<table>
<thead>
<tr>
<th>Contract No.</th>
<th>218606</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document type</td>
<td>DEL</td>
</tr>
<tr>
<td>Version</td>
<td>V1.0</td>
</tr>
<tr>
<td>Status</td>
<td>Final for WP10 consensus</td>
</tr>
<tr>
<td>Date</td>
<td>110531</td>
</tr>
<tr>
<td>WP</td>
<td>WP6</td>
</tr>
<tr>
<td>Lead Author</td>
<td>Peter Wigger (TRIT)</td>
</tr>
<tr>
<td>Contributors</td>
<td>RATP (sub-clause 3.3)</td>
</tr>
<tr>
<td></td>
<td>UITP (sub-clause 5.1)</td>
</tr>
<tr>
<td>Other Contributors</td>
<td>-</td>
</tr>
<tr>
<td>Description</td>
<td>Deliverable D6.3 V1.0</td>
</tr>
<tr>
<td>Document ID</td>
<td>DEL_D6.3_TRIT_WP6_110531_V1.0</td>
</tr>
<tr>
<td>Dissemination level</td>
<td>PU</td>
</tr>
<tr>
<td>Distribution</td>
<td>Consortium</td>
</tr>
</tbody>
</table>

**Document History:**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>05-10-2010</td>
<td>Mike Schick</td>
<td>Preparation of the structure</td>
</tr>
<tr>
<td>V0.1</td>
<td>07-11-2010</td>
<td>Peter Wigger</td>
<td>First draft, structure and first chapters</td>
</tr>
<tr>
<td>V0.2</td>
<td>31-01-2011</td>
<td>Peter Wigger</td>
<td>Completion for WP6 consensus</td>
</tr>
<tr>
<td>V0.3</td>
<td>28.02.2011</td>
<td>Peter Wigger</td>
<td>Updated according to WP6 comments</td>
</tr>
<tr>
<td>V0.4</td>
<td>25.03.2011</td>
<td>Peter Wigger</td>
<td>WP6 consensus</td>
</tr>
<tr>
<td>V0.5</td>
<td>09.05.2011</td>
<td>Peter Wigger</td>
<td>Updated according to WP10 comments</td>
</tr>
<tr>
<td>V0.6</td>
<td>11.05.2011</td>
<td>Peter Wigger</td>
<td>Incorporation of UITP comments</td>
</tr>
<tr>
<td>V0.7</td>
<td>30.05.2011</td>
<td>Peter Wigger</td>
<td>Incorporation of RATP comments</td>
</tr>
<tr>
<td>V1.0</td>
<td>31.05.2011</td>
<td>Peter Wigger</td>
<td>WP10 consensus Final</td>
</tr>
</tbody>
</table>

**Approval:**

<table>
<thead>
<tr>
<th>Authority</th>
<th>Name/Partner</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP responsible</td>
<td>TRIT / WP6 Approval</td>
<td>2011-03-24</td>
</tr>
<tr>
<td>EB members</td>
<td>WP 10 Approval</td>
<td>2011-05-30</td>
</tr>
<tr>
<td>Coordinator</td>
<td>TRIT</td>
<td>2011-05-31</td>
</tr>
</tbody>
</table>
Table of Contents

1 Introduction ........................................................................................................... 5
  1.1 References ........................................................................................................... 6
  1.2 Terms and Definitions ........................................................................................ 8
  1.3 Abbreviations ...................................................................................................... 10

2 Objectives of the Work Package .......................................................................... 11

3 Basis for the Life Cycle Approach Proposal .......................................................... 13
  3.1 MODSafe Deliverable D6.2 .................................................................................. 13
  3.2 CENELEC Life Cycle .......................................................................................... 15
  3.3 New Revision of CENELEC Standards ................................................................ 16

4 Methodology .......................................................................................................... 18

5 Common Life Cycle Approach Proposal ............................................................... 19
  5.1 Concept ................................................................................................................. 20
  5.2 System Definition & Application Conditions ....................................................... 22
  5.3 Risk Analysis ........................................................................................................ 24
  5.4 System Requirements ........................................................................................... 26
    5.4.1 Handling of different UGT systems ................................................................. 29
    5.4.2 Handling of different Grades of Automation ..................................................... 30
  5.5 Apportionment of System Requirements ............................................................... 31
  5.6 Design and Implementation .................................................................................. 33
    5.6.1 Handling of Sub-systems ............................................................................... 35
    5.6.2 Handling of Sub-systems – Example CBTC Sub-system ................................. 37
  5.7 Manufacture ....................................................................................................... 38
  5.8 Installation .......................................................................................................... 39
  5.9 System Validation & Safety Acceptance ............................................................... 40
    5.9.1 Supplier’s Verification and Validation ............................................................... 41
    5.9.2 Integration of Sub-systems into UGT System Safety Case ............................... 42
  5.10 System Acceptance ............................................................................................. 43
    5.10.1 Approval Milestones ...................................................................................... 45
    5.10.2 Independent Safety Assessment ................................................................... 46
    5.10.3 Life Cycle Approach Phase related Roles and Responsibilities ...................... 48
    5.10.4 Application of Cross-Acceptance .................................................................. 49
  5.11 Operation & Maintenance .................................................................................. 50
    5.11.1 Operations Manager Concept ...................................................................... 53
    5.11.2 Operations Manager duties .......................................................................... 53
  5.12 Performance Monitoring ..................................................................................... 54
  5.13 Modification & Retrofit ..................................................................................... 55
  5.14 Decommissioning & Disposal ............................................................................. 57

6 Summary and Conclusion ....................................................................................... 58
Index of Figures

Figure 1: Relationship to MODSafe Deliverables.................................................................12
Figure 2: EN 50126 Life-Cycle Model ................................................................................16
Figure 3: Common Life Cycle Approach Proposal ...............................................................19
Figure 4: Life Cycle Approach Phase “Concept”.................................................................21
Figure 5: Life Cycle Approach Phase “System Definition & Application Conditions” .......23
Figure 6: Life Cycle Approach Phase “Risk Analysis”.........................................................25
Figure 7: Proposed Requirement Specification Refinement ..................................................27
Figure 8: Life Cycle Approach Phase “System Requirements Specification” .................28
Figure 9: Handling of different UGT systems ....................................................................29
Figure 10: Handling of different Grades of Automation .....................................................30
Figure 11: Life Cycle Approach Phase “Apportionment of System Requirements” ..........31
Figure 12: Life Cycle Approach Phase “Design & Implementation” .................................33
Figure 13: Application of the lifecycle for a system and its sub-systems .........................35
Figure 14: Example for sub-system specification refinement (CBTC system) ...............37
Figure 15: Life Cycle Approach Phase “Manufacture” .......................................................38
Figure 16: Life Cycle Approach Phase “Installation”..........................................................39
Figure 17: Supplier’s Verification and Validation throughout the life cycle approach ........41
Figure 18: Life Cycle Approach Phase “System Validation & Safety Acceptance” ..........40
Figure 19: Principle hierarchy and structure of safety documentation ...............................42
Figure 20: Life Cycle Approach Phase “System Acceptance” ...........................................44
Figure 21: Safety Approval Milestones – Examples ............................................................45
Figure 22: Independent Safety Assessor Involvement.........................................................47
Figure 23: Life Cycle Approach related roles, responsibilities and interfaces ..................48
Figure 24: Process of Application of Cross Acceptance ....................................................49
Figure 25: Life Cycle Approach Phase “Operation & Maintenance” ...............................52
Figure 26: Life Cycle Approach Phase “Performance Monitoring” ....................................54
Figure 27: Life Cycle Approach Phase “Modification & Retrofit” .....................................56
1 Introduction

In Europe, Light Rail, Metros and Trams are characterized by a diversified landscape of safety requirements, safety models, roles and responsibilities, schemes for safety acceptance and approval; however, there are convergences between some architectures and systems, [MODUrban D93].

There are currently no standardised procedures at the European level for bringing Urban Guided Transport into service. There are no common standard procedures in Europe for safety evaluation (each country applies its own safety conformity assessment). Recent applications have been increasingly assessed by taking into account the European standards EN 50126/50128/50129, [CENELEC].

Most Urban Guided Transport stakeholders believe that the development of European (and even worldwide) standards should be encouraged, in order to facilitate the voluntary reference to such standards by relevant national authorities and the various stakeholders, [MODUrban D93].

The European Commission is favouring this approach, notably through its support of major European research projects such as the MODSafe project.

This work package focuses on Metros, Light Rail Systems, and Trams, covering the whole transportation system including all sub-systems, e.g. signalling system or rolling stock. Heavy rail and urban commuter trains like “S-Bahn” in Germany or SNCF “RER” in France are not within the focus.

Based on the survey gained in [MODSafe D6.1], and following the comparison [MODSafe D6.2], which identified differences and similarities in the process of the different EU countries, revealed the regulation background and analysed the main phases of the safety life cycles, the objective of this deliverable D6.3 is to propose a common safety lifecycle approach for urban guided transport systems.
### 1.1 References

<table>
<thead>
<tr>
<th>Reference-ID</th>
<th>Document title, identifier and version</th>
</tr>
</thead>
<tbody>
<tr>
<td>[CENELEC]</td>
<td>EN 50126:2000 &quot;Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)&quot;</td>
</tr>
<tr>
<td></td>
<td>EN 50128:2001 “Railway applications - Communications, signalling and processing systems - Software for railway control and protection systems&quot;</td>
</tr>
<tr>
<td></td>
<td>EN 50129:2003 “Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling”</td>
</tr>
<tr>
<td>[MODSafe D1.2]</td>
<td>WP 1 – MODSafe Deliverable – D1.2 State of the art on safety responsibilities and certification</td>
</tr>
<tr>
<td>[MODSafe D2.3]</td>
<td>WP 2 – MODSafe Deliverable – D2.3 Risk Analysis</td>
</tr>
<tr>
<td>[MODSafe D4.1]</td>
<td>WP 2 – MODSafe Deliverable – D4.1 State of the art analysis and review of results from previous projects</td>
</tr>
<tr>
<td>[MODSafe D4.2]</td>
<td>WP 2 – MODSafe Deliverable – D4.2 Analysis of common Safety Requirements Allocation</td>
</tr>
<tr>
<td>[MODSafe D4.3]</td>
<td>WP 4 – MODSafe Deliverable – D4.3 Analysis of On Demand Functions and Systematic Failures</td>
</tr>
<tr>
<td>[MODSafe D5.1]</td>
<td>WP 2 – MODSafe Deliverable – D5.1 Safety Object Model</td>
</tr>
<tr>
<td>[MODSafe D5.2]</td>
<td>WP 2 – MODSafe Deliverable – D5.2 Combined Functional Model / Object Model</td>
</tr>
<tr>
<td>[MODSafe D5.3]</td>
<td>WP 5 – MODSafe Deliverable – D5.3 Safety Attributes Allocation Matrix</td>
</tr>
<tr>
<td>[MODSafe D6.2]</td>
<td>WP6 – MODSafe Deliverable – D6.2 Comparison of current safety lifecycle approaches</td>
</tr>
<tr>
<td>Reference-ID</td>
<td>Document title, identifier and version</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------</td>
</tr>
</tbody>
</table>
| [MODSafe D7.3] | WP 7 – MODSafe Deliverable – D7.3  
Generic Model for AAC processes |
| [MODSafe D7.4] | WP 7 – MODSafe Deliverable – D7.4  
Proposal of a typical optimized AAC process |
| [MODSafe DOW] | MODSafe Annex 1 – Description of Work |
Conformity Assessment, Guidelines for Functional and Technical Specifications |
Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Guide to the application of EN 50126-1 for safety |
Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Guide to the application of EN 50126-1 for Rolling Stock RAMS |
Railway applications – Communication, signalling and processing systems – Application guide for EN 50129 – Part 1: Cross-acceptance |
Railway applications – Communication, signalling and processing systems – Application guide for EN 50129 – Part 2: Safety assurance |
The German TR SIG ZA, which stands for approval of Signalling and Train Control and Protection Systems according to BOSTrab, is developed in order to implement the use of the standards EN 50128 / EN 50129, in reference to the German legislation (e.g. regarding the risk acceptance criteria and responsibilities of involved actors). For the description of how system approval and acceptance procedure shall be conducted TR SIG ZA strictly follows the life cycle concept introduced in EN 50126. |

Note: Some of the MODSafe deliverables were not yet finished and published at the date of the document at hand, in particular [MODSafe D2.3], [MODSafe D3.2], [MODSafe D4.3], [MODSafe D5.3], [MODSafe D7.2], [MODSafe D7.3] and [MODSafe D7.4]. It is however considered justified to cite and refer to the relevant MODSafe deliverables throughout the document at hand aiming to depict their life cycle approach relation. The cited MODSafe deliverables do not and will not have an impact on the life cycle approach introduced here.
1.2 Terms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic Application</td>
<td>System with specific functions that are related to “a category of applications” associated with a general environmental and operational context, which is developed on the basis of criteria of standardization and parameterization of its elements, so as to render it serviceable for various tangible applications. By combining generic products or combining these with other generic applications, it is possible to obtain a new generic application, ref. [TR 50506-2].</td>
</tr>
<tr>
<td>Generic Product</td>
<td>Component or product capable of performing certain functions, with specific performance level, in the environmental and operational conditions stated in the reference specifications. It can be combined with other products and Generic Applications to form other generic applications, ref. [TR 50506-2].</td>
</tr>
<tr>
<td>Independent Safety Assessor</td>
<td>“Independent Safety Assessor” (ISA) is an independent third party to assess safety in the field of urban guided transport applications.</td>
</tr>
<tr>
<td>Light Rail</td>
<td>Light Rail Transit (LRT) is an electric rail-borne form of transport which can be developed in stages from a tram to a metro-like system operated partially on its own right-of-way.</td>
</tr>
<tr>
<td></td>
<td>The general term ‘light transit’ covers those systems whose role and performance lie between a conventional bus service running on the highway at one extreme and an urban heavy rail or underground metropolitan railway at the other. Light rail systems are thus flexible and expandable. Source: <a href="http://www.uitp.org/public-transport/light-rail/index.cfm">http://www.uitp.org/public-transport/light-rail/index.cfm</a></td>
</tr>
<tr>
<td>Metros</td>
<td>Metropolitan railways are urban, electric transport systems with high capacity and a high frequency of service.</td>
</tr>
<tr>
<td></td>
<td>Metros are totally independent from other traffic, road or pedestrians. They are consequently designed for operations in tunnel, viaducts or on surface level but with physical separation. Metropolitan railways are the optimal public transport mode for a high capacity line or network service.</td>
</tr>
<tr>
<td></td>
<td>Some systems run on rubber-tyres but are based on the same control-command principles as steel-wheel systems.</td>
</tr>
<tr>
<td></td>
<td>In different parts of the world metro systems are also known as the underground, subway or tube.</td>
</tr>
<tr>
<td>Operator</td>
<td>“Operator” means a public or private undertaking, the activity of which is to provide the transport of passengers by urban guided transport (UGT) systems.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Safety Authority</td>
<td>“Safety Authority” refers to the body responsible for certifying that a safety-related system is fit for service and complies with relevant statutory and regulatory safety requirements, ref. EN 50129, [CENELEC].</td>
</tr>
<tr>
<td>Safety Case</td>
<td>The documented demonstration that the product complies with the specific safety requirements.</td>
</tr>
<tr>
<td>Supervisory Authority</td>
<td>&quot;Supervisory Authority&quot; refers to the body entrusted with the tasks regarding supervision of the operation and maintenance of urban guided transport systems. The supervisory authority can be the same body as the safety authority with the legal power to grant operation (licensing) or to close it.</td>
</tr>
<tr>
<td>Supplier</td>
<td>“Supplier” is defined as a contractor who provides the urban guided transport system or one of its sub-systems. Generally, a supplier is a manufacturer of a sub-system such as Rolling Stock or Infrastructure. In addition, a supplier may also be appointed as a company supplying the whole urban guided transport system by means of sub-contractors.</td>
</tr>
<tr>
<td>Tram</td>
<td>A tram is an urban electric rail-borne system sharing the track right-of-way with the general road traffic. It is a special kind of “Light Rail”.</td>
</tr>
<tr>
<td>Validation</td>
<td>Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled, ref. EN 50126, [CENELEC].</td>
</tr>
<tr>
<td>Verification</td>
<td>Confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled, ref. EN 50126, [CENELEC].</td>
</tr>
</tbody>
</table>

Refer also to [GLOSSARY.en]
### 1.3 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAC</td>
<td>Acceptance, Approval, Certification</td>
</tr>
<tr>
<td>BOStrab</td>
<td>Verordnung über den Bau und Betrieb der Straßenbahnen (German Federal Regulations on the construction and operation of light rail transit systems)</td>
</tr>
<tr>
<td>CENELEC</td>
<td>Comité Européen de Normalisation Electrotechnique (European Committee for Electrotechnical Standardisation)</td>
</tr>
<tr>
<td>DOW</td>
<td>Description Of Works (refer to [MODSafe DOW])</td>
</tr>
<tr>
<td>EB</td>
<td>Executive Board</td>
</tr>
<tr>
<td>EN</td>
<td>European Standard</td>
</tr>
<tr>
<td>GARTs</td>
<td>Generally Accepted Rules of Technology</td>
</tr>
<tr>
<td>GOA</td>
<td>Grade of Automation</td>
</tr>
<tr>
<td>HA</td>
<td>Hazard Analysis</td>
</tr>
<tr>
<td>ISA</td>
<td>Independent Safety Assessor</td>
</tr>
<tr>
<td>LRT</td>
<td>Light Rail Transit</td>
</tr>
<tr>
<td>MODSafe</td>
<td>Modular Urban Transport Safety and Security Analysis</td>
</tr>
<tr>
<td>MODUrban</td>
<td>Modular Urban Guided Rail System project</td>
</tr>
<tr>
<td>PHA</td>
<td>Preliminary Hazard Analysis</td>
</tr>
<tr>
<td>RAM</td>
<td>Reliability, Availability, Maintainability</td>
</tr>
<tr>
<td>RAMS</td>
<td>Reliability, Availability, Maintainability, Safety</td>
</tr>
<tr>
<td>SIL</td>
<td>Safety Integrity Level</td>
</tr>
<tr>
<td>THR</td>
<td>Tolerable Hazard Rate</td>
</tr>
<tr>
<td>UGT</td>
<td>Urban Guided Transport (System)</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>Verification and Validation (according to [CENELEC])</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>

Refer also to [GLOSSARY.en]
2 Objectives of the Work Package

This Chapter briefly describes the objectives of Work Package 6 (WP6) in general and the task of this deliverable in specific.

"The objective of WP6 is to identify common practices and/or similarities for the safety approval of guided urban transport systems, in particular ATC-Systems by safety authorities and other involved actors, throughout the different countries of the European Union. On this basis a potential common procedure for building, assessing and approving the different safety files will be developed and proposed bearing in mind the different responsibilities along the safety lifecycle and the roles and authorizations of the different actors." ref. ([MODSafe DOW], Sub-clause B.1.3.5).

WP 6 comprises of the following deliverables:

- Deliverable D6.1 - Survey on current safety lifecycle approaches
- Deliverable D6.2 - Comparison of current lifecycle approaches
- Deliverable D6.3 - Proposal of a common safety life cycle approach (this report)

Based on the results of the previous analysis [MODSafe D6.2], this deliverable defines and proposes a common safety life cycle approach for urban guided transport systems. The respective description especially considers the interfaces between the different life cycle approach phases and responsibilities.
Relation to other Work Packages

As described in the [MODSafe DOW], results of [MODSafe D1.2] have been used as input for the survey [MODSafe D6.1], mainly taking credit of the case studies. Additionally, synergy effects have been used, sharing the results with WP7 [MODSafe D7.1] due to the fact that Work Packages 6 and 7 have a common base and interdependencies.

This proposal of a common life cycle approach [MODSafe D6.3] considers the interfaces between the different life cycle approach phases and responsibilities and therefore cross-wise offers synergy effects to the generic approach of AAC procedures [MODSafe D7.3] and the proposal of a typical optimized AAC process [MODSafe D7.4].

The deliverables of Work Packages 3 – 5 (hazard and risk analysis, hazard control and safety response analysis, common requirements specification, functional / object safety model) and Work Package 7 (AAC, acceptance, approval and certification) are referred to in the respective life cycle approach phases of the proposed common life cycle approach. The relationship to these MODSafe deliverables is shown in the figure below.

**Figure 1: Relationship to MODSafe Deliverables**
3 Basis for the Life Cycle Approach Proposal

The main basis for the life cycle approach proposal is [MODSafe D6.2] as well as the CENELEC life cycle. Furthermore, results of [MODSafe D7.1] were considered, while the generic approach of Acceptance, Approval, Certification (AAC) procedures [MODSafe D7.3] and the proposal of a typical optimized AAC process [MODSafe D7.4] will be matched with the common life cycle approach proposal as proposed in the document at hand, [MODSafe D6.3].

3.1 MODSafe Deliverable D6.2

[MODSafe D6.2] concluded that “Most of the EU-countries apply to processes which are at least tentatively compliant to the CENELEC life cycle, deviating in range and depths. Some countries follow CENELEC to ensure system safety performance during the whole life cycle. An application of the CENELEC procedures is evident and steadily growing.”

This forms the base and bridge for the proposal of a common life cycle approach, which naturally will be based on and driven by the CENELEC life cycle.

[MODSafe D6.2] concluded the following differences throughout Europe:

- The involvement of the Safety Regulatory Authority differs in range and depth.  
  - This topic is subject to proposal in [MODSafe D7.4].

- Risk criteria for obtaining system approval are mandatory, but there is no common or regulated approach, although CENELEC gives guidance.  
  - This topic is subject to proposal in [MODSafe D6.3] - the document at hand - with respect to life cycle approach activities and in [MODSafe D7.4] with respect to authority involvement.

- Procedures on installation & operation are not uniformly regulated but in practice commonly in use with a different level of operator involvement.  
  - This topic is subject to proposal in [MODSafe D6.3] - the document at hand - with respect to life cycle approach activities and in [MODSafe D7.4] with respect to authority involvement.

- Light rail, tram or metro systems are not uniformly treated in terms of approval process and requirements.  
  - This topic is subject to proposal in [MODSafe D6.3] - the document at hand - with respect to life cycle approach activities and in [MODSafe D7.4] with respect to authority involvement.
[MODSafe D6.2] concluded the following similarities throughout Europe:

- A legal basis for the Safety Regulatory Authorities is mostly given with acts or decrees / regulations.
  - This topic is subject to proposal in [MODSafe D7.4].
- Safety Regulatory Authorities appointed to urban guided transport are commonly in use.
  - This topic is subject to proposal in [MODSafe D7.4].
- Liability for safety & orderly operation is mostly dedicated to the operator / responsible person / infrastructure provider.
  - This topic is subject to proposal in [MODSafe D7.4].
- The involvement of an Independent Safety Assessor is not consistently regulated but in practice commonly in use.
  - This topic is subject to proposal in [MODSafe D6.3] - the document at hand - with respect to life cycle approach aspects and in [MODSafe D7.4] with respect to authority involvement.
- Verification & Validation activities prior to operation are not uniformly regulated but in practice commonly in use, the performance along the lifecycle differs in scope and depth.
  - This topic is subject to proposal in [MODSafe D6.3], the document at hand.
- Examples for cross-acceptance in European level are evident, ref. [MODSafe D6.2]. The CENELEC standards and their guidelines contribute to this increasing harmonisation.
  - This topic is subject to proposal in [MODSafe D6.3], the document at hand.
- CENELEC Standards are commonly used as guidelines for obtaining system approval.
  - This is the basis of the common life cycle approach proposal in [MODSafe D6.3], the document at hand.
3.2 CENELEC Life Cycle

To date, the CENELEC railway application standards EN 50126 series - being also transferred to international IEC level - have reached a mature state and are implemented practically in every new rail technology project. These standards may not only apply to heavy rail systems - as their heading 'Railway applications' may imply, but also to urban guided transport systems including light rail, tram and metro systems.

These standards have been created with the goal to develop compatible rail systems and to enable cross-acceptance of generic approvals by the different railway authorities not only throughout Europe. The application range of the three CENELEC railway standards is as follows. While EN 50126 covers the total railway system concerning RAMS, EN 50129 deals with safety-related electronic systems for signalling, and EN 50128 applies to (safety related) software for railway control and protection systems. The standards EN 50126, EN 50128 and EN 50129 represent the railway application-specific interpretation of the international standard series IEC 61508 (functional safety of electrical/electronic/programmable electronic safety-related systems).

The standards introduce a probabilistic approach into rail technology; such an approach was primarily used in nuclear and aerospace technologies in the past. Furthermore, the standards provide a structured approach and flexible methodology, they standardise the demonstration of system safety of complex rail systems and they allow the integration of proven and new technologies and the apportioning of the safety case concept to all sub-systems.

The standard EN 50126 is often called the 'RAMS standard' since it deals with Reliability, Availability, Maintainability and Safety. There are further CENELEC standards for rail applications focusing more on technical details, such as electromagnetic compatibility or communications. However, the set of the three standards EN 50126, EN 50128 and EN 50129 represents the backbone of the process of demonstrating the safety of a railway system.

The overall procedure of the railway standard EN 50126 is based on the life cycle model. The life cycle model distinguishes between different phases. Each phase contains well defined, phase-related tasks, which are general, RAM (Reliability, Availability, Maintainability) and safety tasks.

The CENELEC standards are based on the life cycle model as depicted in the following figure. This consists of a total of 14 phases, starting with the concept phase followed by system definition, risk analysis, system requirements, apportionment of system requirements, design and implementation, manufacture, installation, system validation and safety acceptance, system acceptance, operation and maintenance, de-commissioning and finally disposal. The concept also caters for the phases of performance monitoring, modification and retrofit, which are arranged in parallel to the operations and maintenance phase.

The single phases are described in detail in the standard EN 50126, defining each phase’s objectives, inputs, requirements and verification tasks. In most cases it might be necessary to adapt the V Model to the particular needs of the scheme.
3.3 New Revision of CENELEC Standards

The CENELEC railway application standards – introduced in the middle of the 1990’s and since then more and more proven in use – are now subject to review and revision.

This section reminds the motivation and the structure on the new revision of the CENELEC standards. The four following standards are currently under revision at CENELEC level: EN 50126, EN 50128, EN 50129 and EN 50155.

Historically driven, the standards EN 50126, EN 50128 and EN 50129 were developed by different working groups in overlapping periods of time. EN 50126 is dedicated to system approach to RAMS specification and demonstration. EN 50128 and EN 50129 are dedicated to communications, signalling and processing systems. EN 50155 is dedicated to electronic equipment used on rolling stock.

Since the date of issuing of these standards the railways safety context has significantly evolved in Europe. The Member States expressed the need for extending the scope of these standards in order to define a common approach to safety for the signalling systems, rolling stocks and fixed installations, in connection with RAM, thus to facilitate integration to the whole railway system.

The revision of EN 50126 with a new structure including EN 50128 and EN 50129 at system level is still in progress. No draft is available for the time being. Drafts for secretariat enquiry should be available in mid 2011.
The future EN 50126 “Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)” will consist of four parts:

- Part 1: Generic RAMS process
- Part 2: Systems approach to safety
- Part 4: Functional safety: Electric and electronic systems
- Part 5: Functional safety: Software

Part 3 (Safety management system for Railway Undertaking and Infrastructure Manager) is not decided yet.

The basis for these four parts is not only the current EN 50126, EN 50128 and EN 50129 but also the following documents:

- [TR 50126-2]: Guide to the application of EN 50126-1 for safety
- [TR 50126-3]: Guide to the application of EN 50126-1 for Rolling Stock RAMS
- [TR 50506-1]: Communication, signalling and processing systems - Application guide for EN 50129 – Part 1: Cross-acceptance
- [TR 50506-2]: Communication, signalling and processing systems – Application guide for EN 50129 – Part 2: Safety assurance
- EN 50155: Electronic equipment used on rolling stock

What concerns the life cycle model introduced in EN 50126, it has led operators and suppliers to adopt the fourteen life cycle phases of the standards and map their processes on them. Quite often, real life processes were for example “planning”, “design and manufacture”, “installation and test”, and “operation and maintenance”.

However, the life cycle model as practiced is well accepted today and has proven its suitability for more than a decade – similar to life cycle models in other safety critical industries.

Therefore, a change of the life cycle model is not expected in the new revision of EN 50126.
4 Methodology

This Chapter describes the methodology for the development of a common life cycle approach for urban guided transport systems.

The common life cycle approach proposal in general:

- applies for complete urban guided transport systems as well as for sub-systems,
- is based on the life cycle as defined in EN 50126,
- considers input and output per life cycle phase as specified in EN 50126,
- considers activities per life cycle phase as specified in EN 50126,
- does therefore NOT intend to copy & paste EN 50126 clauses,
- considers guidelines and code of practices as far as reasonable,
- specifies interfaces, roles and responsibilities within the life cycle approach,
- introduces principle processes and aspects per life cycle approach phase.

As a general rule, each life cycle approach phase requires the proper closure and the availability of the respective deliverables and documentation of the previous life cycle approach phase.
5 Common Life Cycle Approach Proposal

This Chapter defines the life cycle approach proposal for urban guided transport (UGT) systems under consideration. The life cycle approach should apply for the overall system including all technical sub-systems as well as operation and maintenance aspects.

Life cycle approach phases 1 to 4 are under the responsibility of the Operator to specify the requirements of the (new or modified) urban guided transport system.

Life cycle approach phases 5 to 9 are under the responsibility of the Supplier to build the system as specified; this includes the Supplier validation and acceptance of the system.

Life cycle approach phase 10 covers and ends with the Safety Authority’s licensing for commercial operation.

Life cycle approach phases 11 to 14 are under the obligation of the Operator and cover the operation and maintenance of the system (including performance monitoring and potential modification and retrofit) up to the potential decommissioning and disposal.

The following figure (taken from [TR SIG ZA]) shows the principle life cycle approach phases.

![Figure 3: Common Life Cycle Approach Proposal](image-url)
5.1 Concept

Sub-clause 5.1 provides an overview of the principle processes for the concept phase for a new urban guided transport system (life cycle approach phase 1).

The concept phase is used to develop a level of understanding of the (new) system sufficient to enable all subsequent lifecycle and respective tasks to be performed according to the initial intentions of the project.

The studies to be performed during the concept phase for new urban guided transport systems or extensions of existing systems have to take into account the existing institutional environment as well as the existing legislations into force regarding environment, land use and transportation planning. These regulations are mandatory for any construction activity, be it airports, roads, railways, infrastructure or buildings – public or private.

Besides institutional and legal aspects many other aspects have to be considered in order to provide enough details for a decision by relevant political authorities to agree on the project in terms of general development program and funding.

This “concept” phase includes successive studies (often repeated over time before a political decision is achieved) such as:

- Pre-Feasibility Studies (or part of a transportation plan) including transport planning and traffic forecast setting up and justifying the proposed main characteristics of the project, such as broad alignment, location of stations, overall functions and performance of the project, preliminary cost-benefit analysis.

- Feasibility Studies and Preliminary Design Studies.

- Cost-Benefit and Financial Analysis.

Information is provided on the volumes of passengers to be used for relevant preliminary and later more detailed design studies as well as on the main characteristics of the interfaces with other transport modes. Once the project approved, some detailed drawings can be produced.
The following figure shows the main actor for the Concept phase (life cycle approach phase 1). 

Figure 4: Life Cycle Approach Phase “Concept”

The main responsibility for the Concept phase (life cycle approach phase 1) is shared between the bodies in charge of the studies and the Political Decision Maker funding the project (the “Competent Authority” of the Public Service Requirements Regulation (EC) 1370/2007). The Safety Authority may be involved at an early stage of the design, however the Operator and, if any, the Safety Authority, start their work after the project programme has been approved by the Political Authority funding the project.” Refer to Figure 3 and Figure 23.
5.2 System Definition & Application Conditions

Sub-clause 5.2 provides an overview of the principle processes of the UGT system definition & application conditions phase (life cycle approach phase 2).

The planned system has to be defined specifically. This definition should take into consideration the scope, context and purpose of the system as well as environmental aspects such as system interfaces, physical issues and also financial, social and economical issues.

Therefore, in the early phase of system definition (life cycle approach phase 2), those comprehensive system safety concepts should be taken into account which might have an impact on the system decision and overall system design. These are:

- Basic operational concept (incl. Grade of Automation)
- Safety concept
- Safety concept in tunnels (if applicable)
- Evacuation and rescue concept
- Fire protection concept
- Environmental concept
- Concept for people with reduced mobility
- Integration of all different transport modes
- Interchanges with all transport modes including public transport internal interchanges
- Park and Ride concept
- Cyclists concept
- Pedestrian concept

As mentioned above, these aspects should be carried out as far as they have an influence on the system decision and overall system design. The comprehensive concepts at the system definition phase should outline the decisive requirements. They do not demand completeness. The complete requirements with respect to the comprehensive concepts will be part of the detailed requirements of the system requirements phase.
The following figure shows the main actor for the system definition & application condition phase (life cycle approach phase 2).

![Figure 5: Life Cycle Approach Phase “System Definition & Application Conditions”](image)

The main responsibility for the system definition & application condition phase (life cycle approach phase 2) lies with the Operator in simple cases of project development, but may involve other actors depending on the project development general organisation (e.g. Public Private Partnership). The Safety Authority should be informed about the (new) UGT system / sub-system definition. Refer to Figure 3 and Figure 23.
5.3 Risk Analysis

Sub-clause 5.3 provides an overview of the principle processes of the UGT system risk analysis phase (life cycle approach phase 3).

Following the definition of the Tolerable Hazard Rate / the Overall Safety Target for the overall system, a first Preliminary Hazard Analysis (PHA) should be produced immediately at the beginning of the development, as it forms the basis for the Safety Requirements Specification. In particular, the risk analysis should include:

- Identification of the hazards and risks for human lives (system users, staff, third party).
- Material and environmental injuries that can be caused by the system (i.e. certain physical or chemical properties, problems that the operator experiences while dealing with the system, failures of the system, e.g. resulting from internal defects).
- Consideration of events that cause hazards, which turn into unwanted incidents possibly causing accidents in a cause and effect chain (trigger events).
- Consideration of accident scenarios, which can be triggered by the cause and effect chain (e.g. consequence analysis).
- Consideration of external events, which may cause internal failures of the system and consequently cause events as described above.
- Consideration of external events, which directly influence the system and / or cause internal failures of the system and consequently cause events as described above.
- Evaluation of risks caused by the system as a combination of severity (possible effects) and frequency of an accident (without putting certain measures in place to reduce the probability, but under consideration of the possible external events).
- Identification of mitigation measures, which reduce the consequences or the probability of occurrence of these risks. These measures form the basis for the following Safety Requirements Specification.

As a result of the increasing experience with the future operational environment of the system and the development progress, the analyses become more detailed in the course of the development cycle (refinement from PHA to Hazard Analysis (HA)). The analyses can then refer to the overall system, to sub-systems, to safety functions or to sub-functions. The aspects of operation (including operation with driver or driverless operation) and maintenance are also considered.
The following figure shows the main actors for the risk analysis phase (life cycle approach phase 3).

Figure 6: Life Cycle Approach Phase “Risk Analysis”

The main responsibility for the risk analysis phase (life cycle approach phase 3) lies with the Operator, it may be proposed to be checked and audited by the Independent Safety Assessor. Refer to Figure 3 and Figure 23.

MODSafe has worked out a generic Risk Analysis [MODSafe D2.3] as well as a Hazard Control and Safety Measures Analysis [MODSafe D3.2]. Refer to Figure 1.
5.4 System Requirements

Sub-clause 5.4 provides an overview of the principle processes of the UGT system requirements specification phase (life cycle approach phase 4).

This section describes how the requirements should be developed for UGT application or sub-system to be compliant with applicable standards. The main focus has been set on the structure of the development phases and how this should be documented.

The specification of the system requirements should be strictly separated into Functional Requirements, Safety Requirements, Operational Requirements and Environmental Requirements. Functions (incl. safety functions) should be specified independently from potential technical solutions in the first instance.

Furthermore, it should be highlighted that requirements, e.g. Functional and Safety Requirements, are defined on system level, but detailed in the top-down approach for the related sub-functions and technical sub-systems. For example, on the system level, the system should respect the overall system performance and safety target requirements. But on sub-system level, the requirements differ for vehicle and station equipment.

The System Requirements Specification document should contain the initial design, which defines the technical properties of the (future) system. In particular, the UGT application's behaviour and its interfaces to the environment should be defined. The principle of a Black Box approach is valid. What the system should achieve should be detailed. However, how this achievement will be performed should not be specified. In particular, the document should describe:

- Type of system for which the application is planned (UGT system).
- Requirements with which the UGT application should comply.
- Standards, regulations and operator's requirements which should be considered.
- Safety requirements particularly derived from a Risk Analysis, with which the system should comply.
- The interfaces by which the system is interacting with other systems. This should comprise technical components as well as user interfaces.
- Performance and reaction times which the system should meet.
- Methods of verification for the requirements after completion (requirements should have clear acceptance criteria).
- Separation of safety-related requirements from non-safety-related requirements with well defined interfaces.
- Specification of external measures necessary to achieve the requirements.
The following figure is an approximate outline to identify the principle top-down process and its dependencies (document tree) as an outcome of the described system development process.

Figure 7: Proposed Requirement Specification Refinement
The following figure shows the main actors for the requirements specification phase (life cycle approach phase 4).

![Diagram of life cycle approach phase 4](image)

**Figure 8: Life Cycle Approach Phase "System Requirements Specification"**

The main responsibility for the system requirement specification phase (life cycle approach phase 4) lies with the Operator, it may be proposed to be checked and audited by the Independent Safety Assessor. Refer to Figure 3 and Figure 23.

MODSafe has worked out a “State of the art analysis and review of results from previous projects” [MODSafe D4.1] and an “Analysis of Safety Requirements for MODSafe Continuous Safety Measures and Functions” [MODSafe D4.2] and [MODSafe D5.2], complementary an “Analysis of On Demand Functions and Systematic Failures” [MODSafe D4.3]¹.

¹ refer to the note in sub-clause 1.1
5.4.1 Handling of different UGT systems

It is proposed to commonly handle the different urban guided transport systems such as light rail, tram or metro systems from the principle life cycle approach process and acceptance and approval point of view.

The obvious difference should be initially handled in the risk analysis and system requirements phase, where the different systems vary in their functional and technical needs and requirements. It goes without saying that an underground metro system has more safety scenarios to be considered than a tram – both in quantity and complexity. Requirement traceability and compliance demonstration is then handled throughout the further life cycle approach phases.

The following figure shows the principle process to handle the different UGT systems (light rail, tram, or metro) throughout the life cycle approach.

![Figure 9: Handling of different UGT systems](image-url)
5.4.2 Handling of different Grades of Automation

[MODSafe D6.2] concluded that the number and complexity of safety scenarios to be considered can be different depending on the grade of automation (GOA), but being based on the same legal basis and following the same principle life cycle approach approval process.

It is proposed to commonly handle the different grades of automation (GOA) such as operation with driver and unattended / driverless operation from the principle life cycle approach process and acceptance and approval point of view.

The obvious difference should be initially handled in the risk analysis and system requirements phase, where the different grades of automation vary in their functional and technical needs and requirements. It goes without saying that an unattended / driverless underground metro system has more safety scenarios to be considered than a tram with a driver – both in quantity and complexity. Requirement traceability and compliance demonstration is then handled throughout the further life cycle approach phases.

The following figure shows the principle process to handle the different grades of automation (GOA 1 – GOA 4) throughout the life cycle approach.

![Handling of different Grades of Automation](image-url)

**Figure 10: Handling of different Grades of Automation**
5.5 Apportionment of System Requirements

Sub-clause 5.5 provides an overview of the principle processes for the apportionment of system requirements (life cycle approach phase 5).

This section describes the division of the overall system / system functions into sub-functions and the corresponding assignment of safety integrity requirements.

Starting with the list of identified hazards from the initial risk analysis phase (ref. sub-clause 5.3), and under consideration of the related hazard control measures and system requirements (ref. sub-clause 5.4), tolerable hazard rates (THR’s) can be assigned to individual safety related functions / sub-functions.

Following the principle described in [CENELEC], tolerable hazard rates (THR’s) can be transferred to so-called Safety Integrity Levels (SIL). Safety integrity correlates to the probability of failure to achieve required safety functionality. Functions with greater integrity requirements are likely more expensive to realise. Safety integrity is basically specified for safety functions.

The concept of Safety Integrity Levels is used as a means of creating balance between measures to prevent systematic faults and random failures. Safety Integrity Level is defined by a range of values for tolerable rates of hazardous events and defines measures to be implemented into the design and procedures to overcome / avoid systematic faults.

The following figure shows the main actor for the apportionment of system requirements phase (life cycle approach phase 5).

![Figure 11: Life Cycle Approach Phase “Apportionment of System Requirements”](image-url)
Safety functions should be assigned to safety systems and/or to external risk reduction facilities. This assignment process is interactive, in order to optimise the design and cost of the overall system.

The main responsibility for the system architecture specification and safety requirement assignment process, the apportionment of system requirements phase (life cycle approach phase 5) lies with the Supplier, it may be proposed to be checked and audited by the Independent Safety Assessor. Refer to Figure 3 and Figure 23.

MODSafe has worked out a “State of the art analysis and review of results from previous projects” [MODSafe D4.1] and an “Analysis of Safety Requirements for MODSafe Continuous Safety Measures and Functions” [MODSafe D4.2], complementary an “Analysis of On Demand Functions and Systematic Failures” [MODSafe D4.3].

[MODSafe D4.1] describes methods for the allocation of safety integrity requirements on safety functions. It represents the state of the art of approaches described and outlined in standards and guidelines as well as actual methods used by railway operating companies.

[MODSafe D4.2] concludes the results of the safety requirement allocation process to continuous mode safety functions while [MODSafe D4.3] concludes the results of the safety requirement allocation process to on demand safety functions.

---

2 refer to the note in sub-clause 1.1
5.6 Design and Implementation

Sub-clause 5.6 provides an overview of the principle processes of the (new) UGT design & implementation phase, covering sub-processes such as detailed and final design (life cycle approach phase 6). Preliminary design is part of earlier life cycle phases.

Typical key processes, principles and general requirements for design are as follows:

- **Organisation:** The supplier should establish an organisation as appropriate, ensuring compliance with the relevant requirements. This should in particular include a safety management and verification and validation organisation appropriate for the relevant safety integrity of the system to be designed and developed.

- **Design and Development Process:** The supplier should establish a design and development process as appropriate, ensuring compliance with the relevant system requirements. This should also include a process to resolve failures and incompatibilities.

- **Quality:** The supplier should establish a quality management system including staff qualification and training, in particular covering design and development.

- **Environment:** The supplier should implement processes and measures to cope with environmental requirements for design and development.

- **Health and Safety:** The supplier should implement processes and measures to cope with health and safety requirements during design and development.

The following figure shows the main actor for the design and implementation phase (life cycle approach phase 6).

![Life Cycle Approach Phase “Design & Implementation”](image)
The main responsibility for the design and implementation phase (life cycle approach phase 6) lies with the Supplier, it may be proposed to be checked and audited by the Independent Safety Assessor. Refer to Figure 3 and Figure 23.

MODSafe has worked out an “Object Safety Model” [MODSafe D5.1], a “Combined Functional / Object Model [MODSafe D5.2] and a “Safety Attributes Allocation Matrix” [MODSafe D5.3].

[MODSafe D5.1] derives plausible object models for those entities that typically build up the safety functions analysed in [MODSafe D4.2] and as summarized in [MODSafe D5.2]. Finally, [MODSafe D5.3] provides a cross-reference between the objects / functions and the related hazards.

---

3 refer to the note in sub-clause 1.1
5.6.1 Handling of Sub-systems

This proposal mainly refers to the life cycle approach of an urban guided transport scheme that includes the integration of various sub-systems such as rolling stock, permanent way, signalling and communication, stations etc. This also covers renewal / modernisation projects where new sub-systems such as signalling or rolling stock are integrated into existing UGT systems, also affecting operational aspects in case of change in the Grade of Automation.

Therefore, for complex UGT systems, it is highly recommended to refine the general life cycle approach model in order to address overall system aspects as well as sub-system specific issues. Some of the equipment being used could also be developed as part of the project, but this activity would also have its own V life cycle approach that would integrate with the V life cycle approach of the overall project. This situation is illustrated in the figure below.

![Diagram](image)

Figure 13: Application of the life cycle approach for a system and its sub-systems
This means in practice, that the design and development processes for the individual sub-systems run in parallel. The sub-systems are developed, manufactured and tested in the factory (according to the respective sub-system life cycle approach) before finally being integrated into the overall urban guided transport system.

The handling of sub-systems depends on whether the sub-systems are part of an overall UGT system process or whether they are considered stand alone, for example a signalling / train control system in case of a signalling system renewal project or in the case of buying new Rolling Stock for an existing UGT system.

In the first case (sub-system part of a (new) overall UGT system), the sub-system may run its own life cycle approach as an “underlying life cycle approach”; this should apply at least for the signalling / train control sub-system. In the second case (stand alone sub-system), the sub-system may run its own life cycle approach as a “stand alone life cycle approach”; this should apply at least for the signalling / train control sub-system. In both cases, basically the same life cycle approach process applies as described for the overall UGT system, of course limited and focussed on the sub-system boundaries.
5.6.2 Handling of Sub-systems – Example CBTC Sub-system

Referring to the description of the requirement specification and refinement process on UGT system level in sub-clause 5.4 and Figure 7 and the application of the life cycle approach for a system and its sub-systems in sub-clause 5.4.1 and related Figure 13, the figure below shows an example of the specification and refinement process for a Communication Based Train Control (CBTC) sub-system.

![Diagram of CBTC System Specification and Refinement Process](image)

Figure 14: Example for sub-system specification refinement (CBTC system)
5.7 Manufacture

Sub-clause 5.7 provides an overview of the principle processes for the manufacture of new or modified UGT systems (life cycle approach phase 7).

Typical key processes, principles and general requirements for manufacture from a life cycle approach perspective are as follows:

- **Manufacturing Process**: The supplier establishes a manufacturing process as appropriate, ensuring compliance with the relevant design intend and requirements. It could also include a process to resolve failures and incompatibilities.

- **Factory Testing**: The supplier establishes a factory test process as appropriate, ensuring compliance with the relevant test requirements. This also includes a process to resolve failures and incompatibilities.

- **Quality**: The supplier establishes a quality management system including staff qualification and training, in particular covering manufacture and factory processes.

- **Environment**: The supplier implements processes and measures to cope with environmental requirements for manufacture.

- **Health and Safety**: The supplier implements processes and measures to cope with health and safety requirements during manufacture.

The following figure shows the main actor for the manufacture phase (life cycle approach phase 7).

![Figure 15: Life Cycle Approach Phase “Manufacture”](image_url)

The main responsibility for the manufacture phase (life cycle approach phase 7) lies with the Supplier. Refer to Figure 3 and Figure 23.
5.8 Installation

Sub-clause 5.8 provides an overview of the principle processes for the installation of new or modified UGT systems (life cycle approach phase 8).

Typical key processes, principles and general requirements for manufacture are as follows:

- **Installation Process:** The supplier establishes a field installation process as appropriate, ensuring compliance with the relevant system integration intend and requirements. It could also include a process to resolve failures and incompatibilities.

- **Field Testing:** The supplier establishes a field test process as appropriate, ensuring compliance with the relevant test requirements. This also includes a process to resolve failures and incompatibilities.

- **Quality:** The supplier establishes a quality management system including staff qualification and training, in particular covering field installation.

- **Environment:** The supplier implements processes and measures to cope with environmental requirements for installation.

- **Health and Safety:** The supplier implements processes and measures to cope with health and safety requirements during installation.

The following figure shows the main actor for the installation phase (life cycle approach phase 8).

![Figure 16: Life Cycle Approach Phase “Installation”](image)

The main responsibility for the installation phase (life cycle approach phase 8) lies with the Supplier. Refer to Figure 3 and Figure 23.
5.9 System Validation & Safety Acceptance

Sub-clause 5.9 provides an overview of the principle processes for the system validation & safety acceptance of new or modified UGT systems (life cycle approach phase 9).

Verification and Validation applies on both, UGT system level (ref. EN 50126) as well as for sub-systems, at least for the signalling and train control sub-system (ref. EN 50128 and EN 50129). This means, that validation & safety acceptance applies first for the signalling and train control sub-system for the sole sub-system functions and second for the whole UGT system with respect to functional integration and interfaces incl. operational aspects. Figure 13 shows the interrelationship between the sub-system’s validation and the UGT system validation.

The following figure shows the main actors for the system validation & safety acceptance phase (life cycle approach phase 9).

Figure 17: Life Cycle Approach Phase “System Validation & Safety Acceptance”

The main responsibility for the verification and validation phase (life cycle approach phase 9) lies with the Supplier, it may be proposed to be checked and audited by the Independent Safety Assessor. Refer to Figure 3 and Figure 23.
5.9.1 Supplier's Verification and Validation

The CENELEC standards define the so called verification and validation activities, which lie in the sole responsibility of the supplier. The standards define requirements regarding the independence and qualification of the supplier's verification and validation staff. Verification means the confirmation by examination and provision of objective evidence that the specified requirements have been fulfilled, and is performed in each life cycle approach phase against the requirements of the previous life cycle approach phase.

Validation means the confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use have been fulfilled, and is performed during life cycle approach phase 9 (System Validation & Safety Acceptance) against the design intend as specified in life cycle approach phase 4 (Requirements Specification).

The following figure shows the principle relationship of the verification and validation in relation to the life cycle approach phases. The activities as such are described in the respective standards as mentioned above.

![Figure 18: Supplier's Verification and Validation throughout the life cycle approach](image-url)

Figure 18: Supplier’s Verification and Validation throughout the life cycle approach
5.9.2 Integration of Sub-systems into UGT System Safety Case

Overall, the system life cycle approach phases 1-5 provide the input and requirements for the individual sub-systems, whereas each sub-system itself (once having completed the sub-system design and development process) comes with potential application conditions and Operation & Maintenance requirements to be observed on system level forming the input for life cycle approach phases 8 – 10.

On this basis, the overall life cycle approach (as well as the Independent Safety Assessment process) can focus on a clear and precise set of Safety Documentation and afterwards on thorough checks, that the defined targets have been achieved. The following figure shows the principle hierarchy of safety documentation, following a top-down approach at the beginning of the project (life cycle approach phases 1-5) and a final bottom-up approach for the collection of the sub-system safety evidence (life cycle approach phases 8-10) and forming an integrated system level safety case.

![Principle Hierarchy and Structure of Safety Documentation](image)

The cited MODSafe deliverables can be used as far as the sub-system under consideration is concerned. Especially for the signalling / train control sub-systems, the MODSafe deliverables are of benefit since the majority of UGT hazards and requirements are mainly related to the signalling and train control system.
5.10 System Acceptance

Sub-clause 5.10 provides an overview of the principle processes for system acceptance for a new or modified UGT system (life cycle approach phase 10).

The standard EN 50126 “does not define an approval process by the safety regulatory authority” (ref. section Scope of the standard). The standard is applicable “for use by Railway Authorities and railway support industry” (ref. section Scope of the standard) and therefore offers a sound basis for the definition of an approval process under consideration of the specific needs and local specialities.

This section defines the approval process which could be applied for new or modified UGT systems. Beyond Safety, the approval process could also cover RAM aspects.

The approval process should be based on the life cycle approach model as defined in Sub-clause 3.2. As an integral part, the CENELEC approach and process requires an appropriate safety management concept. Like the well known quality management concept ISO 9001, the CENELEC safety management concept establishes the assumption that the level of safety of a complex product can seldom be proven simply by testing the finished product - especially with regard to electronic software and hardware components this is impossible. Safety just like quality has to be an integral part of the design and production process in order to lead to products that possess a suitable level of safety. Furthermore, the required level of safety of a product is hugely dependent upon on the system it will be embedded in.

The CENELEC safety management system therefore lends itself for combination with more prescriptive safety standard / regulation series, which may differ throughout the European member states.

In Germany for example, the BOStrab (German Federal Regulations on the construction and operation of light rail transit systems) does not only apply to conventional tramway systems - as the title may imply - but also to (new) types of urban guided transport systems including fully automatic systems. BOStrab distinguishes between the inspection of documents, the inspection during manufacturing and the final safety acceptance as the different main steps of the assessment. BOStrab further refers to the "generally accepted rules of technology" (GARTs), represented by a series of light rail safety standards.

In conclusion, it can be stated, that CENELEC and further appropriate national safety standards / regulations form a sound basis for the approval process of new or modified UGT systems. Respective safety concepts and a safety demonstration / approval process can be derived thereof.
The following figure shows the main actors for the system acceptance phase (life cycle approach phase 10).

![Diagram showing the main actors for the system acceptance phase]

**Figure 20: Life Cycle Approach Phase “System Acceptance”**

The main responsibility for the acceptance phase (life cycle approach phase 10) lies with the Operator and possibly the Safety Authority, it may be proposed to be checked and audited by the Independent Safety Assessor. Refer to Figure 3 and Figure 23.

MODSafe has worked out a proposal for a typical optimized Approval, Acceptance and Certification process [MODSafe D7.4]⁴.

---

⁴ refer to the note in sub-clause 1.1

Doc Name: DEL_D6.3_TRIT_WP6_V1.0_110531.doc  Date: 110531
ID: DEL_D6.3_TRIT_WP6_110531_V1.0  Revision: V1.0  Page 44/58
5.10.1 Approval Milestones

The more complex the system the more detailed has the approval process to be planned. The life cycle approach model (also in conjunction with other standards / regulations) may form the basis to define an Acceptance / Authority Approval Process based on Authority Approval Milestones derived from the life cycle approach.

In order to allow for a project accompanying safety approval and continuous evaluation, whether all relevant safety activities and the corresponding submittals are in place, it is recommended to introduce interim Safety Approval Milestones after certain life cycle approach phases.

The following project milestones / safety approval milestones are recommended. They should be matched with respective supplier's project planning. The final definition of milestones is topic of mutually agreement between the actors affected namely the Safety Authority, the Independent Safety Assessor, the Operator and the Supplier.

![Figure 21: Safety Approval Milestones – Examples](image)

Doc Name: DEL_D6.3_TRIT_WP6_V1.0_110531.doc  Date: 110531
ID: DEL_D6.3_TRIT_WP6_110531_V1.0  Revision: V1.0  Page 45/58
5.10.2 Independent Safety Assessment

If there is – as recommended - an agreement between the Safety Authority and the Operator and if applicable the Supplier to involve an Independent Safety Assessor, the following rules should be respected.


It might be recommended to use an “Independent Safety Assessor” at least for the overall UGT system comprehensive aspects as well as for the sub-system signalling and train control. The initial introduction and involvement of an Independent Safety Assessor should take place in the early life cycle approach stages.

If the safety case concept of EN 50129, after matching it to individual technologies, is applied on a total system basis including all sub-systems, then an appropriately distributed safety level for the whole rail system can be achieved. This implies that independent safety assessment of the safety evidence of all included sub-systems has also been performed.

The Independent Safety Assessor’s role is to verify, that the required level of safety and quality is achieved by all actors concerned to ensure a safe implementation of the project to the required safety standards.

The Independent Safety Assessment Services should be performed following the principles and processes described in the CENELEC Railway Application Standards EN 50126 and EN 50129.

This means that the Supplier carries the overall responsibility for the detailed Verification & Validation activities and thus the evidence of safety within his contractual scope, whereas the Independent Safety Assessment will focus on the judgement whether the Supplier’s Verification & Validation (V&V) and Safety Management Organisation has applied appropriate processes and techniques in line with the requirements of the standards.

It is the goal of an Independent Safety Assessment to put the Safety Authority into a position to grant the allowance for operations (licensing) after the finalisation of all necessary evaluations, examinations, analyses, inspections, tests, etc.

The license can be issued for single modes or sub-modes of operation.

At the discretion of the Safety Authority, an Independent Safety Assessor may be part of the supplier's organisation or operator’s organisation but, in such cases, the assessor should

- be authorised by the Safety Authority,
- be totally independent from the project team,
- report directly to the Safety Authority.
The following figure shows the suggested involvement of the Independent Safety Assessor in relation to the life cycle approach phases. At the discretion of the Operator and/or the Safety Authority, the Independent Safety Assessor may be involved in all life cycle approach phases.

MODSafe has worked out a proposal for a typical optimized Approval, Acceptance and Certification (AAC) process with the involvement of an Independent Safety Assessor [MODSafe D7.4].

---

5 refer to the note in sub-clause 1.1
5.10.3 Life Cycle Approach Phase related Roles and Responsibilities

The following figure (taken from [TR SIG ZA]) shows the life cycle approach phase related roles and responsibilities and related interfaces, in particular the involvement of an Independent Safety Assessor (if required) and a Safety Authority. In individual cases the Operator may be the Safety Authority.

![Figure 23: Life Cycle Approach related roles, responsibilities and interfaces](image)

---

**Legend:**
- Final Safety Case
- Assessor Report
- Authority Approval
5.10.4 Application of Cross-Acceptance

The application of cross-acceptance has been described in [MODSafe D6.2]. The following figure (taken from [TR SIG ZA]) shows the principle process of the application of cross-acceptance, meaning the re-use of available equipment / products / sub-systems already pre-approved / pre-certified as generic products or generic applications.

![Diagram of the Process of Application of Cross Acceptance]

**Figure 24: Process of Application of Cross Acceptance**

The decision process should be applied in the early life cycle approach stages on UGT system level and / or at the beginning of the design stage in case of applying for sub-systems such as re-use of pre-approved signalling and train control equipment.

The Acceptance Criteria for Cross-Acceptance can be derived from [TR 50506-1].
5.11 Operation & Maintenance

Sub-clause 5.11 provides an overview of the principle processes for operation and maintenance for a (new or modified) UGT system and its sub-systems (life cycle approach phase 11).

The operator ensures that the requirements for safe and proper operation are met. He in particular makes absolutely certain, that the installations and vehicles are always in proper condition and that operation is conducted safely.

The operator is required in the selection, deployment and supervision of operational staff to ensure safe and orderly convenience of passengers.

Typical key processes, principles and general requirements for operation and maintenance from a life cycle approach perspective are as follows:

- Operations Licence: Commercial operation requires licensing by a Safety Authority. The licence shall be available prior to start of operation (life cycle approach phase 11).

- Operation Plan: The Operator of an UGT system develops a comprehensive operation plan for the complete system covering at least performance targets, operating strategies, handling of all safety relevant functions and systems as well as key processes and staffing, etc.

- Maintenance Plan: The Operator / maintainer of an UGT system develops a comprehensive maintenance plan for the complete system covering at least key reliability, maintainability and availability targets, maintenance conditions, maintenance strategies (preventive / corrective maintenance), facilities, logistics, costs, as well as key processes and staffing, etc.

- Operation Procedures: The manual of operating procedures provide detailed instructions for the operation of the system such as e.g. start up, shut down, modes of operation and changing, vehicle dispatching, vehicle operation and function, controlling the system consoles, failure management, emergency response, passenger communications, service, power distribution system management, etc.

- Maintenance Procedures: The manual of maintenance procedures provide detailed maintenance instructions for the system such as e.g. main steps, frequency and duration, necessary equipment and components, execution of work, results, documentation, effort estimates, etc.
• Driverless / Unattended Operation: In case of driverless / unattended operation, the operational concept and procedures reflect the UGT system features (e.g. evacuation and rescue concept, safety concept in tunnels), various functions (e.g. obstacle detection) that are to be performed by technical means (instead of by a driver). The initial version of the operational concept and procedures or at least the initial concepts with respect to driverless / unattended operation is available during the early life cycle approach phases 1-4 (refer to Figure 23).

• Quality and Safety: The Operator / maintainer establish a performance and quality policy, a quality management system including staff qualification and training. The quality system is maintained throughout the entire operation life time of the UGT system / the entire life cycle approach phase 11 (which may last decades).

• Environment: The Operator / maintainer establish an environmental policy, an environmental management system to fulfil all legal and operational provisions as well as emergency preparation and response procedure for the event of an environmental threat. The environmental management system is maintained throughout the entire operation life time of the UGT system / the entire life cycle approach phase 11 (which may last decades).

• Contingency: The Operator creates and introduces a contingency plan before commencing the operation. A contingency plan has the objective to document and to instruct how to operate in an emergency case. The contingency plan is available during life cycle approach phase 10 at the latest since it is subject to approval and a prerequisite for licensing.

• Authority Approval: The initial version of the operation plan and maintenance plan or at least the initial concepts are available during the early life cycle approach phases 1-4 (refer to Figure 23). The Operator’s / maintainer’s management systems, operation and maintenance procedures are available during life cycle approach phase 10 at the latest since they are subject to Safety Authority approval and a prerequisite for licensing.

• Supervision: The Supervisory Authority supervises the operation and maintenance of the UGT system. This is an ongoing task and applies throughout the entire operation life time of the UGT system / the entire life cycle approach phase 11.

• Outsourcing: Operators can outsource (parts of) the operation and maintenance and functions. However, the Operators’ obligations to the supervisory authorities remain unchanged.
The following figure shows the actors and key processes for operation (life cycle approach phase 11).

Figure 25: Life Cycle Approach Phase “Operation & Maintenance”

The main responsibility for operation and maintenance (life cycle approach phase 11) lies with the Operator / maintainer; generally supervised by the Supervisory Authority. Refer to Figure 3 and Figure 23.
5.11.1 Operations Manager Concept

The operator, in fulfilment of the obligations placed upon him by these regulations and without diminishing in any manner his personal responsibility, may appoint responsibility to an Operations Manager.

Sub-clause 5.11.1 provides – as an example - a brief description of the Operations Manager Concept, which is used in Germany according to BOSstrab (German Federal Regulations on the construction and operation of light rail transit systems). This concept has also been used for the Copenhagen Metro in Denmark. The German term for Operations Manager is “Betriebsleiter”.

The operations manager concept anchors responsibilities for operational safety and for security in the organisational structures of UGT operators and transfers some functions of the supervisory authority directly to the operators (so called government relieving activities). By that outsourcing of supervisory functions the operator is very efficient in duty to ensure the operational safety and the authority will be partly discharged from liabilities for internal procedures of operators.

This applies to operators of UGT systems as well to the operators of networks as to the operators of rolling stock, if these subsystems are operated by different undertakings.

5.11.2 Operations Manager Duties

The Operations Manager acts in functional and legal relationships to the Operator’s board, operational staff, and the Supervisory Authority.

In relationship to the operator’s board, the operations manager is the competent person in all questions of operational safety and security. He reports to as well as advises and consults the board in all safety and security relevant questions. He has no veto against decisions of the board. But if he can not accept and take into his responsibility the boards decisions or actions he is by law on duty to inform the authority directly without delay. By that duty - it is not only a right to inform the authority - the operational safety gains a very strong position in the management procedures of the operator.

In relationship to the safety relevant operational staff, including superiors, the operations manager ensures that there is transparency and he may take measures as he sees fit. At any given time, and in respect to every safety relevant matter, the operations manager can assign and instruct members of the safety relevant operational staff. The operations manager can give internal rules, guidelines, regulations, decrees and procedures for ensuring the operational safety and the security.

In relationship to the supervisory authority the operations manager has to report directly to the authority and vice versa he receives supervisory advice and instructions.

In consequence there is a triangle of relations - duties and rights - between the operations manager, the operator’s board and the supervisory authority.
5.12 Performance Monitoring

Sub-clause 5.12 provides an overview of the principle processes for performance monitoring of UGT systems (life cycle approach phase 12).

Performance monitoring is an UGT life cycle approach phase which is timely running in parallel with the operation and maintenance of the system / with life cycle approach phase 11.

Typical key processes, principles and general requirements for performance monitoring from a life cycle approach perspective are as follows:

- Data Establishment: The Operator of the UGT system implements processes and measures for the regular collection of relevant performance / RAMS data.

- Analysis: The Operator of the UGT system implements a process for the regular analysis and statistical evaluation of the performance / RAMS data. A review of results in improvement / corrective actions for the further operation and maintenance of the system as needed.

- Record: The Operator of the UGT system regularly records and report on the results of the performance monitoring, including corrective actions, if any. The report is generally submitted to the Supervisory Authority.

The following figure shows the actors and key processes for performance monitoring.

The main responsibility for performance monitoring (life cycle approach phase 12) lies with the Operator; generally supervised by the Supervisory Authority. Refer to Figure 3 and Figure 23.

Figure 26: Life Cycle Approach Phase “Performance Monitoring”
5.13 Modification & Retrofit

Sub-clause 5.13 provides an overview of the principle processes for modification and retrofit of UGT systems (life cycle approach phase 13).

Depending on the impact on the existing UGT and the corresponding need for approval, the re-application of the life cycle approach should consider the nature of modification and retrofit.

Basically, the following types of modification and retrofit can be assumed:

- Complete shut down of an existing UGT system to be substituted by a new one
- Extension of an existing UGT system, e.g. extension of a line or building of a new line
- Modernisation / upgrade of a sub-system, e.g. renewal of the signalling and control system or upgrade to a Communication Based Train Control (CBTC) system
- Renewal of Rolling Stock, modernisation or new vehicles
- Upgrade of an existing UGT system operational mode, e.g. upgrade to driverless operation

The following figure shows the life cycle approach re-entry points for the different types of modification and retrofit (life cycle approach phase 13). Extension, modernisation / upgrade or renewal should usually re-entry in life cycle approach phase 2 since the operational concept or safety concept or application conditions might be affected and subject to modification.

Cross-Application should be applied to the extent possible (refer to sub-clause 5.10.4).
The main responsibility for modification and retrofit (life cycle approach phase 13) lies with the Operator; with generally the involvement of a Safety Authority, (refer to Figure 3).
5.14 Decommissioning & Disposal

Sub-clause 5.14 provides an overview of the principle processes for decommissioning & disposal of UGT systems or parts thereof (life cycle approach phase 14).

Decommissioning and disposal (life cycle approach phase 14) may run in parallel with modification and retrofit (life cycle approach phase 13).

Basically, the following types of decommissioning and disposal can be assumed:

- Complete shut down of an existing UGT system to be substituted by a new one, i.e. decommissioning and disposal of an existing UGT system
- Modernisation / upgrade of a sub-system, e.g. renewal or upgrade of the signalling and control system, i.e. decommissioning and disposal of the old sub-system
- Renewal of Rolling Stock, modernisation or new vehicles, i.e. decommissioning and disposal of the old vehicles

Typical key processes, principles and general requirements for decommissioning and disposal from a life cycle approach perspective are as follows:

- Environment: The Operator of the UGT system implements processes and measures to cope with environmental requirements for decommissioning and disposal
- Health and Safety: The Operator of the UGT system implements processes and measures to cope with health and safety requirements during decommissioning and disposal. This includes operational precautions in case decommissioning is performed during normal operation or under specified conditions.
- Report: The Operator of the UGT system reports on the results of the decommissioning and disposal, as needed to relevant authorities, if any.

The main responsibility for decommissioning and disposal (life cycle approach phase 14) lies with the Operator. Refer to Figure 3 and Figure 23.
6 Summary and Conclusion

The deliverable at hand defines and proposes a common safety life cycle approach for urban guided transport systems. It should be read in conjunction with [MODSafe D7.4], which provides a proposal for acceptance, approval and certification of urban guided transport systems.

The potential future common life cycle approach for planning, building, assessing and approving the different stages and corresponding safety files considers the different responsibilities along the life cycle approach and the roles and authorizations of the different actors.

The proposed life cycle approach applies for both, urban guided transport systems as a whole as well as for its sub-systems such as signalling and train control, Rolling Stock, etc.

The proposed life cycle approach allows for consideration of the life cycle costs associated with the RAMS aspects of an UGT system due to the structured, top down and risk based approach.

Following and based on the analyses and evaluations performed, the proposal at hand is backed by proven practice and similarities throughout the European member states.