MODSafe

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

Safety Attributes Allocation Matrix

Deliverable No. D5.3

Contract No.	218606
Document type	DEL
Version	V2.0
Status	Final
Date	29. April 2011
WP	WP 5
Lead Author	WP 5
Contributors	WP 5 partners
Description	Allocation of Functional Safety Requirements to Objects
Document ID	DEL_D5.3_TUD_WP5_110429_V2.0
Dissemination level	PU
Distribution	MODSafe Consortium

Document History:

Version	Date	Author	Modification
V1.1	4. March 2011	WP5	New document, First Draft
V1.2	24. March 2011	WP5	Accounting for WP5 comments
V2.0	20. April 2011	WP5	Accounting for WP10 comments

Approval:

Authority	Name/Partner	Date
WP responsible	TUD	24. March 2011
EB members	WP10	2. May 2011
Coordinator	TRIT	3. May 2011

Table of contents

1. Summary of this Document

The MODSAFE deliverable D5.2 (“Functional and Combined Object/Functional Guided Transport Model”) provides for the safety relevant functions of an Urban Guided Transport System and the MODSAFE deliverable D4.2 (“Analysis of Safety Requirements for MODSafe Continuous Safety Measures and Functions”) associates Safety Requirements with each of the functions.
The MODSAFE deliverable D5.1 (“Urban Guided Transport Object Safety Model”) lists a number of objects, that are typically used to realize the functions.
This deliverable D5.3 links the objects of D5.1 with the safety requirements of D4.2 of the functions, where the objects and functions are arranged in the form of an allocation matrix.

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-D80_BVG_WP21_090317_V2-5

/5/ DEL_MODURBAN-D129_RATP_WP20_090317_V27 MODURBAN GLOSSARY

/6/ COMITÉ EUROPÉEN DE NORMALISATION ÉLECTROTECHNIQUE: "EN 50126 Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS)", CENELEC 1999

/7/ COMITÉ EUROPÉEN DE NORMALISATION ÉLECTROTECHNIQUE: "EN 50129 Railway application – communication, signalling and processing systems – safety related electronic systems for signalling", CENELEC 2003

/8/ 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 2006

/9/ INTERNATIONAL ELECTROTECHNICAL COMMISSION: "IEC 62267 Railway Applications - Automated Urban Guided Transport (AUGT) - Safety Requirements", IEC 2009

/10/ DEL_D10.5_RATP_WP10_101005_V3, MODSafe Glossary

/11/ DEL_MODSYSTEM_D85 – MODURBAN architecture, identification of key interfaces and some preliminary FIS

/12/ INTERNATIONAL ELECTROTECHNICAL COMMISSION: "IEC 62290-2 Railway applications - Urban guided transport management and command/control systems (UGTMS) - Part 2 Functional requirement specification", IEC 2010

/13/ DEL_D4.2_UITP_WP4_101210_V1.1 ("Analysis of Safety Requirements for MODSafe Continuous Safety Measures and Functions")

/14/ DEL_D5.2_TUD_WP5_110218_V2 ("Functional and Combined Object/Functional Guided Transport Model")

/15/ DEL_D5.1_TUD_WP5_110222_V1.1 ("Urban Guided Transport Object Safety Model")

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)	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
ATC	Automatic Train Control
ATP	Automatic Train Protection
CRC	Cyclic Redundancy Check
DoW	Description of Work
GOA	Grade of Automation
HMI	Human Machine Interface
ID	Identification
IL	Interlocking
OCC	Operations Control Centre
PAX	Passenger
SIL	Safety Integrity Level
THR	Tolerable Hazard Rate
UGT	Urban Guided Transport
UGTMS	Urban Guided Transport Management System
UML	Unified Modelling 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 in other 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.

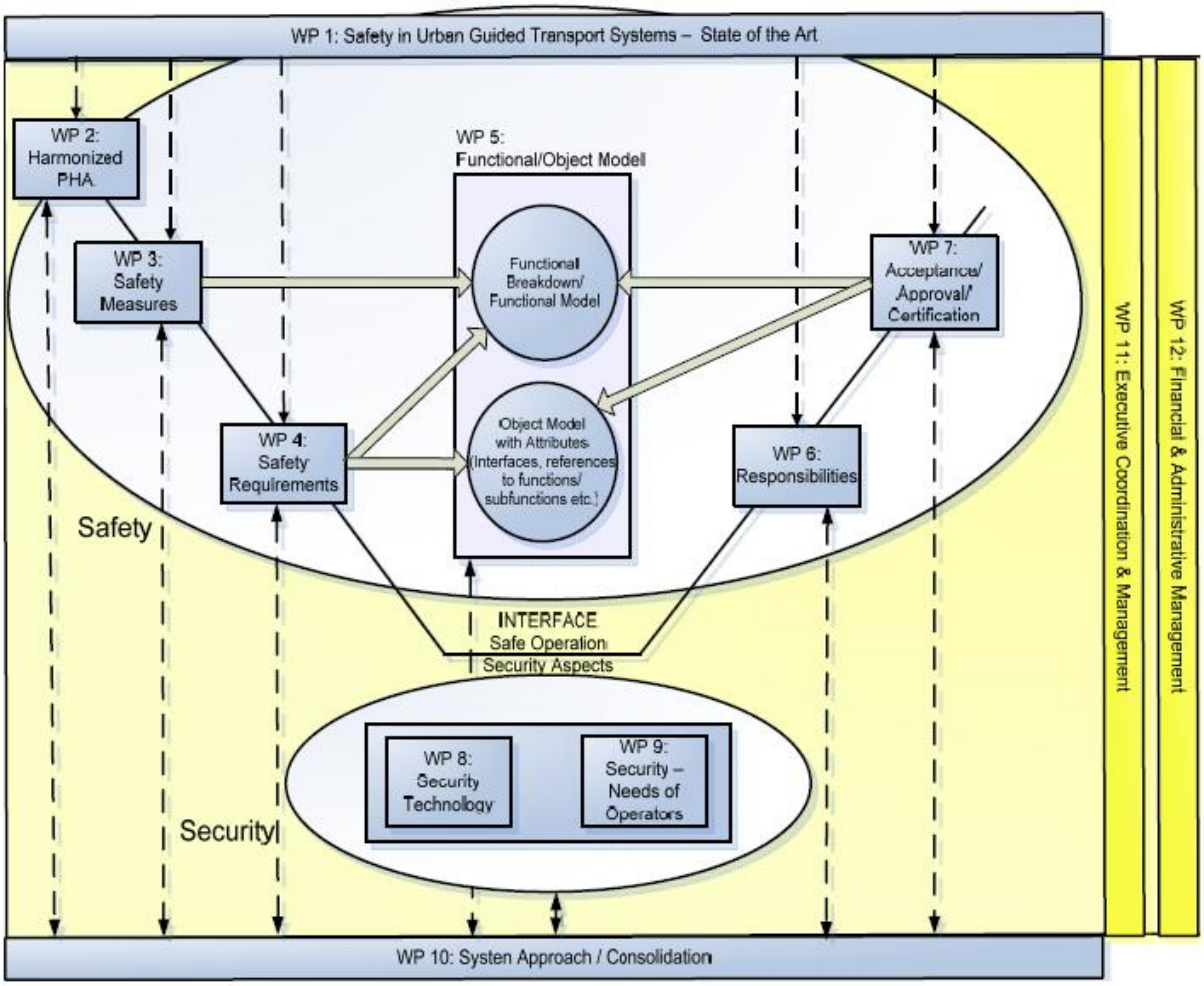

Figure 1 Overview over the MODSafe tasks, arranged into a V-Model like structure

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 third one is presented with this document.

WP5 is highly linked to WP4 (Safety Requirements), 5.2 (Safety Functional Model) and 5.1 (Safety Objects Model).

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 of Task 5.1.

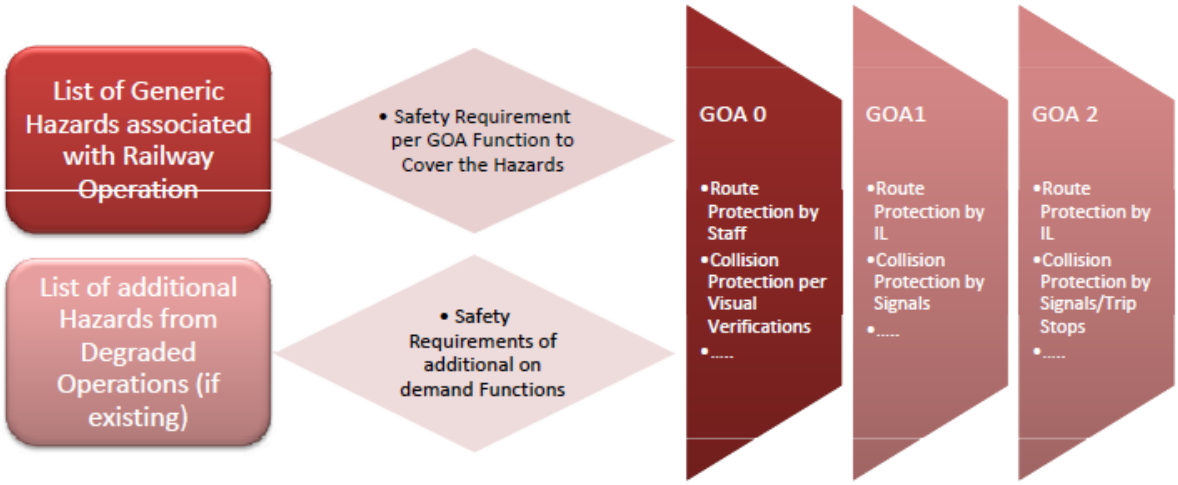

Figure 2 MODSafe Safety Model elements split up into work packages

2.2 Purpose of Task 5.3 (Safety Attributes Allocation Matrix)

In task 4.2, the WP4 endeavors to allocate Safety Integrity Requirements to generic safety relevant functions, based on agreed risk analysis approaches.

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. Any of the technical “Functions” are, however, in fact realized by one or multiple objects that may “fail” wrong side, leading to wrong side behaviour of the safety functions they realize. It is therefore the purpose of this deliverable D5.3 to link the safety attributes of the functions with relevant objects that may build up the function.

It shall be noted, that the question of statistical breakdown of safety requirements to lower level constituents is not addressed in this allocation work, since the object model remains at highest level of

detail. Also for this reason, no “arbitration” between objects had been performed (in the sense that several objects at a lower level of safety cover a function at a higher level of safety due to their non-minimal configuration).

“Safety requirements” is understood as in the analysis of D4.2, meaning it addresses the nominal operating state, not any degraded operating state.

For certain functions, no safety requirement is allocated because no safety requirement had been derived in D4.2 (eg. “Manage Driving Mode”) although in physical implementations it may be a SIL4 function. In these cases, the reader is advised to add the safety requirements as deemed adequate.

Some objects may be pertaining to the safety of a function in which they participate, but their “safety” characteristics are warranted by other objects (eg. continuous transmission, OCC). In this case the allocation is suppressed only, if it can be assumed that the respective object safety is in all possible realizations of this object covered by the other objects.

2.3 Methodology

First, a linking between functions and objects must be established. The deliverable D5.2 already defined a preliminary linking of the objects with functions of D5.2 by a UML model by associations.

The starting point for the association are the functions. For every function (in a certain GOA), all objects are screened. If it appears plausible, that a safety relevant object may interfere in the realization of a function, then it is linked (“associated”) to the function. 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.

For some objects, like the safety related information communication between trains and trackside equipments (Continuous Communication) the safety of the object itself may to large fraction be established by other objects (Onboard Controller, Wayside Controller in the example). These objects have been kept anyway since the subsystem as such have safety requirements that concern the object themselves (for reference Cenelec EN 50129 advises mitigation measures such as sequence number, time stamp, time out, source and destination identifier, feedback message, identification procedure, safety code / CRC, cryptographic techniques and respective evidence, e.g. calculation of remaining transmission failure probability).

The purpose of the linking is to express, that objects that participate in the realization of a function shall respect the safety requirements of this function. The purpose of the link is NOT to prescribe what objects shall be mandatorily used to realize a function. The generic linking is therefore “overcomplete” in the sense, that it represents the maximum of possibly interfering objects and – for a specific architecture – is likely that only a subset of the selected objects are retained.

In spite of the widespread use of UML, most of the tools available on the market at this time are not fully interoperable so possible computer file outputs are limited in usability.

For better readability the linking is therefore presented in a spread sheet format in D5.3 (MS Excel) in this deliverable. This representation is not reducing information, since the matrix shows all attributions equivalently to the UML-Associations.

The allocation matrices contain directly the SILs of the respective function of D4.2. Since for some functions the D4.2 refers to a later SIL-Determination (“low demand rate” functions in D4.3) a “d” is introduced (instead of a natural “SIL” number 1-4). Depending on the results of D4.3, the “d” can be replaced by the ultimate result.

For some particular functions, D4.2 yields the safety requirement depending on operational context (like passenger flows or further precisions of the GOA). In this case, an “x” is introduced in the matrix, and the possible values of D4.2 for the “x” are indicated with the function.

As a general guideline, the allocation procedure starts with the highest Grade of Automation (Unmanned Train Operation, GOA4) since the highest number of entries is expected at this level. Subsequently, the Grade of Automation is reduced and the allocations are reduced equivalently.

3. Allocation Matrices GOA0 to GOA4

For better readability, the matrices are annexed in printout format as A3.

Remark:

Note, that the allocation of SILs in the above matrix represents a guideline only; actual/ultimate values will depend on further progress/analysis in Work Package 4 and/or by future specific operator analysis.

4. Conclusion

Utilizing the previous deliverable's results (functions, objects, safety requirements to functions) makes it straightforward to distribute the function's safety requirements also to the objects that may build up the function. The paradigm to avoid further detailed "architectures" but rather stay at generic levels shows, however, also the limitations of the safety requirement allocation matrix process. While the matrix may serve as a high level allocation for participating objects, it is therefore recommended to apply an equivalent analysis for object/function matrices in an individual realization.

5. Annex: Matrix pdf-Printouts