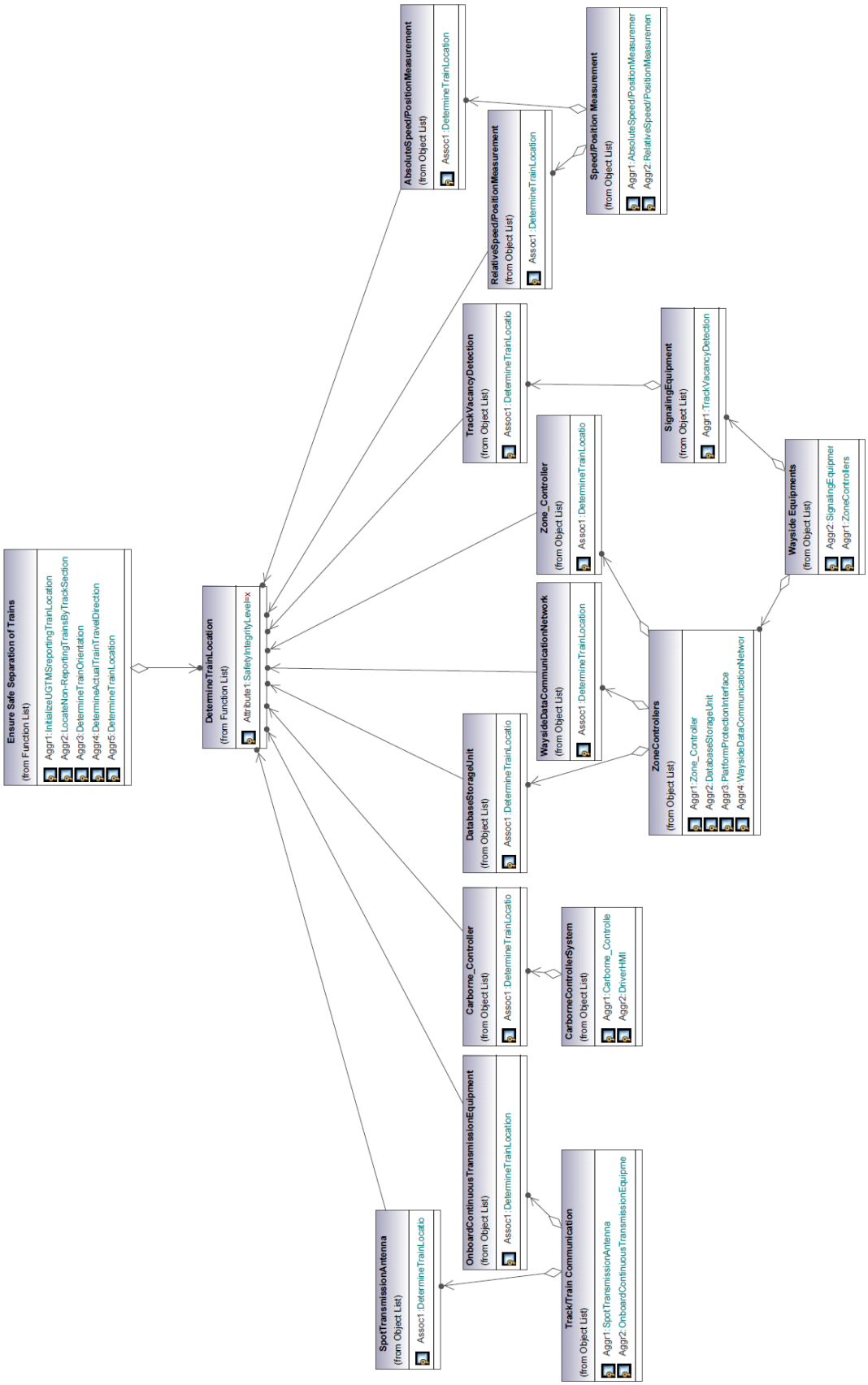

Fig. 1 Association Example for function "Determine Train Location" with different objects

As described further above, the selection of Objects does not mean, that the Functions must consist of these objects. It shall rather express that, if the Object is used for the realization of the Function, then it must respect the Safety Requirement of the Function or demonstrated to be free of safety relevance for the function. The generic linking is therefore “overcomplete” in the sense, that it represents the maximum of possibly interfering objects and – for a concrete architecture – is likely that only a subset of the selected Objects are retained.

Since the final linking requires discussions in the context of D5.3 (and will be part of D5.3), the annex of this deliverable contains a preliminary UML version of the linking for GOA4 (the mode with the largest number of associations) as an example in XMI-format.

7 Conclusion

This safety functional model represents the functional model for MODSafe containing safety relevant functions. It is input and basis for the work packages two, three, four and five. A preliminary (GOA4) version of the Combined Objects/Functions Model is included in the annex.

8 Informative annex

The annex contains a XMI (XML metadata interchange) file with the UML representation of the Objects/Functions linking.