TÜV Rheinland Group

TÜV InterTraffic GmbH
ISA – Independent Safety Assessment

Initial Assessment Report on the Level Maturity for Safe Application of the SKY BUS Metro System Concept (Konkan Railways, India)

Cologne, 2004-06-30

Report –No.: 101/B 04/206

Authors: Dipl.-Ing. Thomas Brandt, TÜV InterTraffic GmbH

Dipl.-Ing. Winfried Steinert, TÜV InterTraffic GmbH

Dipl.-Ing. Peter Wigger, TÜV InterTraffic GmbH

Dipl.-Ing. Maik Wuttke, TÜV InterTraffic GmbH

Reviewers: Dipl.-Ing. Srinivas Chakravarthy, TÜV Rheinland India Pvt. Ltd.

Dr. Herbert Jansen, TÜV InterTraffic GmbH

TÜV Rheinland Group

Initial Assessment Report on the Level Maturity for Safe Application
of the SKY BUS Metro System Concept (Konkan Railways, India)

Report No.:	101/B 04/206
Date:	2004-06-30
Number of pages:	74
Item under Inspection:	Conceptual Design Document Sky Bus Metro Concept Version 1 – November 05, 2003
Client:	Konkan Railway Corporation, Limited (a Government of India Undertaking)
Order / Date:	KR/CO/SG/ITS / March 15, 2004
Report performed by:	TÜV InterTraffic GmbH ISA – Independent Safety Assessment Am Grauen Stein, 51105 Cologne Germany
Communication through	TÜV Rheinland India Pvt. Ltd. 504-506 Prestige Center Point Cunningham Road, Bangalore, Republic of India
TÜV Order Number:	101 – 477020 Pos. No. 0
Authors of Report:	Dipl.-Ing. Thomas Brandt, TÜV InterTraffic GmbH Dipl.-Ing. Winfried Steinert, TÜV InterTraffic GmbH Dipl.-Ing. Peter Wigger, TÜV InterTraffic GmbH Dipl.-Ing. Maik Wuttke, TÜV InterTraffic GmbH
Reviewer of Report:	Dipl.-Ing. Srinivas Chakravarthy, TÜV Rheinland India Pvt. Ltd. Dr. Herbert Jansen, TÜV InterTraffic GmbH
Project Manager:	Dipl.-Ing. Maik Wuttke, TÜV InterTraffic GmbH
Result:	**Refer to chapter 0, Executive Summary**

Table of Contents

List of Tables

List of Figures

List of Attachments

Terms and Definitions

Assessment	The process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for it intended purpose.
Validation	The activity applied in order to demonstrate, by test and analysis, that the product meets in all respects the specified requirements (ref. EN 50129)
Verification	The activity of determination, by analysis and test, at each phase of the life cycle, that the requirements of the phase under consideration meet the output of the previous phase and that the output of the phase under consideration fulfils its requirements (ref. EN 50129)

List of Abbreviations

ALARP	As Low As Reasonably Practicable
ATP	Automatic Train Protection
BOStrab	Verordnung über den Bau und Betrieb der Straßenbahnen BOStrab (Federal Regulation for the Construction and Operation of Tramways, which is applicable in Germany for driverless urban mass transit systems)
CDD	Conceptual Design Document, Version 1
CENELEC	European Committee for Electrotechnical Standardization (Comité Européen de Normalisation Électrotechnique)
EN	European Standard (Norm)
EMC	Electromagnetic Compatibility
FMEA	Failure Modes and Effects Analysis
GAMAB	Globalement Au Moins Aussi Bon
ISO / IEC	International Organisation for Standardisation / International Electrotechnical Commission
KRCL	Konkan Railway Corporation Limited, a Government of India Undertaking
MEM	Minimum Endogenous Mortality
PHA	Preliminary Hazard Analysis
PPHPD	Passengers per hour per direction
RAMS	Reliability, Availability, Maintainability, Safety
SIL	Safety Integrity Level
THR	Tolerable Hazard Rate
V&V	Verification & Validation

0 Executive Summary

The subject of this report is the Sky Bus Metro system concept under development by Konkan Railway Corporation Limited (KRCL), a Government of India Undertaking, as described in the Conceptual Design Document, Version 1, KRCL, 09.01.2004.

This report provides the results of the determination of the "Level of Maturity for Safety Application" of the Sky Bus Metro system concept before starting a CENELEC safety certification according to EN 50126 - EN 50129.

The results are limited to the information supplied in the Conceptual Design Document, Version 1, KRCL, 09.01.2004.

The results can be summarized as follows:

The general concept of Sky Bus Metro as a suspended light rail system appears technical feasible as a mass transportation system and development potential to reach a state required for safe implementation has been identified, based on a number of conditions as per chapter 0.

In general the currently available information given in the Conceptual Design Document, Version 1, KRCL, 09.01.2004 is not consistent enough to make a more detailed decision about the level of maturity of the Sky Bus Metro system concept in terms of safety.

Regarding a proper CENELEC safety certification and management approach further steps are recommended in chapter 7.3.

1 Scope

1.1 Introduction

Konkan Railway Corporation Limited (KRCL), a Government of India Undertaking, plans to develop a holistic Urban Mass Transit System which can transport people or carry containers. The top of the guideway construction shall further serve as basis for developing shop, office or housing buildings along the route.

The idea of Sky Bus Metro is to use existing and proven technologies and recombine them into a new method of a transport system where the coaches are suspended from bogies running overhead on rails in a concrete box girder. The basic vehicle will be a Sky Bus Consist of two coaches which will be carrying 300 passengers. Maximal three of this Sky Bus Consists shall be combined to a train of six coaches.

The conceptual design determines a maximum speed of 100 kph and a headway between 40 seconds and 1 minute in a fully automated system controlled by a microprocessor based signalling and control system. This will lead to a capacity of the entire system of up to 81,000 PPHPD.

The risks of a newly designed mass transport system even with adopting proven technologies from other systems can not all be minimised by testing with following trial and error development. It is of high importance that the obvious as well as hidden safety implementations of the new system are systematically identified and addressed during the progress of the project. In order to prove the quality of the safety management during the design as well as the construction of the system KRCL has opted to employ the world wide accepted CENELEC (Comité Européen de Normalisation Électrotechnique) safety certification and safety management process. The process requirements are laid down in the standards EN 50126 to EN 50129. When starting to design a publicly operating system the CENELEC safety certification and safety management process has to be employed from start of design through to passenger operations. In order to successfully certify the safety of an ambitious project of the size of Sky Bus Metro to the CENELEC process, the production quality and work quality of the mechanical and civil engineering works is as important as the design calculation and documentation, due to the fact that production faults in highly loaded structures can often not be identified retrospectively.

This study shall serve as a preliminary step to assess the current status of the Sky Bus Metro concept and to determine the “Level of Maturity for Safety Application”.

Figure 1 shows the design demonstrator of Sky Bus Metro built at Madgaon, Goa.

Figure 1: Design demonstrator at Madgaon, Goa

1.2 The Task

The task of this initial assessment is to determine “the Level of Maturity for Safe Application” of the Sky Bus Metro concept before starting a CENELEC safety certification according to EN 50126-EN 50129.

The CENELEC process has to cover the entire system and has to be strictly performed in parallel to the engineering progresses during design and construction. It is not possible to successfully assess any finished systems after completion in retrospective.

This study shall mainly be based on the document: Conceptual Design Document, Version 1, from 09-Jan-2004 as prepared by KRCL. The assessors had the possibility to inspect the technology demonstrator at Madgaon, Goa and discuss some technical aspects with the KRCL design team.

The revision and assessment of the provided calculations, drafts and expertises up to now has raised a couple of questions as shown before in the Commencing Report on the Work document from September 2003. In addition to the statements at that time, this assessment report will give further and more detailed statements of the current and expected safety level of Sky Bus Metro.

The whole assessment will be performed in a sequence of four steps of which this declaration will be the completion of step 1 (Phase I, Part A1).

According to the defined scope of work which shall eventually lead to a safety certification to the CENELEC process, this step 1 initial step is intended to:

- achieve a thorough understanding of the Sky Bus Metro technology,
- verify all safety-related aspects of the relevant sub-systems and the overall system,
- issue an initial declaration of the level of “Maturity for Safe Application”

which is now presented with the assessment report at hand.

The next steps are to establish a certification plan and afterwards the certification itself which will be based on the required inspections.

The presented assessment does neither include checking of any quantitative assumptions of any kind nor incorporate detailed review of static calculations.

2 Basis of the Inspection

The assessment will employ world wide accepted and practically proven safety concepts on guided transport technology for reference. These are mainly the CENELEC standards on safety management and the BOStrab set of rules and regulations for design and operations of metro and light rail systems. Additional relevant and internationally accepted and used standards will be introduced to serve as reference to state of technology.

A listing of these standards is given in annex 1.

A detailed choice and customising of appropriate standards for the Sky Bus Metro development process is an important part of future steps of the CENELEC process and has therefore been omitted from this initial step.

3 Sky Bus Metro Concept (Item under Inspection (IUI))

The Sky Bus Metro system is a world unique idea and concept to create a suspended dual rail Urban Mass Transport System. Several new patents are closely related to the Sky Bus Metro technology. The system uses existing and proven technology aspects and recombines them in new concept. This offers many opportunities as well as it contains a lot of technological, economical and safety related risk potential like every new technology does. To reduce this risk potential suitable standards can be used to increase safety as well as system availability. Where no suitable standards exist, individual system related solutions have to be established.

While designing and constructing the Sky Bus Metro system it has to be kept in mind that using technology aspects which are proven for decades in other systems and functions does not allow to assume that it is safe to use them

- in the new and different environment,
- in new design combinations,
- under new physical constraints and interfaces,
- with new production procedures,
- within the proposed Sky Bus Metro specific operation procedures

at the Sky Bus Metro system without thorough investigation where required.

The review and initial assessment of the provided Sky Bus Metro system concept has in this regard let to specifically addressing a number of aspects in the succeeding chapters. The assessors notes are systematically assigned to the following subsystems and functions:

- Introduction to CENELEC Safety Certification Approach
- From Theory to Practice – How to introduce a Sky Bus Metro Certification Process
- Assessment of Sky Bus Metro Concept on its Maturity for Safe Implementation
  - Formal Criteria
  - Initial Assessment Results
    - System Level
    - Guideway
    - Sky Stations and Platforms
    - Rolling Stock

  - Rail-wheel interaction
  - Signalling and Control
  - Traverser
  - Power Supply and Propulsion System
  - Maintenance Concept
  - Emergency concept
- Summary of Assessment

Available Information about the concept of Sky Bus Metro:

The initial assessment of the sub-systems as well as of the overall system is based on the Conceptual Design Document, Version 1, from 09-Jan-2004. Further design information are taken from the video and PowerPoint presentation of the Sky Bus Metro system received in January 2004 as well as handed over during the visit of two assessors from TÜV InterTraffic GmbH at Mumbai and Goa in September 2003.

More design information was sent in May 2004 answering the assessors questions and notes shown in the “Notes on Visit to Mumbai” from September 2003.

In general, all available documents do provide a high level overview about the Sky Bus Metro Concept. Some isolated aspects of the system have been covered in more detail.

The nature of the available documentation is appropriate to the level of detail required for this initial study.

4 Introduction to CENELEC Safety Certification Approach

To date the European railway standards EN 50126, EN 50128 and EN 50129 have reached a mature state and are implemented at practically every new rail technology project. They have been developed by CENELEC (Comité Européen de Normalisation Électrotechnique) the European Committee for Electrotechnical Standardization in Brussels. These standards do not only apply to heavy rail systems - as their heading 'Railway applications' may imply, but also to light rail and urban mass transportation including people mover systems.

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 EN 50121 on electromagnetic compatibility or EN 50159 on 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 standards introduce a probabilistic approach, – in the past mainly used in nuclear and aerospace technologies, into rail technology. The standards further provide a structured approach and flexible methodology, they standardize the demonstration of system safety of complex rail systems and they allow the integration of proven and new technologies and the matching of the safety case concept to all sub-systems.

They 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 applies to safety-related electronic control and protection systems, and EN 50128 applies to (safety related) software for railway control and protection systems. The standards 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 CENELEC standards have already caused interest in the European approach also in the US and in Asia and meanwhile the CENELEC standards are on the way to be transferred to ISO / IEC standards.

As an integral part, the CENELEC certification approach and process requires an appropriate safety management concept. Like the well known quality management concept ISO 9000, 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 soft- 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 a product that possesses a suitable level of safety. Furthermore the required level of safety of product is hugely depending on the system it shall be embedded in.

The CENELEC safety management system therefore leads itself for mating with more prescriptive safety standard series, of which the BOStrab series promises the highest benefit for this specific project. The BOStrab (German regulation for the construction and operation of tramways) does not only apply to conventional tramway systems - as the title may imply - but also to new, unconventional types of tracked transport systems including fully automatic rapid transit 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 BOStrab form a sound basis for the certification process of new modern mass transit systems like the Sky Bus Metro. Respective safety concepts and a safety demonstration / approval process can be derived thereof.

The overall procedure of the European Standard EN 50126 is based on the lifecycle model. The lifecycle model distinguishes between different phases. Each phase contains well defined, phase-related general, RAM (reliability, availability, maintainability) and safety tasks.

The CENELEC standards are based on the life cycle model as demonstrated in Figure 2. This consists of all-in-all 14 phases, starting with the concept phase followed by system definition, risk analysis, system requirements, design and implementation, manufacture, installation, system validation and acceptance, through operation and maintenance up to decommissioning and disposal. The concept does also cater for the phases of performance monitoring, modification and retrofit, which are arranged in parallel to the operations & maintenance phase. The single phases are described in detail in the standard EN 50126, defining each phases' objectives, inputs, requirements, and verification tasks.

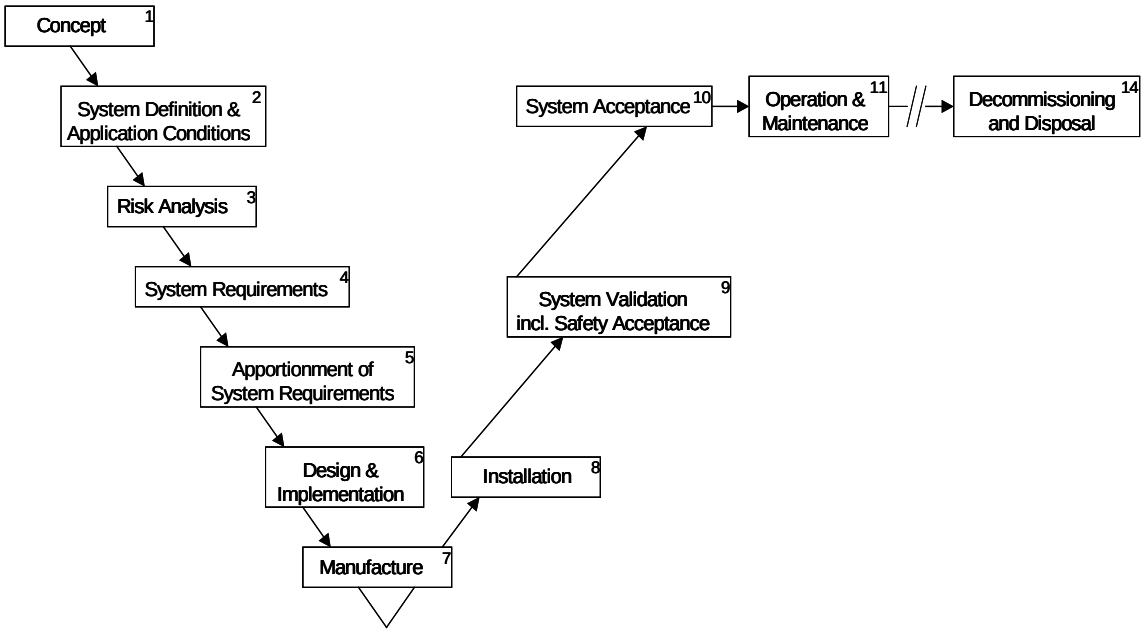

Figure 2: Life-Cycle Model

The following chapters provide an high level overview on the purpose of the respective life cycle phases (phase 12 monitoring, modification and 13 retrofit not shown here).

4.1 Concept (1)

The concept phase shall develop a level of understanding of the (new) system sufficient to enable a subsequent lifecycle and respective tasks.

The planned system (here Sky Bus Metro) shall be acquired in the context of the planned performance regarding scope, context and purpose of the system as well as under environmental aspects such as system interfaces, physical issues but also financial, social and economical issues, etc.

Finally, the current Railway Authority Safety Policy and Targets shall be clarified and should be brought into a balance with the planned system.

When applying the CENELEC railway standards on a complex project for a safety assessment, a strongly regulated process has to be planned. The CENELEC standards (also in conjunction with BOStrab) may form the basis to define an Approval / Authority Acceptance and Certification Process based on Approval / Authority Acceptance Milestones derived from the life cycles.

4.2 System Definition (2)

In the first stage of a railway application development (here the Sky Bus Metro) the general functional capabilities and the related acceptance criteria for a system are fixed. This includes among others (e.g. lifecycle cost or capacity requirements) the safety acceptance criteria. The latter are often given by a national or international authority, based on basic principles and experience. For example the GAMAB principle (Globalement Au Moins Aussi Bon) in France (i.e. the new system must be at least as good/safe as any equivalent existing system), the MEM (Minimum Endogenous Mortality) principle in Germany (i.e. the new system should not significantly increase the MEM), or ALARP (As Low As Reasonably Practicable) in UK (i.e. below an “Unacceptable” risk-region there could be a cost/benefit trade-off), refer also to EN 50126, Annex D. There are two basic viewpoints to derive the safety requirements for a system from a risk analysis: the social viewpoint, i.e. what risk is the society willing to tolerate, and the individual viewpoint, i.e. what risk is an individual user of the system willing to tolerate. Both viewpoints can be combined.

After the tolerable risk is defined by the authority and a system concept is derived, the risks that are inherent to the systems operation (system functional viewpoint) are analysed (hazard identification and analysis). This defines the safety integrity level that the functions are required to comply with.

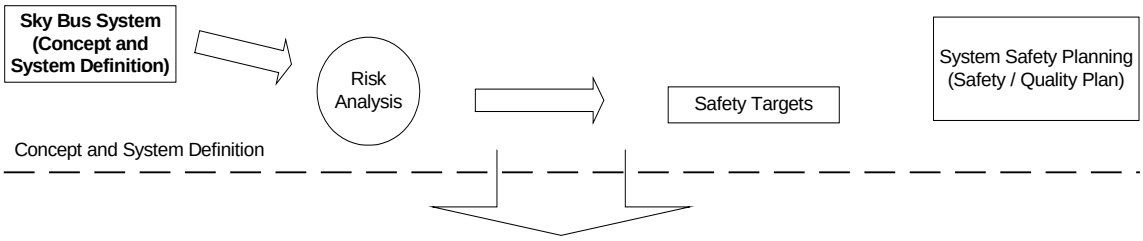

Figure 3: Concept and System Definition Phase

4.3 Risk Analysis (3)

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

- Identification of the threats and risks for human lives (system users, staff, third party), animals,
- material assets and environment, that can be caused by the system (i.e. certain physical or chemical properties, problems the operator experiences while dealing with the system, failures of the system, e.g. resulting from internal defects).
- Consideration of events that cause threats, which turn into unwanted incidents which can cause 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 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 then can refer to the overall system, to sub-systems, to safety functions or to sub-functions. The aspects of Operation & Maintenance are considered as well.

For tracing of the individual hazards a Hazard Log is being prepared. The Hazard Log is a list (database or similar), which contains all hazards, describes their assignment to system / sub-system / function / sub-function, refers to measures taken to eliminate or reduce the risk (design and / or procedures) and finally describes their status (e.g. open, closed).

Risk analysis may need to be repeated at several stages of the life cycle.

4.4 System Requirement (4)

The following chapter describes, how the requirements according a CENELEC compliant railway application or sub-system e.g. the Sky Bus Metro system, shall be developed. The main focus has been set on the structure of the development phases and how this shall be documented.

The specification of the system requirements of the Sky Bus Metro system should be strictly separated into Functional Requirements, Safety Requirements, Operational Requirements and Environmental Requirements.

Further it must 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-systems. For example, on system level the Sky Bus Metro system must respect the overall system performance and safety target requirements. But on subsystem level the requirements differ for vehicle and station equipment.

4.4.1 General Requirements for System Requirement Specification

The System (here Sky Bus Metro) Requirements Specification document shall contain the initial design, which defines the technical properties of the (future) system. Especially the railway application's behaviour at its interfaces to the environment shall be defined. The principle of a Black Box approach is valid. It shall be detailed, what the system should achieve. But it should not be included, how this achievement is performed. In particular the document shall describe:

- For which kind of railway system the application is planned, e. g. a heavy rail system, light rail system or the Sky Bus Metro in this case) etc.
- Which requirements the railway application shall comply with.
- Which standards, regulations, and operator's requirements must be considered.
- Which safety requirements, particularly derived from a Risk Analysis or FMEA, the system shall comply with.
- The interfaces by which the system is interacting with other systems. This shall comprise technical components as well as user interfaces.
- Which performance and reaction times the system shall meet.
- How the requirements shall be verified after completion.
- Separation of safety-related requirements from non-safety-related requirements with well defined interfaces.
- Specification of external influences.

4.4.2 Documentation Structure for Railway Application Development

During each life-cycle phase, presented in the previous chapter, several deliverables are necessary to demonstrate the evidence of the performed actions. Figure 4 is the raw attempt to identify the necessary high-level documentation of the development process of the Sky Bus Metro system, based on the CENELEC standards EN 50126, EN 50128, EN 50129 and the system architecture as per Figure 4.

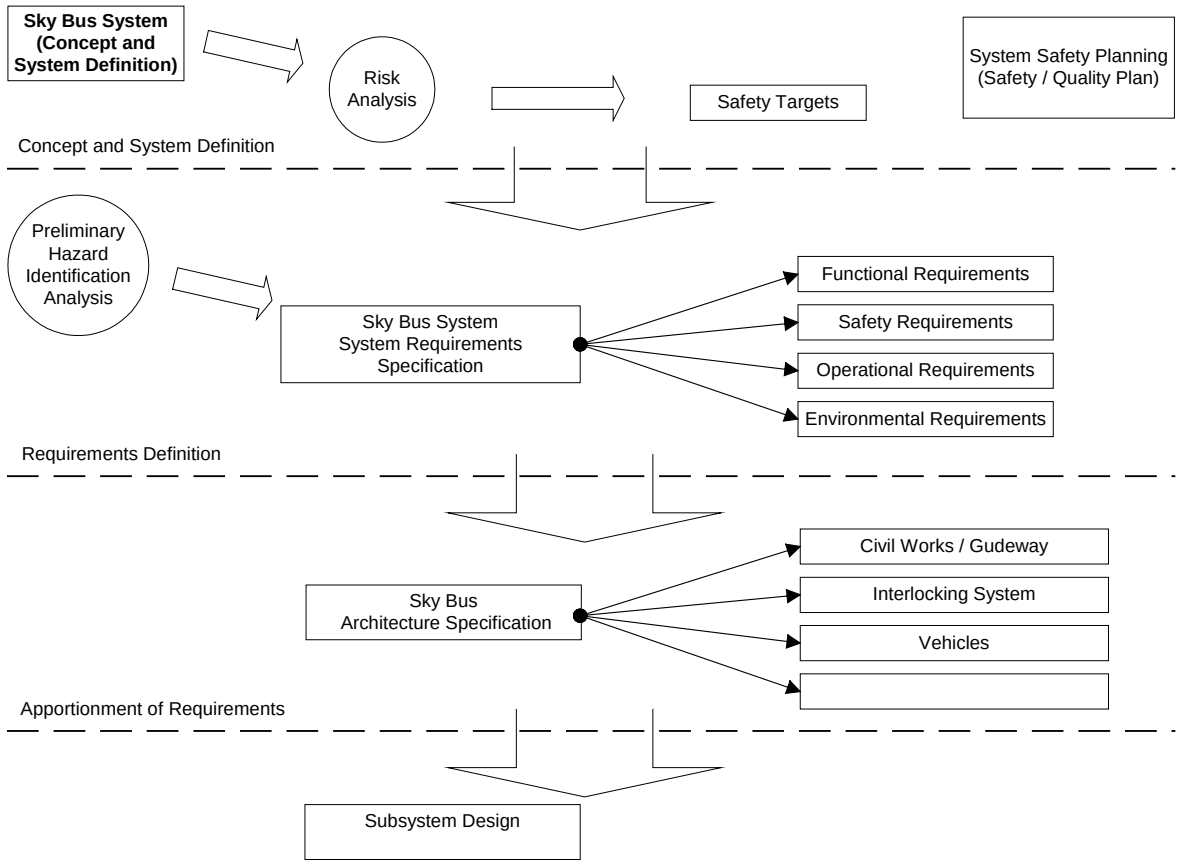

Figure 4: Expected Sky Bus Metro Document Structure

4.5 Apportionment of System Requirement (5)

In the following sections an introduction is provided, how system (safety) and functional (safety) requirements of a railway application and the main sub-systems are defined and derived. Further the scope of the system and requirements specifications for safety and non-safety requirements of a railway application is detailed.

After the definition of the Tolerable Hazard Rate / the Overall Safety Target (quantitative safety goal) for the overall system and the preparation of a Preliminary Hazard Analysis (PHA) it is possible to define safety functions necessary to eliminate the hazard or to reduce its risk. Functions contributing to risks / accidents can be identified on the basis of the identified and analysed Hazards following CENELEC standard. These functions can now be allocated to SILs on system level (assignment of qualitative measures to quantitative safety goals).

The next step is to incorporate the system architecture into the analysis and to allocate the functional safety integrity requirements to the subsystems involved in implementing the functions. For sake of simplicity only the simplest case is regarded here, that a function is implemented by exactly one single subsystem. Then the subsystem directly “inherits” the safety integrity requirements. The next step is to design the subsystem according to the requirements, or to choose an appropriate existing system that complies with the requirements (e.g. an already certified subsystem).

In the best case all subsystems are capable to comply with the foreseen requirements, and thus the overall system risk tolerability criteria is fulfilled. If one subsystem however does not comply completely with the requirements, this might be balanced by some additional or external means with respect to the respective safety function. Of course such scenario is only acceptable, if the overall system risk tolerability criteria is still fulfilled (depending on the overall architecture of the system).

If such a mutual balance of requirements is not possible, the system architecture must be changed. For example by introducing additional protective measures. This might be a parallel subsystem that protects from failures of the initial subsystem that is not capable to handle its safety requirements alone. For example a train control system, where every loss of function will lead to a potentially hazardous situation (e.g. derailment or collision). By adding an independent train protection system that is capable of “filtering” out any potentially hazardous

train control command the safety responsibility (i.e. the safety requirements) of the train control system are lowered and nevertheless the overall safety requirements can be met.

Summarizing the outlined approach describes an iterative top-down apportionment of safety integrity requirements combined with a bottom up investigation of capabilities. The sum of all potential hazards caused by subsystem failures must comply with the overall risk tolerability criteria.

4.5.1 General Requirements on Requirements Specifications

This document shall contain the initial design, which defines the internal properties of the railway application. The railway application shall be divided systematically into smaller functional blocks, based on the functional requirements specified in the System Requirements Specification.

The resulting functional blocks may represent complete sub-systems (e.g. the partitioning of a transport system (the Sky Bus Metro in this case) into it's subsystems Signalling and Control, Power Supply, Rolling Stock, Civil Construction, etc.).

In particular these documents shall describe:

The functional requirements shall be unambiguously defined for each of the resulting smaller subsystems:

- Which functional requirements of the System Requirement Specification does the subsystem fulfil?
- Which interfaces of the subsystem interact with other subsystems (this can also include external interfaces of the overall system) and are the interfaces completely defined?
- Which performance and reaction time criteria the subsystem should meet?
- What are the conditions of requirements and the limitations of the individual item of equipment and what has to be documented in the operation and maintenance instructions?

The safety integrity requirements of each of the resulting subsystems shall be unambiguously defined.

The entirety of the subsystems shall result in a complete and consistent image of the overall system (=> proof of complete and consistent refinement).

Separation of safety-related requirements from non-safety-related requirements with well defined interfaces.

4.5.2 Verification of System Requirements

The CENELEC standards define V&V (verification & validation) tasks in the system life cycle.

In each phase it has to be shown by analysis and test, that the safety requirements identified in the previous phase are met by the consecutive phase (verification).

It has to be proven by analysis and test, that the completed system / sub-system / equipment fulfils the specified safety requirements (validation).

Depending on the Safety Integrity Level (SIL), different degrees of independence of the verifier and the validator from the designer is demanded. For all SIL > 0, an independent safety assessment is required. Figure 5 shows the verification and validation with respect to the life cycle phases (refer also to EN 50126, Figure 11).

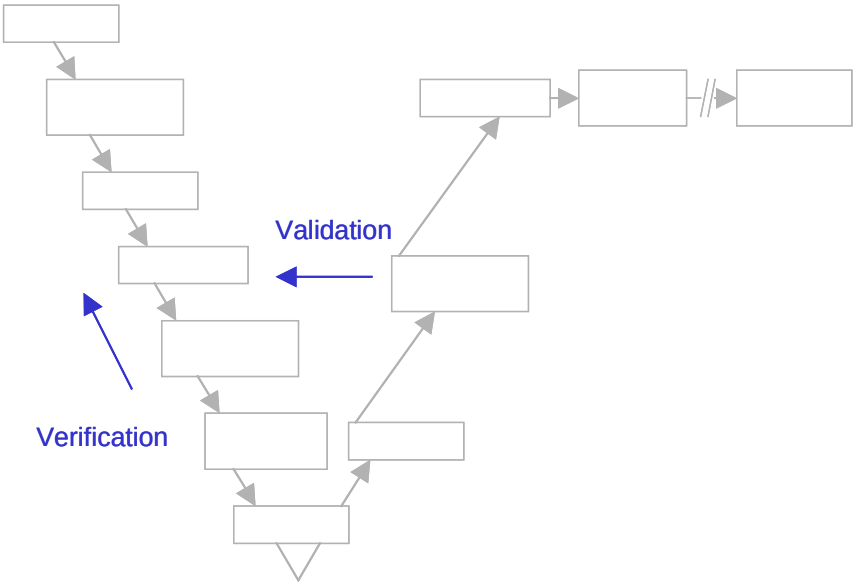

Figure 5: Verification and Validation

4.6 General aim of safety validation

In general two sources are distinguished to compromise safety:

systematic faults, i.e. faults in the design of the system, and

random faults, i.e. faults caused by hardware malfunction, e.g. due to aging or stress.

Like in a chain, where the weakest link determines the strength, both types of faults are equally important and need to be addressed by a well balanced set of countermeasures in order to achieve a design that is sufficiently robust and safe.

The safety integrity level (SIL) requirements for a system or subsystem are derived from the risk analysis approach outlined before. The SIL defines both, the required capability of the system development process to avoid systematic faults, and a numeric safety target concerning the occurrence of random faults (i.e. the tolerable hazard rate THR).

4.6.1 Control of systematic faults

For the control of the systematic faults countermeasures like hierarchical top-down design with strict review and testing are known and generally accepted (refer for example to EN 50128). These techniques apply equally to structurally redundant architectures (e.g. two-out-of-two) and non-redundant architectures (reactive fail-safety).

Diversity in the design, e.g. use of hardware and / or software diversity, is not prescribed in the standards. Also, it is not commonly applied in many safety related systems, due to the higher effort in synchronization. Use of design diversity as a central argument against design faults is sometimes also seen as an admission that the design is too faulty to “survive” without a second instance. This viewpoint could conflict with a “historical” philosophy, that a safety related design must be free of any design faults. However, the standardization bodies have recognized that in the reality today a design without faults can in general not be guaranteed for complex (software based) systems. Systematic failure integrity cannot be assessed by quantitative methods. Therefore, the required safety integrity levels “are used to group methods, tools and techniques which, when used effectively, are considered to provide an appropriate level of confidence in the realization of a system to a stated integrity level” (see EN 50129, Annex A3). Diversity can be considered as additional countermeasure against potentially remaining systematic faults and other common mode failures.

Instead of prescribing diversity, the main countermeasures prescribed by the standards against systematic faults are related to use of good proven methods, tools and techniques, and high quality assurance requirements to avoid these systematic faults or to detect them by sufficiently stringent V & V measures. Usually not a single possible solution is prescribed in the standards, but a set of possible solutions. The fitness of the applied solutions is to be assessed by an Independent Assessor. To support a smooth assessment process a project accompanying safety assessment is recommended, where the Assessor is involved early in the lifecycle.

The general philosophy of the design method for safety related systems can be summarized as risk-driven top-down design approach with stepwise design refinement and rigorous documentation and validation of the system requirements and verification against the requirements from the previous stage of the design. Each implementation stage is thoroughly tested (V-model approach). Of course the general approach needs project specific adaptation, and formal methods with automatic consistency checks and formal proofs might replace specific “standard” verification steps.

4.6.2 Control of random failures

For random hardware failures architectural solutions with structural hardware redundancy are generally accepted, e.g. two-out-of-two-architectures with inherently fail-safe comparison. A single failure of any of the two components is detected by the comparison, which shuts down the system into a safe state. In addition at specific proof check intervals the components are thoroughly tested, in order to detect any potential dormant faults that otherwise could lead to the accumulation of faults, and thus the necessity to deal with more complex multiple fault scenarios. Often, the redundant components are those with complex, unknown, or not well-defined failure modes, like processing units. The effectiveness of self tests is limited. For such complex components in general analytic proof of safety is difficult and exhaustive and thus structural redundancy is often used.

The comparison and shut-down mechanism can be constructed inherently fail safe, meaning that any possible single failure mode will lead to a safe state. The inherent fail-safety is based on physical properties of the components, e.g. the breakdown of a resonance circuit at parameter drifts.

A third possible safety principle is regular monitoring, where a more complex component, e.g. one with redundant architecture, tests other components which are by themselves not

based on fail-safe principles. Safety of the tested components is based on the correct and timely performance of the tests on the monitoring component and the fault detection capabilities of this component (hardware in the feedback loop).

Beside these well known and proven techniques, also so called “reactive fail-safety” hardware solutions (i.e. without complete structural hardware redundancy) are mentioned in EN 50129. They also require demonstration of compliance with given quantitative safety targets (maximum tolerable hazardous failure rate).

5 From Theory to Practice – How to introduce a Sky Bus Metro Certification Process

Following chapter 4, Introduction to CENELEC Safety Certification Approach, and facing the general KRCL attempt to finally achieve a Sky Bus Metro certification as the basis for the future system operation with passengers, this chapter aims to provide the baseline information to enable the effective definition of a certification process and the effective application of such.

Since the scope of this report is to provide the results of the determination of the "Level of Maturity for Safety Application" of the Sky Bus Metro concept before starting a CENELEC safety certification according to EN 50126 - EN 50129 (refer to chapter 1.2, The Task), the best way from theory to Practice appears to be to focus on the first CENELEC life cycle phases and to outline the phase related tasks to be performed and the respective deliverables.

The following chapters provide a general idea on how to proceed with focus on the phase related safety tasks as per Table 1: Project Phase related tasks as per EN 50 126 (phases 1 – 4 shown, only). It is worth while to mention that beyond the safety aspects further general and RAM tasks are to be considered.

LIFECYCLE PHASE	PHASE RELATED GENERAL TASKS	PHASE RELATED RAM TASKS	PHASE RELATED SAFETY TASKS
1. CONCEPT	. Establish Scope and Purpose of Railway Project . Define Railway Project Concept . Undertake Financial Analysis & Feasibility Studies . Establish Management	. Review Previously Achieved RAM Performance . Consider RAM Implications of Project	. Review Previously Achieved Safety Performance . Consider Safety Implications of Project . Review Safety Policy & Safety Targets
2. SYSTEM DEFINITION AND APPLICATION CONDITIONS	. Establish System Mission Profile . Prepare System Description . Identify Operation & Maintenance Strategies . Identify Operating Conditions . Identify Maintenance Conditions . Identify Influence of Existing Infrastructure Constraints	. Evaluate Past Experience Data for RAM . Perform Preliminary RAM Analysis . Set RAM Policy . Identify Long Term Operation and Maintenance Conditions . Identify Influence on RAM of Existing Infrastructure Constraints	. Evaluate Past Experience Data for Safety . Perform Preliminary Hazard Analysis . Establish Safety Plan (Overall) . Define Tolerability of Risk Criteria . Identify Influence on Safety of Existing Infrastructure Constraints
3. RISK ANALYSIS	. Undertake Project Related Risk Analysis		. Perform System Hazard & Safety Risk Analysis . Set-Up Hazard Log . Perform Risk Assessment
4. SYSTEM REQUIREMENTS	. Undertake Requirements Analysis . Specify System (Overall Requirements) . Specify Environment . Define System Demonstration & Acceptance Criteria (Overall Requirements) . Establish Validation Plan . Establish Management, Quality & Organisation Requirements . Implement Change Control Procedure	. Specify System RAM Requirements (Overall) . Define RAM Acceptance Criteria (Overall) . Define System Functional Structure . Establish RAM Programme . Establish RAM Management	. Specify System Safety Requirements (Overall) . Define Safety Acceptance Criteria (Overall) . Define Safety Related Functional Requirements . Establish Safety Management

Table 1: Project Phase related tasks as per EN 50 126 (phases 1 – 4 shown, only)

5.1 Previously Achieved Safety Performance

During CENELEC life cycle phases 1 (Concept) and 2 (System definition and application conditions) EN 50126 requires the design process to include a study of previously achieved safety performances of the system to which the newly developed equipment shall be added. As Sky Bus Metro is a generic new development there is no existing safety performance available. This requires to broaden the view to include other existing mass transportation systems which show similar safety relevant aspects to Sky Bus Metro.

Obviously no single system has the same combination of safety relevant aspects as Sky Bus Metro, but a combination of aspects found in a number of existing mass transportation systems can be generated in order to reference most of those aspects found in Sky Bus Metro.

However, the choice of reference aspects from other systems requires great care and a good understanding of Sky Bus Metro technology as well as the technology of the reference system to avoid invalid comparisons or simplifications.

No Review- and Evaluation-Document on achieved safety performance of safety related Sky Bus Metro design aspects has been made available by KRCL. To serve as a reference for this report a basic research has been performed. According to the limited scope of this study the basic research has been focussed on a small number of systems.

Other mass transportation systems of general relevance for a comparison with Sky Bus Metro are:

- Metro Systems
- Monorail Systems (both the Alweg type with vehicle on top of guideway structure and the Safege type with the vehicle hanging underneath the guideway structure)
- Maglev Systems (Magnetic Levitation Systems)

The relevance of the mentioned systems for a comparison is as follows.

Metro systems, Monorail systems and Maglev systems can be relevant for comparison of the safety aspects:

- safety of vehicle construction,
- fire prevention concepts,
- emergency concepts.

Monorail systems and Maglev systems can be relevant for comparison of the safety aspects:

- safety of guideway construction,
- safety during operation and passenger boarding,

Metro systems and Maglev systems can be relevant for comparison of the safety aspects:

- Automatic driverless operation

No reference system has been identified for the aspect guidance stability (wheel rail contact). Due to the significantly different mass distribution caused by the main vehicle mass suspended under the rail, a comparison with Rail and Metro Systems is not valid.

The in general appearance similar looking Monorail systems of the Safege type are employing a more or less restraining forced guidance concept by additional horizontal guide wheels. This is completely different from the Sky Bus Metro approach.

Keeping the above mentioned constraints in mind, following systems have been chosen to serve as reference:

5.1.1 Wuppertaler Schwebebahn

Figure 6: Wuppertaler Schwebebahn

This system is positioned at Wuppertal, Germany and in operation since 1901. The carrying and guidance concept employs a double flanged steel wheel on a single steel rail. The operation is based on signalised driver operation. The track length is 13.3 km of dual track. The top speed is 60 kph. The car body swing is unrestrained up to 15 deg also at platforms, which requires a special and open access platform arrangement.

Common aspects of KRCL Sky Bus Metro with Wuppertaler Schwebebahn are the following:

- The car body is supported underneath the rail which requires special emergency procedures.
- Due to the suspended nature of the car body the system requires special platform and boarding procedures to cater for any swing or tilting angle of the vehicle.
- The supporting structure in many cases is placed in the public traffic area and has to be secured against impact loads.
- Due to public traffic underneath the track area, certain requirements have to be met to avoid collisions of lorries or construction engines with the trains.
- The installation of long welded rail on a civil structure subjected to thermal stresses and related expansion and retraction movements.

Conclusion of this KRCL Sky Bus Metro comparison with the Wuppertaler Schwebebahn:

The Schwebebahn system has a continuous high safety performance in comparison with other mass transport systems. Technical solutions for fire prevention (especially choice of materials) and for accommodation of long welded rail on civil structures have been developed. The max. speed of the system is however 60kph which is significantly less than the proposed 100kph at Sky Bus Metro. This in turn means reduced dynamic forces. Special system related procedures to evacuate passengers from an immobilised vehicle had to be developed. These are mainly based on technical and personal support by the fire brigade whose close support is available in the urban environment of the whole system.

5.1.2 Sky Train Düsseldorf

Figure 7: Sky Train Düsseldorf

The Sky Train system is an airport people mover system in Düsseldorf, Germany. Operation is unattended automatic and started in 2002. The guidance and support system is of the Safege type and uses 4 carrier wheels and 8 horizontal guidance wheels per bogie. Thus the bogie is fully restrained inside the guideway and is transferring all rotational moments into the guideway. Car body swing is restrained to 6.5 deg which required special platform arrangements to constrain the vehicle in its position and bridge the required clearance gap. Due to the design (restrained bogie, chosen load interface between bogie and guideway) the max. speed of 60kph has to be reduced in curves, even though clothoid transitions are in use.

Common aspects of KRCL Sky Bus Metro with Sky Train Düsseldorf are the following:

- The system is automatically controlled by a suitably designed and embedded signalling and control system. It is furthermore fitted out with additional features to allow unattended passenger traffic. A limited signalling and control system is fitted for manual back up operation.

- The car body is supported underneath the rail which requires special emergency procedures.

- Due to the suspended nature of the car body the system requires special platform and boarding facilities including an automatic clamp to normalise any tilting angle and a retractable structure to bridge the gap between vehicle and platform.

- Due to public traffic underneath the track area, certain requirements have to be met to avoid collisions of lorries or construction engines with the trains.

Conclusion of this KRCL Sky Bus Metro comparison with the Sky Train Düsseldorf:

The Sky Train system shows, that the safety requirements of automatic train operation and the safety features connected with suspended transport systems can be successfully combined.

The guidance concept is different from the proposed Sky Bus Metro system. The bogie is restrained against longitudinal rotational moments and the swing of the suspended body is restrained. As physical constraints of mass distribution are somewhat similar between the systems this outlines that the guidance function, the alignment concept and the loading limits of the structure do require thorough review in a coordinated approach. Without full definition and understanding of this interface between guideway and vehicle, load or speed limitations might be required. Sky Bus Metro might be prone to this effect as the suspenders are in relation significantly longer than with the Sky Train system (as well as in comparison with other suspended systems). Technical solutions to this safety aspect are however available.

Specific emergency concepts have been developed and are augmented by the close support by the airport and urban emergency services. Provisions have been made to allow ground vehicle access to most areas of the track. A railway line has been bridged by provision of a false slab under the guideway.

5.1.3 Shonan

Figure 8: Shonan

The system is based at Shonan, Japan and in operation since 1970. It employs the Safege type system of rubber carrying and additional guidance wheels.

Common aspects of KRCL Sky Bus Metro with the Shonan system are the following:

- The car body is supported underneath the rail which requires special emergency procedures.
- The system is a high capacity people mover in an urban environment.

Conclusion of this KRCL Sky Bus Metro comparison with the Shonan system:

The Shonan system is like the Wuppertaler Schwebebahn a high capacity public transport system. This further shows the technical feasibility of combining suspended car bodies with mass transit safety requirements.

5.1.4 Metro Copenhagen

Figure 9: Metro Copenhagen

The Copenhagen Metro system in the capital of Denmark has been opened in 2002. Signalling and control are automatic. Passenger operation is unattended. To ensure safe passenger operations, the entire system (infrastructure, power supply, rolling stock, platform screen doors, communication systems, emergency systems and state of the art signalling and control system) has been integrated using a design and construction and certification process according to the CENELEC standards.

Common aspects of KRCL Sky Bus Metro with the Metro Copenhagen are the following:

- The mass transit system is automatically controlled and additional safety equipment for safe passenger operation has been developed for this type of operation.

Conclusion of this KRCL Sky Bus Metro comparison with the Metro Copenhagen:

The performance requirements towards the automatic signalling and control system of the Copenhagen system towards train separation and collision avoidance are similar to the Sky Bus Metro proposed performance. The tight system headway of 90sec is also comparable to the Sky Bus Metro system requirements. The automatic service required to develop technical solutions for the necessary additional safety equipment. The CENELEC safety approach has been successfully used by the system suppliers to demonstrate safety of the automatic control equipment, the rolling stock, the infrastructure and the operational procedures for the system.

5.1.5 Transrapid Shanghai

Figure 10: Transrapid Shanghai

The Shanghai Transrapid Magnetic Levitation system connects Pudong International Airport with Shanghai, P.R. of China since 2002. The double track alignment allows a service speed of 430kph. Signalling and control are automatically.

Common aspects of KRCL Sky Bus Metro with the Transrapid Shanghai are the following:

- The performance requirements towards the automatic signalling and control system of the Shanghai Transrapid system towards train separation and collision avoidance are similar to the Sky Bus Metro system.

- Specific emergency concepts have been developed to allow rescue of passengers from an immobilised vehicle.

Conclusion of this KRCL Sky Bus Metro comparison with the Transrapid Shanghai:

The exposed position of an immobilised vehicle on the guideway requires special emergency concepts. This has to include sufficient on-board equipment, as the cross country alignment is not fully accessible to emergency services and response time of such services would be unduly long. In addition technical solutions are provided to increase the capability to reach the next station. The comparison shows, that technical solutions for safe operation despite of the named aspects are feasible.

5.2 Safety Policy and Safety Targets

Two substantially different phases of the process of risk identification and risk reduction have to be distinguished.

In the first phase - during CENELEC life cycle phases 1 (Concept) and 2 (System definition and application conditions) - the requirements, especially the tolerable rate of dangerous failures and the resulting Safety Integrity Level (SIL) are defined (i.e. appropriate qualitative measures have to be assigned to the quantitative safety target). The responsibility for this phase belongs in principle to the Supervisory Authority. That means, that the Authority either defines the targets or approves the analysis of an assessor or a supplier.

The second phase - during the further CENELEC life cycle phases 3 (Risk Analysis) and the following phases, refer to chapter 5.4, Preliminary Hazard Analysis) includes hazard analysis, especially analysis of the consequences, and the control of the risk reduction process.

Based upon evaluations e.g. as outlined in chapter 5.1, Previously Achieved Safety Performance and further KRCL evaluations, the following main aspects (which are not known to the Assessor so far) are to be clarified and to be specified.

- Railway Authority Approval Process

  This includes to identify the authority, roles and responsibilities for the final approval, to agree upon an appropriate approval process between the parties (Authority, KRCL, Assessor, suppliers)

- Railway Authority RAM and Safety Policy and Targets

  This includes to achieve a common understanding of the RAMS policy between the parties involved and to specify the RAMS Targets (RAM targets in terms of figures, e.g. availability of 98% and safety target in terms of target figures, e.g. targeting the max. number of accidents / fatalities per million kilometres and / or per time unit and / or per million passengers, by targeting the tolerable rates of dangerous failures for all safety functions and the resulting Safety Integrity Level (SIL), etc.

5.3 Certification Plan / Safety Plan

During CENELEC life cycle phases 1 (Concept) and 2 (System definition and application conditions) EN 50126 requires to establish a Certification Plan / Safety Plan based upon and phase related RAMS tasks performed so far in these phases and for the purpose of planning the further phases.

Based upon evaluations e.g. as outlined in chapter 5.1, Previously Achieved Safety Performance, chapter 5.2, Safety Policy and Safety Targets and further KRCL evaluations, the following main aspects (which are not known to the Assessor so far) are to be clarified and to be specified within the Certification Plan / Safety Plan.

In particular the Certification Plan / Safety Plan shall include:

- Commitment that a safety life-cycle consistent to EN 50126 is set-up and appropriate description of such
- Appropriate description of project organisation (organization diagram etc.)

  A typical and possible organisation is shown in the following figure.

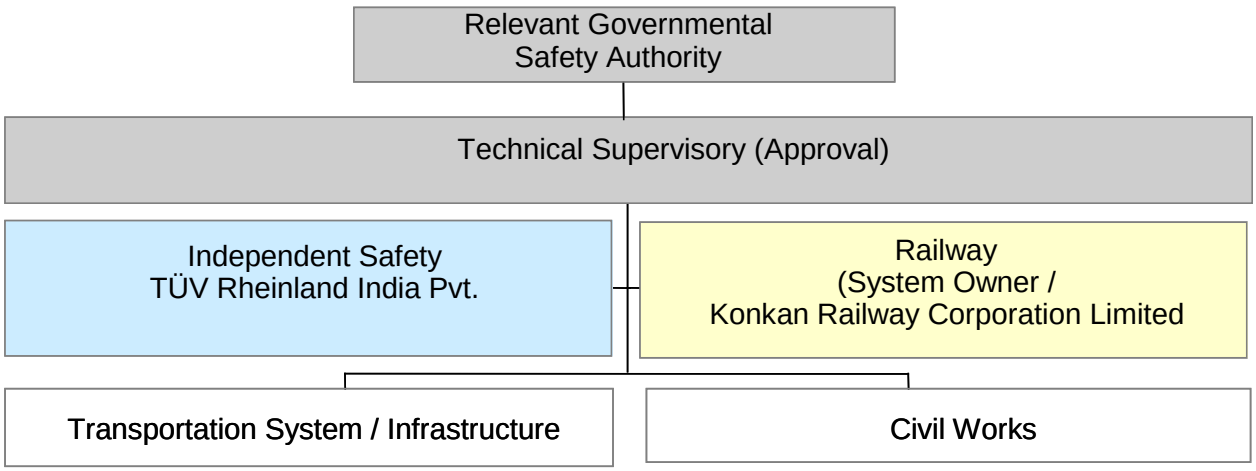

Figure 11: Possible Project Organisation

- Appropriate description of safety management organisation (organization diagram etc.)

  This has to include the proof of independence of project staff – where required - according to the relevant safety requirements to CENELEC standards. Education/experience/training requirements of project staff according to safety requirements has to be detailed.

- Appropriate description of safety related activities planned, including

  - Hazard and Risk handling and monitoring process / hazard log planning and handling
  - Safety requirement specification and treatment process and handling
  - Safety functions specification process and handling
  - Design checking process for fulfilment of operational and safety requirements
  - Definition of (safety related) Approval milestones
  - Requirements for review and update of the safety plan

5.4 Preliminary Hazard Analysis

During CENELEC life cycle phases 1 (Concept) and 2 (System definition and application conditions) and 3 (Risk Analysis) EN 50126 requires to analyse potential hazards and risks in an early stage, resulting on an preliminary hazard analysis (refer also to chapter 5.2, Safety Policy and Safety Targets).

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

The identification of sources of hazards and the performance of a preliminary hazard analysis is an essential and a key step to be done early in the project. It is not clearly made available to the Assessor how or if these steps have been performed.

In particular the analysis shall:

Identify the source of hazards,

identify hazards associated with the system,

identify the trigger events leading to the hazards,

determine the risk associated with the hazards,

establish a process for on-going risk management,

document the respective results in a preliminary hazard analysis (PHA).

5.5 System Requirements Specification

During CENELEC life cycle phases 1 (Concept) and 2 (System definition and application conditions) and 3 (Risk Analysis) and 4 (System Requirements) EN 50126 requires to specify the system level requirements (refer to chapter 4.4.2, Documentation Structure for Railway Application Development).

In the first instance, the evaluation of the basic system safety concepts is a sound basis as outlined in the following chapters. Based on these System Safety Concepts (Safety Functions, Evacuation and Rescue Concept, Fire Protection Concept, other aspects) the System Requirement Specification can be developed. Details on this process can be taken from chapters 4.4, System Requirement (4) and 4.5, Apportionment of System Requirement (5) and are therefore not repeated here.

5.5.1 System Safety Functions

After the definition of the Tolerable Hazard Rate / the Overall Safety Target (quantitative safety goal) for the overall system and the preparation of a Preliminary Hazard Analysis (PHA) it is possible to define safety functions necessary to eliminate the hazard or to reduce its risk. Functions contributing to risks / accidents can be identified on the basis of the identified and analysed Hazards following CENELEC standard. The safety functions are defined on the basis of the Hazard Analysis for the overall system. For each Hazard (or a class of Hazards) a safety function is defined, which is necessary to eliminate the occurrence of a hazard or to reduce its risk. Functions, which contribute to a risk / accident, are defined as well. Functions in general can be realised by design and / or procedures. Safety functions can then be assigned to safety systems and / or external risk reduction facilities. This process is interactive.

What often is not realized at the first glance are safety functions that do not fall under common ATP functions. For conventional trains these are performed by the train driver who detects dangers by his senses and reacts to remove or lower these, e.g. he hears/feels the derailment of a bogie and thus operates the brakes. For driverless systems such safety functions have to be performed by automatic devices. Examples are:

- Alarm Generation and Emergency Stop,
- Vehicle Automatic Sensing Devices,
- System Reaction Times.

Further, these functions can now be allocated to SILs on system level (assignment of qualitative measures to quantitative safety goals). As a matter of principle Safety Integrity is defined for safety functions. Refer to chapter 4.5, Apportionment of System Requirement (5) for further details on this process.

5.5.2 Emergency Concept / Evacuation and Rescue Concept

In order to gain a sufficient level of safety for the new Sky Bus Metro system, technical and procedural measures and plans for emergencies have to be established. These concepts have to take into consideration the kind of system and the specific conditions of the system surrounding. The basic principles to manage the evacuation of passengers should be specified in the early Overall System Design phase. Possible scenarios and situations, in which the evacuation of passengers may be necessary, must be identified and analysed (i.e. at unfavourable positions of the guideway over water, high speed traffic lanes, etc.)

As an outcome, basis infrastructure requirements and safety functions / system / sub-system requirements are to be specified, which must be further refined in the respective Safety Functions, System and Sub-System Requirement Specification(s). Furthermore, basic operational requirements towards the System Operator, the Operational Procedures and towards third parties like the fire brigade are to be evaluated. A lack of clarity with respect to these basic evacuation and rescue strategies may easily end up in a change of requirements towards safety functions and sub-systems at a later stage of the project, with all consequences with respect to the time schedule and the integration effort.

5.5.3 Fire Protection Concept

Typical safety functions are fire detection and alarm in stations and in vehicles. The Fire Protection Concept should be part of the operational concept and procedures, also with respect to the interfaces to and integration of external parties like the fire brigade.

As a general rule, the aim should be to keep the fire load of the equipment and the vehicles as low as possible and to choose materials with the lowest possible risk in case of a fire with respect to flammability and toxicity.

Consequently, an inspection and verification of the operational procedures and rules as well as the required equipment and vehicle fire safety criteria flammability, combustible materials, smoke development and toxicity of fumes in terms of documentation reviews and factory inspections are deemed essential.

6 Initial Assessment of Sky Bus Metro Concept on Its Maturity For Safe Application

The presented assessment is generally divided into formal criteria on the presented documentation and into the assessment of the supplied content.

6.1 Formal Criteria

The Assessment of Maturity for Safe Application of Sky Bus Metro Concept is mainly based on the assessment of the Conceptual Design Document, Version 1, (CDD). The formal criteria have been checked using a generic check list (see Table 2: Checklist Formal Criteria below).

The table presents whether the requirements regarding the identification of the document as well as the requirements regarding the structure and the format of the document are met or not. If necessary, remarks are made why a respective requirement is regarded as met or not met.

Aspect/Requirement	Met	Remarks
Unique Document-ID	No	The document has no unique document identification number.
Unique Document Version Number	Yes	
Unique Document Date	No	Different Document Dates
Author(s)	No	No authors specified.
Status of the Document (approved, draft, ..)	No	Non-Approved and Non-Authorized version.
Amendment Record (Version Number, Status, Date, Author, Changes made)	No	A separate page should be reserved for the Amendment Record.
Page Numbering/Identification	Yes	
Identification of Insertions and Deletions	N / A	First reviewed revision (applies for future revisions)
Table of Contents	Yes	
Terms and Definitions	Yes	
References	Yes	
Appendices	Yes	

Table 2: Checklist Formal Criteria

Apart form the remarks mentioned in the table above some additional formal issues were recognized in the Conceptual Design Document:

- the arrangement of the contents of the document could be structured more systematically,
- the consistency of the content of the conceptual design document could be improved
- relating aspects of the document do not refer to each other

6.2 Assessment Results

6.2.1 System Level

To verify the safety-related aspects of the relevant sub-systems as well as those of the entire system a thorough understanding of the design of Sky Bus Metro is needed. In a “System Requirement Specification Sky Bus Metro” all relevant aspects shall be systematically presented

In addition to the aspects mentioned in chapters 4.4, 4.5 and 5.5 the content of this document should include at least:

- *Transport performance*
- *Interfaces between the subsystems*
- *Alignment parameters*
- *Comfort and dynamic parameters*
- *Environnemental Conditions incl. EMC*
- *Safety concept (failure, incidents)*
- *Emergency concept / Evacuation and Rescue Concept*
- *Fire Protection Concept*
- *Maintenance concept*
- *Clearance envelope*
- *Description of “sectionised” Guideway construction.*

Here the BOStrab series of standards could be used to systematically develop this structured approach.

In general the currently available information given in the Conceptual Design Document, Version 1, KRCL, 09.01.2004 is not consistent enough to make a final decision about the level of maturity of the Sky Bus Metro system concept in terms of safety.

However for this high level approach the given level of detail is appropriate to assess the proposed concept.

Conclusion:
The proposed suspended mass transportation system combines proven aspects of rail technology and recombines them into a new technical solution. Some aspects have hardly been changed with regard to existing proven implementations, others are being used

- in a new and different environment,
- in new design combinations,
- under new physical constraints and interfaces,
- with new production procedures,
- within the proposed Sky Bus Metro specific operation procedures

and require closer investigation with regard to their level for safe implementation.

On system level the concept of Sky Bus Metro appears feasible for safe implementation with respect to the suitable existing safety standards that could be used for design, construction and operation and with respect to the positive safety record of the reference systems chosen for this study (see chapter 5.1 of this report).

6.2.2 Guideway

For an initial assessment regarding the ability of Sky Bus Metro (including its subsystems) to be certified a detailed knowledge of the entire system including all details of the static behaviour of the construction and the load assumptions is required.

Reinforced concrete

In contrast to other suspended transportation systems the guideway of Sky Bus Metro shall be built in a reinforced concrete construction with prestressed pre-fabricated elements instead of a steel-girder construction. This type of construction requires a number of specific design and manufacturing solutions especially concerning the construction quality. Especially for the design and production of those prestressed and pre-fabricated elements required for curves or other non standard parts of the guideway.

The presented construction approach of the highly loaded guideway necessitates a very high quality of work with very tight construction tolerances to allow a safe and reliable service of Sky Bus Metro for the period specified.

With special respect to the chosen concrete construction a subsystem requirement specification should be created and include at least the following aspects:

- Tolerances, gaps / angular deviations / offset between sections of guideway
- Measurement and supervision of girders, and tolerances of gaps between girders
- Geometry
- Components (third rail, ballastless rails, etc.)
- Bearings
- Alignments in detail
- Substructures

Additional Remark:

It appears, that due to the enclosed and suspended nature of the concrete box, the maintainability including the monitoring and the surveying of the rail system inside the box will require complex solutions in respect to known track systems.

Alignment and Profile

The presented alignment parameters give a rough overview of the salient parameters. A number of questions and inconsistencies concerning the design alignment limits of Sky Bus Metro do remain. On one hand the super elevation on curves is nil and on the other hand a compensation for grade is shown. Furthermore no cant will be provided on curves while a cant deficiency about 75 mm only will be permitted. Those parameter will only allow a relatively low speed in curves which does not fulfil the ambitious performance requirements of Sky Bus Metro.

Load Assumptions

In chapter 4.3 of the conceptual design document design loads for the elevated track structure are shown but no further prove of calculation is given. It is not clear if the load assumptions have lead to any impact on dimensioning of the structure.

The ballastless track system with long welded rails will have an impact on the load assumptions due to its thermal expansion which has to be taken into account for the static calculations of the concrete box.

It is also necessary to consider dynamic loads. At this point it will be not sufficient to take a coefficient of dynamic augment of 0.3 into account without any further review. A state of the art approach should include FEM calculation.

Furthermore it can not be seen if any superimposing of loads is taken into account.

At this point of the assessment a calculation could show that the centre of gravity in vertical direction of the entire concrete girder including all of its traffic-, wind- and other loads will always be in-between the bearings, even under its worst combinations including centrifugal forces on curves. This is of special importance as in opposite to a steel girder, which is usually screwed to its columns, a concrete superstructure normally just lies on its bearings without fastening.

At least the following loads taken into account for designing the system:

- Thermal effects,
- Wind during operation,
- Concrete creep and shrinking,
- Impact of road vehicles (collision with columns),
- Earthquake,
- Displacement of bearings,
- Traffic loads (mass, acceleration, braking, track imperfections, centrifugal forces, derailment, multi unit running, push/ pull operations, etc.)

It is not part of this initial study to recalculate the necessary static calculation for the entire system. However the entire static calculation for a structure of this complexity does require checking by an independent test engineer.

Access and ventilation of concrete box

At this stage of the design it is not clear how the access to the inside of the concrete girder for maintenance or during time of construction will be realized. For inspection and maintenance each span of the concrete girder should have an access point for staff on either side of the guideway and for the middle box as well.

In addition to the sun generated heat in the concrete guideway, the electric motors of the Sky Bus Metro consists will produce heat when running which can not be disregarded inside the concrete box due to cooling needs of the motors and power electronics. Therefore a calculation of the thermal effects should check if a ventilation of the inside of sky way will be necessary and if so a ventilation of some kind shall be provided.

Both, the ventilation as well as the inspection entrance shall not weaken the construction.

Prestressing of The Guideway

The positioning of the prestressing cables in longitudinal direction inside the two walls of the concrete girder will have an impact on the composition of stresses in longitudinal direction as well as on the deflection in lateral direction. Annexure 4.6 C of chapter 4 on page 4-16 shows a sketch of match cast joints of the segmental construction. In that sketch it can be seen, that it will be the inner walls only that will carry the stresses in longitudinal direction in-between the span of the columns. It might come to a “keyboard-effect” at the outer side of the concrete girder when a vehicle is running on the line. Each element might move relatively to its neighbouring elements. Detailed calculations have to be done and to be verified by an independent party.

It is still not obvious which kind of guideway will be used other than on straight alignment. A design calculation has to be presented for the guideway in straight and curved alignment as well as for vertical curves (hills and sags) and any permitted superimposing of these effects. Annexure 4.5 in chapter 4 on page 4-13 shows a cross section for elevated track structure in curves, but still a lot of questions do remain. Especially on the way a minimum radius curve of 75 meter or a cubic parabola as a transition curve will be designed and build in prestressed pre-fabricated elements.

Since there is no detailed calculation shown, a final decision about the safety of the construction can not be made yet.

Columns located on outer edge

The basic form of guideway will be the form with single piers placed in the middle of guideway. Where there is no median in the roads possible, the ETS arrangement will have the piers located on the outer edge of the concrete box. A sketch of the guideway for this scenario which is shown in the conceptual design document however seems to have the same profile a the basic form, disregarding the fact that load paths are completely different in this arrangement. Due to the fact that the bearings will be located on the outer edge, the entire static calculation has to consider this. Especially because the prestressing will only be in the middle walls of the concrete box girder.

Horizontal Forces (transversal)

In all common and proven two rail systems, sleepers take the horizontal forces in-between the two rails. Depending on the quality of the rails, the alignment and the wheel rail interface these forces can be significant compared to the static forces which are usually calculated as static strengths. Due to the suspended system sleepers are not possible at Sky Bus Metro, which means that all horizontal forces have to be taken by the concrete girder in addition to the load assumptions stated before.

Fatigue, Vibration, Deflection, (Camber), Structural Deformation

Due to the different length of the inner and outer cantilever arms, the inner one being much shorter than the outer which is hanging form the top slab, the deflection of the arms will be different in the horizontal and the vertical direction. This will lead to gauge spreading, differences in rail inclination and will introduce cant as well.

Also it is quite likely that cracks in the area of tension forces will occur. Especially where no prestressing is provided. In particular the inside surfaces of the outer edges of the cantilever will be on risk to develop cracks which can also cause deflection and furthermore fatigue to the cantilevers. In addition vibrations can also cause damages of the guideway. Therefore it is important that fatigue, vibration and deflection are taken into account at the design phase. A detailed static calculation which is audited by an independent party is required to do a declaration about the safety of Sky Bus Metro.

Supervision of Guideway Construction

The high quality of the complete civil works will be of paramount importance. Therefore a construction supervision on site has to be implemented by an independent party. The quality of the concrete structures is depending on the cement, the surcharges, the thorough mix, the pouring of test samples, the compaction as well as the quality and arrangement of the steel reinforcement and needs ongoing supervision.

At this point, it shall be kept in mind, that the measuring of the position tolerance of the rail system as well as its wear inside this closed concrete box will need the development of new testing solutions.

Conclusion Guideway

It is assessed to be possible to built the guideway of Sky Bus Metro in the drafted method and the designed material in a safe way. But the subsystem guideway and its components need further and more detailed engineering effort followed by a test stage to ensure a safe and reliable operation of Sky Bus Metro. Suitable standards for safe dimensioning and superpositioning of loads are available.

However the supplied calculations, documents and drawings so far do not allow to make a final decision about the safety of the supplied detailed design solutions.

6.2.3 Sky Stations and Platforms

The passenger access and egress points of the Sky Bus Metro system have been named Sky Stations. These stations shall also facilitate the functions access to office, shop or housing constructions on top of the guideway.

From the safety point of view following issues regarding the stations are of relevance:

Measures against overcrowding

The proposed size of the Sky Stations appears relatively small in relation to the proposed passenger exchange capability. It has to be kept in mind that potentially up to 300 passengers are to be exchanged every 60 sec. Further review of this issue should take place according to state of art of technology standards.

Superpositioning of loads cases

The civil structure of the station has to be fit to carry the loads it is submitted to. These loads are depending on the mass of the design, the traffic load and any other additional load cases as required (e.g. earthquakes, strong winds, snow coverage). Regarding the traffic load, it has to be kept in mind, that during rush hour, service disruption or similar cases waiting passengers can accumulate which might require additional design precautions.

It is assumed that this aspect of the Sky Bus system can be safely designed using state of the art building regulations.

High voltage equipment

According to the information supplied, the stations shall incorporate high voltage substations in the same building as the passenger facilities. Safety requirements regarding this aspect are available and thus a technical solution is feasible.

Emergency evacuation from vehicle to station, from station to outside area

In an emergency situation it must be possible to evacuate passengers from the vehicle to the station and from the station to the outside area without delay. This applies also for occupiers of the office, shop or housing constructions on top of the guideway. Again rush hour passenger accumulations have to be included. Two independent exit routes (two staircases) should be considered for good practice.

Regarding the civil structures this issue is not Sky Bus Metro specific, and technical solutions are available for emergency concepts. Sky Bus Metro specific issues are the vehicle doors, platform doors and the passenger access control to the platform. These aspects require the provision of emergency opening aids as back up for a failed automatic system.

Fire fighting to station and to vehicle

Fire fighting solutions for the stations must also have the capability to include fire fighting to fires onboard an arriving vehicle. Operators for this equipment are to be defined.

Technical solutions for this issue are available and this issue is not Sky Bus Metro specific.

Platform interface (gap)

This interface between vehicle and platform requires a thorough review from the safety aspect. Passengers must not fall from height onto road level below or become trapped between vehicle and platform.

In order to avoid any falls, the gap between vehicle and platform must be sufficiently tight. This also improves access conditions to mobility impaired as well as normal able passengers. Several international standards are available in this regard to serve as state of the art requirement.

Due to the suspended car body, the long cantilevers, the lateral hinges and the vehicle suspension at Sky Bus Metro this gap is prone swing and tilt effects of the vehicle due to e.g. movement of passengers or wind loads. KRCL has not proposed a detailed technical solution of this aspect at this state of development.

By comparison with existing systems (refer chapter 5.1.2 of this report) it becomes clear that technical solutions for this aspect have to be developed with great care towards the specific constraints of a given system. A variety of technical solutions is already available, that show potential for adaptation to the special Sky Bus Metro technology. Even though no detailed design information is provided by KRCL in this regard, it is therefore assumed that a suitable and safe technical solution can be developed for the Sky Bus Metro system.

Screen doors

The proposed platform screen doors protect people from falling to the ground below when no vehicle is present. They must therefore be interlocked with the signalling and control system as well as the vehicle doors. During closing they must provide measures to avoid passengers becoming trapped or directly injured by the closing doors. If the doors can not close completely the vehicle shall not be able to depart due to interlocking with the signalling and control system. The proposed automatic operation requires suitable safety equipment in this regard, e.g. platform emergency communication points – possibly interlocked with the signalling and control system in order to stop the vehicle departure – and closed circuit television surveillance into the control room.

Standards regarding door closing speed and closing force limitation as well as for obstacle detection are available as state of the art requirements. Several operational mass transport systems world wide provide feature platform doors, so safe technical solutions are available. This safety aspect of Sky Bus Metro is therefore deemed feasible.

Other issues regarding station safety

The issues passive fire protection, fire detection, minimum lighting requirements in public areas and electrical safety are sufficiently covered by technical standards and are not Sky Bus Metro specific.

Conclusion Sky Stations and Platforms

The provided description for Sky Stations (Refer Chapter 6 of the Conceptual Design Document) is a high level concept which already addresses most of the above mentioned issues. Implementable technical solutions have not been submitted at this stage of the project.

The issues: measures against overcrowding, platform interface (gap) and screen doors require further detailed development and review.

6.2.4 Rolling Stock

The concept for the Sky Bus Metro vehicles is described in chapters 8 to 12 of the Conceptual Design Document. The vehicles consist of an electrically powered suspender frame (comparable to the under frame of standard outline rail car vehicles) and a suspended coach body.

Following aspects are relevant with respect to safety.

Load cases and superpositioning of load cases

To safely design the structural elements of the vehicle it is important to systematically summarise the loads and their superpositioning. This has to include the loads related to mass of the design, the passenger mass, traffic loads (e.g. movement on imperfect track, acceleration/ braking loads, centrifugal loads) and any other additional load cases as required (e.g. earthquakes, strong winds). Furthermore those basic design dimensions, degrees of freedom used in the calculation have to be referenced in technical drawings. Used formulas and standards have to be named. Design loads, mass, mass distribution have to be referenced in technical drawings. Speed, acceleration, braking (e.g. EN 13452) as well as comfort and dynamic parameters have to be available in a systematically structured manner.

As all the stated parameters are interface parameters to the guideway, or are themselves depending on guideway alignment parameters, it has to be verified, that these interface values are the same as used in the guideway construction.

Specific loads named in the available Sky Bus Metro documentation require further review:

Connection between car bodies

To avoid collisions between the car bodies (e.g. due to unbalanced passenger load), a physical load bearing connection should be provided between the bodies (e.g. as part of the gangway).

Passenger load

The planned density of passengers appears too low in comparison with relevant standards and with real loads appearing on current mass transit systems in India and worldwide. To avoid over loading with regard to a fixed load carrying capacity of the vehicle, standing space should be converted to seating space or overall floor space should be reduced in order to avoid over loading in crush load conditions. Alternatively a vital system for vehicle occupation control must be provided, which would be a new and unknown aspect for mass transit systems.

Longitudinal loads

In addition to the loads stated in the Conceptual Design Document, the suspender frames are also subjected to longitudinal forces. Assuming that the vehicles are normally running in an automatic signalling environment crash properties can be reduced to those required during coupling of units and derailment. Any manual back up signalling procedures have to be catered for (using e.g. sufficient speed reduction) in this regard, as no automatic protection will be available. The suspender frames are also subjected to the longitudinal buffing and drawing loads caused by multi unit operation and during pushing and pulling a rescued train.

Passenger comfort

The maximum accelerations and shock level permitted for passenger use is a safety relevant matter, in order to avoid tripping and falling of standing passengers. Safety standards on this issue are available.

Design and safety standards and existing operational technical solutions as part of other mass transport systems on the above issues are available. Suitable factors of safety can be derived from standards of related technical areas (e.g. passenger cableway trolley installations).

With respect to other successfully operating mass transportation systems it is assumed, that this aspect of the Sky Bus Metro system can be developed using suitable design and safety standards to allow safe passenger operation.

As a comment on the proposed design concept, it shall be stated that the relative length of the suspenders, the permitted car body swing in longitudinal direction and possible construction tolerances in length and alignment of the suspender sections and joints will cause higher load cases to the Sky Bus Metro structure than a rigid design and a design placed closer to the suspender frame would.

Coupling between units

A suitable automatic and safe coupling device must be used to couple trains for multi unit operation or emergency assistance to allow push- and pull- operations. Otherwise train separation during downhill driving or braking could not be avoided. Draw gear must allow for the geometrical movement of the suspenderframe at all points of the actual track alignment, otherwise manual assistance would be needed to couple units in an emergency. Any manual assistance to be given from inside the guideway would drastically lengthen reaction times in emergency situations. The gear must also couple in the most unfavourable positions of the track alignment to serve for its emergency purpose, otherwise the emergency concept could not assume an automatic coupling capability.

For this aspect, suitable standards are existing and technical solutions are available.

Clearance envelope

The clearance envelope needs to be known in order to avoid collisions between vehicles or vehicles and infrastructure. Based on the vehicle design parameters (dimensions, possible swing and degrees of freedom), alignment parameters and additional assumptions (e.g. wind load), the required clearance envelope needs to be established in tabular manner and independently reviewed. The clearance is an interface parameter which has implementations on the geometry (and therefore load cases) of the guideway structure. Existing safety relevant standards regarding light rail systems can be adopted to solve this issue.

A special issue is the proposed operation over public streets. Special precautions have to be developed in order to avoid collisions with high road vehicles, construction vehicles or scaffolding.

Further the interface between vehicle and station platforms must allow safe transition of passengers. It is therefore deemed necessary, that the vehicle floor shall not be moving in relation to the platform to avoid trapping, crushing or falling of passengers onto the ground below. Technical solutions on this aspect are existing on other suspended transport systems. A safe technical solution for this aspect is therefore deemed feasible.

Doors

Double leaved doors of 4m width shall be provided according to the proposed concept. They must be interlocked with the signalling and control system as well as the platform doors. During closing they must provide measures to avoid passengers becoming trapped or directly injured by the closing forces. If the doors can not close completely the vehicle shall not be able to depart due to interlocking with the signalling and control system. The proposed automatic operation requires suitable safety equipment in this regard.

External operation of the doors shall be possible by emergency services in order to evacuate passengers.

Standards regarding door closing speed and closing force limitation as well as for obstacle detection are available as state of the art requirements. Safe implementation of this aspect of Sky Bus Metro is therefore deemed feasible.

Comments on this issue:

It is felt, that two pairs of individual doors could have beneficial aspects for availability of the system, as a non operational doorway would deem the relevant car body useless in service.

It is further suggested, that initial calculations on door closing forces are performed, as the extremely wide doors might be too heavy to comply with door closing force standards when operated at 1m/s.

Braking

Suitable standards for braking performances of mass transport systems are existing (e.g. EN 13452). The longitudinal swinging effect will however cause unloading of the rear bogie to a certain degree, which has to be catered for in the brake design calculations.

A fitted anti slide system is a vital system and needs certification according EN 50126-50129. Technological solutions in this regard are however available.

Passive and active fire protection

The Conceptual Design Document states in chapter 8 that suitable fire protection standards will be used for the design. Due to the fact, that passengers can not disembark the vehicle at any point of the guideway, the requirements for metro rolling stock shall be used. Technical solutions are available. Refer to chapter 5.5.3 for general aspects.

Electrical safety

The aspect electrical safety is closely related to fire protection, as it shall prevent the hazards sparking/ fire and electrocution. This aspect is not Sky Bus Metro specific and technical solutions as well as safety standards are available.

Conclusion Rolling Stock

The provided description for Sky Bus Metro rolling stock (Refer Chapter 8 of the Conceptual Design Document) is a high level concept document which already addresses most of the above mentioned issues.

All discussed safety relevant issues are covered by existing safety standards or even existing technological solutions. Technical implementation therefore appears feasible.

Detailed technical drawings or implementable technical solutions have not been included in the submitted documentation at this stage of the project.

All issues regarding rolling stock require further detailed development and review in order to achieve an implementable status.

6.2.5 Rail-wheel interaction

The wheel rail interaction of the Sky Bus Metro system is significantly different from any other steel wheel on steel rail system due to the pendulum effect of the suspended mass under the vehicle. The mass distribution between suspender frame and coach body will significantly shift with changes in passenger loading, likely affecting safety against derailment. The wheel rail contact is greatly depending on the geometrical position of hinges and mass points, which shall be represented in design drawings.

The Derailment Arrestors and the Swing Arrestors would in the eventual case of marginal or unstable vehicle running behaviour bring a small diameter wheel into contact with a suitably designed concrete surface inside, respectively underneath the guideway girder. This would result in a load transfer from the main wheels towards the new contact points, which requires detailed in-depth theoretical and practical review in order to serve as a safety feature in public mass transport systems.

Furthermore the position of the hinges as well as their angular restraints will be of paramount importance for the magnitude of effect on the axle loading and due to this for the interaction of wheel and rail. Without a detailed calculation concerning the rail-wheel-interaction no prediction about the probability of derailment despite derailment arrestors can be given.

Detailed calculations in addition with verifying test results have to show, that the designed derailment arrestors will be suitable to withstand the loads and forces which will occur in the case of derailment.

Further description will also be required on how to suitably bridge the expansion gaps between guideway sections and how the proposed geometrical tolerance of 10mm (required for the Derailment Arrestors) throughout the guideway cross section will be build and maintained during the live of the system (compensation measures for wheel wear, rail wear, settlement/ flex of guideway, thermal expansions would be required).

Sufficient proof is required, that the proposed wheel rail interaction is safe during all possible loading conditions of the vehicle as well as the permitted wear limits of the system and the permitted alignment parameters. It also needs to be proven, that Derailment Arrestors and Swing Arrestors will in critical situations not cause a destabilising effect. A state of the art technological approach should include a series of dynamical calculations between the min / max values of constraining factors (e.g. mass, mass distribution, speed, lateral wind effects, etc.) The theoretical results need to be verified in practical testing.

Conclusion Rail-wheel interaction

In contrast to the common and proven rail-wheel interaction of conventional railway systems the centre of mass distribution will be far below the wheel rail contact points instead of above. Furthermore Derailment Arrestors and Swing Arrestors might engage into an additional contact to the guideway in critical situations. This could potentially cause a destabilising effect in an already marginal situation. In summary this leads to a completely different running behaviour of the entire system which can not be predicted at this state of the project and requires scientific prove by theoretical approach. The theoretical proof shall then be independently assessed and validated in practical testing.

6.2.6 Signalling and Control

The Sky Bus Metro system is an automatic mass transportation system. The signalling and control system of the Sky Bus Metro system has to automatically perform the vital safety tasks

- train separation,
- collision avoidance,
- overspeed control.
- interlocking with the Sky Bus Metro Traversers.

These functions need to be performed with a high degree of safety integrity as any failfunction in this regard can lead to collision of vehicles or vehicles with parts of the infrastructure and a high number of casualties.

For this reason KRCL has stated, that the signalling and control system shall be designed and implement according to safety integrity level (SIL) 4 to EN 50126-50129. This shall ensure, that the system is up to the required degree free from systematic faults and the occurrence of stochastic failures.

Available technical solutions and safety records show that automatic mass transport systems can be safely operated. Even the specific combination of automatic operation and suspended vehicles is proven in use, which shows that KRCL´s aim to develop such a system is technical feasible. No detailed technical solution has been presented in this regard.

6.2.7 Traverser

In the case of Sky Bus Metro Metro, the proposed traverses at the turnaround points at the ends of sky way or at sky way junctions will have to carry a heavy load of Sky Bus Metro consisting of up to 48 tons (if not empty) plus the dead load of the traverser it self.

Due to the fact, that the traversers might be located right over crowded roads or pedestrian areas, as well as that they shall be moved while carrying passengers, the rules and regulations of cranes will be not sufficient. Those of suspended cablecars and chairlifts might be adequate.

Furthermore the traversers have to be safely interlocked with the signaling and control system of Sky Bus Metro.

Despite being relatively big yet moveable technical structures, suitable safety standards for designing the traversers in the proposed way are existing.

6.2.8 Power Supply and Propulsion System

The proposed power supply system will be similar to those of other typical mass transport systems worldwide. All individual aspects as well as the entire power supply system are sufficiently covered by relevant safety standards. Technical solutions are readily available from various suppliers.

All interfaces to the emergency concept, the maintenance concept and others have to be taken into account. The thermal effects created by the propulsion system running in enclosed guideway have to be taken into account.

6.2.9 Maintenance Concept

Maintenance activities at the Sky Bus Metro system are safety relevant regarding two aspects: Maintaining the safety aspects of the system and occupational safety during maintenance.

Maintenance of safety related systems

The safety related systems and their permissive wear limits have to be systematically summarized in the maintenance documentation. Also mandatory maintenance procedures have to be summarized and documented.

In order to maintain the safety properties of the system a systematical approach has to be implemented. This aspect is not Sky Bus Metro specific and suitable safety related standards are available and with implementation of a quality based maintenance system, this aspect is feasible.

Occupational safety during maintenance

In comparison to ground based public transportation systems the height of the guideway and the position of the motorized suspender frame thereon creates additional hazards to the maintenance workers. Existing related safety standards and available technical solutions show, that these hazards can be sufficiently controlled. Special attention has to be given towards safe interlocking of the open rail power supply and the access of workers to the same area.

Conclusion Maintenance System

Chapter 19 of the Conceptual Design Document gives a high level concept which already addresses the above mentioned issues to some extent. Implementable technical solutions have not been submitted at this stage of the project, but appear feasible in respect to available safety standards and technical solutions.

6.2.10 Emergency Concept / Evacuation and Rescue Concept

In addition to the general aspects as outlined in chapter 5.5.2 the assessment results of Sky Bus Metro specific aspects are described as follows.

The problems as well as the solutions in case of emergency of a suspended public mass transport system like Sky Bus Metro will be quite similar to those associated with underground systems. In both cases passenger evacuation shall take place at stations as far as possible, as disembarkment in-between stations will not be as time efficient and create additional hazards to the passengers. A suitable example for a transport system with similar problems regarding the emergency concept is the Shanghai magnetic-levitation system.

Train attendant and platform attendant

The current concept shows that train attendants as well as platform attendants will be supporting the automatic operation. This operating staff can be used with advantage in many safety related aspects. The train attendant could open windows in case of a failure of the aircondition, handle the emergency slides and can hold up the communication with the central control centre.

Evacuation of Sky Bus Metro (various scenarios)

As described in the conceptual design document the first step in case of fire in or on the Sky Bus Metro will be to continue the journey until the next station where the passenger will be evacuated towards the platform and the emergency can be easier addressed as on the free line. The stations will have to be equipped with all necessary fire fighting or first aid equipment and operators have to be nominated. Nevertheless a suitable number of fire extinguishers should be provided on board of each Sky Bus Consist.

The rule to reach the next station in case of emergency should always be the first choice because it will be faster and safer for the passengers than the other solutions mentioned below.

However the concept of evacuation at next station requires a higher availability of the propulsion system and the signaling and control system to ensure safe transport until the next station. A suitable approach usually is to prove a certain degree of diverse redundancy at the design.

In case the distance between two Sky Bus Metro Stations will be too far under the view of safety conditions, an emergency station with false slabs under the Sky Way can be designed in-between as shown in the conceptual design document.

In case of a propulsion problem (with the train still able to be pushed or pulled by another Sky Bus Consist) the first choice should be to push or pull the broken Sky Bus Consist to the next or previous station to disembark the passengers. This is only a possible solution as long there will be no additional problem in the cabin which requires fast evacuation like fire.

The next theoretical case is, that the Sky Bus Consist is completely immobilized due to an emergency situation. Neither on its own nor by being pushed or pulled by another train. This case also has to be divided in two sub cases.

The first is that a controlled evacuation is possible; that means there is no fire or panic inside the cabins so that either the passengers can be

- evacuated into another Sky Bus behind, in front or at the other direction by temporary bridge (depending on suitable capability of signalling and control system, availability of ramp e.g. at every station), or
- evacuated by turntable ladder, (only possible in urban areas with fast availability of fire brigade and street access to the guideway), or
- evacuated by emergency chute/ slide (This is depending on a certain height margin as it will not work in situations where the guideway is too low or too high, this is above freeways depending on prior stopping of the traffic below– respectively in traffic jam situations this is depending on clearing a suitable area from traffic first, and it will not work over water. Night time evacuations will require additional review. Depending on the chosen emergency concept, a suitable substructure might be required in all those situations in order to allow passenger evacuation. In discussions the KRCL design team has already described this idea.)

Evacuating by slide, all traffic underneath the Sky Bus has to be warned and stopped before, which can be quite difficult to arrange especial over fast traffic lanes. Another serious problem in case of evacuating by slide can be heavy wind which makes the slide moving or tipping over. A solution could be to use emergency escape tubes instead of slides. Technical solutions for this tube are available (e.g. on the Shanghai maglev system). Furthermore the evacuation by slide or tube or other means on line will require a very substantial time due to the high number of passengers and can therefore not serve as means to evacuate in case of fire in the cabin.

The second scenario of fire in the cabin and Sky Bus can not move at all, describes one of the worst cases of emergency. Here the suitable approach should be to use state of the art fire redundant materials and suitably reviewed and independly assessed design solutions to reduce ignition sources, ignitebility, fire propagation and suitable separation of critical equipment. In addition the availability of the propulsion system has to be high with could be addressed by diverse redundancy of essential components.

Furthermore a spread of fire from the cabin to the bogies or vice versa, has to be prevented for at least the time required to detect a fire and evacuate the passengers in an orderly manner from an immobilised vehicle by using highly fire-resistant materials only and suitable geometric separation (passive fire protection).

Unbearable Environmental Conditions for Passengers

In case of a failure of the air-conditioning system the vehicle will heat up caused by the body heat of the passengers and the sun radiation. In addition a minimum fresh air flow might not be available. The common solution should be to disembark the passengers at next station and to take the specific Sky Bus Consist out of service. In case passengers can not be disembarked for what ever reason it has to be ensured that, depending on the temperatures, passengers can be evacuated in an orderly manner.

It might be possible that this evacuation can be slightly suspended when the upper quarter of the windows can be opened by the train attendant with a specific key.

Emergency Communication

A public address system shall be provided for communication between control facility and passengers. For the communication between staff and control facility a voice over IP system shall be used.

Use of emergency equipment

The emergency handling of doors, fire alarm buttons or hand fire extinguisher should always be organised in several steps to prevent malpractice. A three step approach could be 1. striking and braking a button cover, 2. pressing button or screwing handle, 3. starting action e.g. open door.

Emergency Signal

For the case of emergency a device which can be activated by passengers for stating an emergency situation has to be provided. This emergency signal device shall not stop the sky train directly. The emergency signal shall be sent to the central control centre and the control and signalling system where further steps will be initiated, e.g. the train will be brought to a halt at the next stop, or the train will not leave a station when still at the platform.

Another emergency braking possibility shall only be accessible by the train attendant and shall stop the train immediately without interaction by the control centre.

Collision between Sky Bus and road vehicle

In case of collision between Sky Bus Consist and obstacles (e.g. the roof or the load of road vehicles or building equipment) this incident has to be detected and the central control centre has to be informed. The detection as well as the notification can be automatically or by the train attendant. Detection and notification have to be followed by initiating an emergency brake to limit further damage and assess the situation.

Sudden and Prolonged System Disruption

It is possible that the Sky Bus system consist has came to a halt due to a signal point problem, that can not be rectified swiftly. In a case like this all Sky Busses on line have to be evacuated either at a station or in case all possible stations are already occupied and shunting is not possible, in-between stations.

In that case, an vital remote control function or an emergency control panel on board the Sky Buses linked with an emergency signalling system should enable the Sky Bus staff to drive all of the Sky Bus consists first to a station to disembark the passengers and afterwards into a parking/waiting position so that other Sky Bus consists can use the same station for disembarking the next train.

Conclusion on Emergency Concept / Evacuation and Rescue Concept

Several of the above mentioned scenarios and possible concepts are in varying level of detail addressed in the supplied concept document. Due to various available international safety standards on this topic, due to available technical solutions and already implemented similar concepts at other mass transport systems, this critical aspect of Sky Bus appears technological feasible. Further detailed design work and conceptual proof are required to represent an implementable level.

6.2.11 Fire Protection Concept

In addition to the general aspects as outlined in chapter 5.5.3 the assessment results of Sky Bus Metro specific aspects are described as follows.

Passive fire protection

All materials of Sky Bus Consist have to withstand fire at least as long as the fire detection and the emergency evacuation will require. That means, that in case of a fully engaged Sky Bus Consist with 300 passenger and the assumption that each passenger will need 10 seconds to disembark via two well working emergency slides, about 25 minutes will have to be taken into account until the last passenger has left the cabin.

Furthermore in case of fire at the propulsion system at the bogies or at the air-condition system on top of the cabin roof, the train attendant and/or the central control centre has to be informed to initiate further steps. This requires vital active fire protection for reducing the fire detection time.

Active fire protection

The fire detection equipment inside the cabin will be backend up by the train attendant and the passenger too. But vital fire detection is very important at the propulsion system and the bogies inside the guideway. Critical parts of the air-conditioning system on the roof of Sky Bus should be covered as well.

A suitable number of on board fire extinguishers inside the Sky Bus Consists shall be provided.

At Sky Stations water hydrants shall be available supported by hand fire extinguishers and further fire fighting equipment.

7 Summary of the Initial Assessment

The subject of this report is the Sky Bus Metro system concept under development by Konkan Railway Corporation Limited (KRCL), a Government of India Undertaking, as described in the Conceptual Design Document, Version 1, KRCL, 09.01.2004.

This report provides the results of the determination of the “Level of Maturity for Safety Application” of the Sky Bus Metro system concept before starting a CENELEC safety certification according to EN 50126 – EN 50129 (refer to chapter 1.2, The Task).

The results are limited to the information supplied in the Conceptual Design Document, Version 1, KRCL, 09.01.2004.

The results are hereby summarized as follows.

7.1 Identification, Format and Structure

Format and structure do not comply with the requirements regarding unique document number, author, and authorization of the document. For future revisions please regard the remarks in the table in chapter 6.1, Formal Criteria.

7.2 Statement on the Level of Maturity for Safety Application

The presented documentation on the Sky Bus Metro system is a connectional level document with some isolated issues covered in more detail. The general level of content is appropriate for the requirements of this initial study. The more detailed parts of documentation could not be reviewed, mainly due to the fact that no systematic technical specification was available and systematic interfacing between subsystems is not suitably detailed or not provided at all at this stage of development.

In summary the general concept of Sky Bus Metro as a suspended light rail system appears technical feasible as a mass transportation system and development potential to reach a state required for safe implementation has been identified, based on a number of conditions:

- Due to the complexity of the system a systematic safety certification and management shall be provided. KRCL is proposing to develop and seek certification for the Sky Bus Metro system (including the automatic signalling and control system) according to the CENELEC standards (EN 50126-50129) in order to ensure that hazards and associated risks of the system will be systematically identified and mitigated in an ongoing process during the design period of the system.
- Those aspects described in the Conceptual Design Document, Version 1, which require further design work and in some cases basic scientific review to reach the level of safe technical implementation are reviewed and identified in detail in chapter 6 of this report.
- The statement is limited to the information supplied in the Conceptual Design Document, Version 1, KRCL, 09.01.2004. The provided statements about the Conceptual Design Document are based on the authors professional knowledge of other mass transportation systems in general, the identification and review of mass transport systems specifically suitable for a comparative review (chapter 5.1 and annex 2 and 3 of this report) and the knowledge and review of suitable safety standards for implementation and operation of guided mass transport systems (annex 1).

In general the currently available information given in the Conceptual Design Document, Version 1, KRCL, 09.01.2004 is not consistent enough to make a more detailed decision about the level of maturity of the Sky Bus Metro system concept in terms of safety.

7.3 Further Steps

KRCL's plan to prove the required general technical assumptions, calculations and scientific research findings at a prototype test track is a generally accepted procedure. Other mass transport systems with similar characteristics (Wuppertaler Schwebebahn, Safege Monorail, Transrapid) have successfully employed the same approach.

However as a prerequisite, a detailed theoretical prove should be available before proceeding into practical testing. Furthermore test running should also use basic safety management concepts in order to avoid safety related incidents.

Test running requires special training of the operators and shall not engage into limited or full scale public transport without thorough prove of system safety.

Regarding a proper CENELEC safety certification and management approach (refer to chapter 4, Introduction to CENELEC Safety Certification Approach and chapter 5, From Theory to Practice – How to introduce a Sky Bus Metro Certification Process) the following further steps (in that sequence) are recommended:

- Clarification and Specification of the Railway Authority Approval Process
  (refer to chapter 5.1, Previously Achieved Safety Performance and
  chapter 5.2, Safety Policy and Safety Targets)

- Clarification and Specification of the Railway Authority RAMS Policy and Targets
  (refer to chapter 5.2, Safety Policy and Safety Targets)

- Preparation of a Certification Plan / Safety Plan
  (refer to chapter 5.3, Certification Plan / Safety Plan)

- Performance of a Preliminary Hazard Analysis (PHA)
  (refer to chapter 5.4, Preliminary Hazard Analysis)

- Establish basis System Safety Concepts and System Requirement Specification
  (refer to chapter 5.5, System Requirements Specification)

Cologne, June 30, 2004
TIT-br-stei-wig-wu
The Authors

Dipl.-Ing. Peter Wigger	Dipl.-Ing. Thomas Brandt	Dipl.-Ing. Winfried Steinert	Dipl.-Ing. Maik Wuttke
For chapters 4 and 5.2 to 5.5	**********	Jointly for the entire report	**********