S9.3 Part 3: Safety Management Report

for the development of an STM ATB

Colophon	
Document ID	S9.3
Version	2.0
Revision	787334
Author	A
Reviewed	787334 ,STMA-82038
Approved	787334 ,STMA-82045
Archive	SID-2156
Date:	2023/04/28 10:35

Authorization

Compiled by: WD Signature/E-sign: 787334 ,STMA-82029	Date: 2023/04/28 11:28
Reviewed by: HRi Signature/E-sign: 787334 ,STMA-82038	Date: 2023/04/28 12:00
Approved by: WD Signature/E-sign: 787334 ,STMA-82045	Date: 2023/04/28 13:08

Contents

1 Preface

1.1 Introduction

This report is part of the Generic Product Safety Case for STM ATB and provides documented evidences of safety management throughout the STM ATB system development phase.

1.2 References

Reference documents

All the documents references used in this document can be found in the document P6.1 Bibliography available in the Polarion folder Processes

Abbreviations, definitions and terminology

An overview of the abbreviations, definitions and terminology used in this document can be found in document P6.2 List of abbreviations, definitions and terms available in the Polarion folder Processes

Requirement identification

The STM ATB project makes use of an automated requirement management system. In this system each requirement has been identified as a work item. Each work item has been automatically assigned with a unique ID, with the format "STMA-<number>". As a result requirement ID's are not in logical order. An overview of all the used STMA-numbers is given in document P6.3 Requirement Overview available in the Polarion folder Processes

2 Evidence of safety management

2.1 Safety Life Cycle

The safety life cycle for the STM ATB product development is described in the Safety Management Plan. This includes the arrangements for qualification, training and independence.

S1.0 Safety Management Plan

For each life cycle of the initial product development a Gate Review has been carried out by the Validation Team. Prior to formal closure of the phases, the requirements from the standard have been verified for that phase. The results are reported separately for each phase.

V1.91 Gate Review Report - Phase 1
V2.91 Gate Review Report - Phase 2
V3.91 Gate Review Report - Phase 3
V4.91 Gate Review Report - Phase 4
V5.91 Gate Review Report - Phase 5
V6.91 Gate Review Report - Phase 6
V7.91 Gate Review Report - Phase 7
V8.91 Gate Review Report - Phase 8
V9.91 Gate Review Report - Phase 9

For STM ATB Version 1.1 The life cycle has been partially repeated dependent on the hardware and software changes described in D4.9. An additional System Validation report (V9.111) has been made by the Validation Team. This covers the modifications in V1.1 and the results of non-regression testing.

2.2 Safety Organisation

For STM ATB V1.0:

The safety organisation is described in the Safety Management Plan. This includes the arrangements for qualification, training and independence.

S1.0 Safety Management Plan

The STM ATB project organisation chart is defined in Q1.3.1 in SVN. The chart is managed and updated by the STM ATB project manager.

For STM ATB V1.1:

The STM ATB project organisation chart is defined in an updated version and is now stored on the NS Sharepoint. The chart is managed and updated by the NS STM ATB project manager.

2.3 Safety Management Plan

A Safety Management Plan (S1.0) has been made.

S1.0 Safety Management Plan

2.4 Hazard Log

The procedure for the Hazard Log is elaborated in the S3.0 Hazard Log Plan.

The hazard log is managed in Polarion S3.1 Hazard Log

In the early phase of the project Hazard Identification session with experts have been held. Additional hazard identified during hazid sessions and the product development have been added to the hazard log.

Risk have been classified. A procedure for closure of Hazard Log items has been described. Key is that the mitigation measures are implemented in the design, taken into account in manuals or exported to the responsible parties.

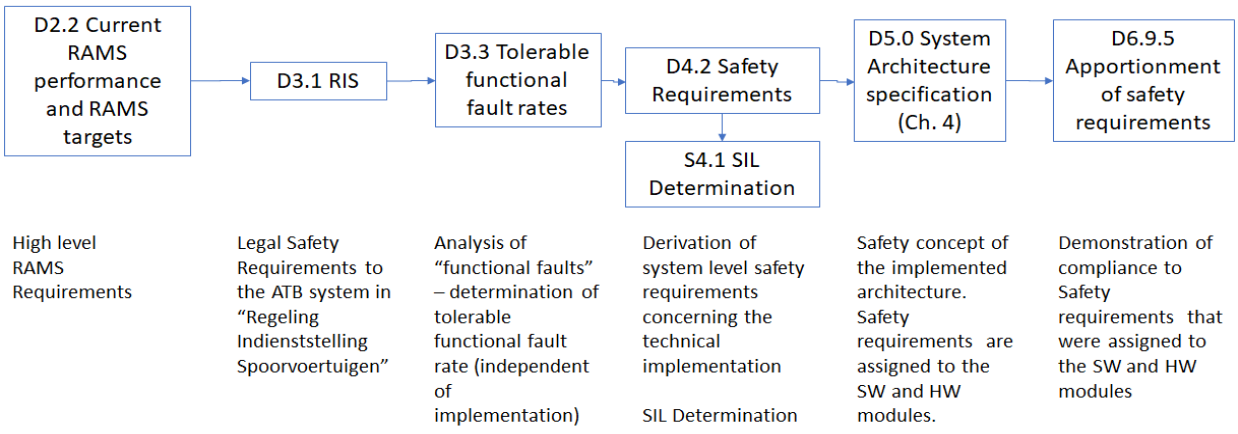
The hazard log (S3.2) report gives a complete overview of the Hazard Log items S3.2 Hazard Log Report

Transferred hazard log items are stored in S3.5 Transferred Hazard Log Items Report

For STM-ATB version 1.1 the above mentioned documents have been updated due to the modifications.

2.5 Safety Requirement Specification

The figure below explains how Safety Requirements have been taken into account within different phases of the life cycle.



In this paragraph the safety management approach is explained. The Safety Requirements for the STM ATB are elaborated during the subsequent life-cycle steps.

In the early phases (1+2) the system concept, the RAM performance of the current systems and the targets for the STM ATB have been studied. In phase 3 the legal requirements are taken from the RIS (see D3.0) and a fault tree has been made to derive the tolerable functional fault rate for all functions of the STM ATB. In phase 3 also a safety study has been carried out to investigate the safety performance of the current ATB systems. In phase 4 safety requirements have been derived taking into account the global technical implementation (such as interfaces, data storage and calculations). Also in this phase, the SIL has been determined. In phase 5 the (safety) architecture of the STM ATB is defined and analysed. More detailed safety requirements are derived for the system functions, which in turn have been apportioned to the hardware and software modules, together with diagnostic functions and safety measures during operation and maintenance. In Phase 6 the STM ATB is designed/implemented in detail and the compliance tot the safety requirements from the previous phase is demonstrated, by analysis and test results..

2.6 System/sub-system/equipment design

For STM ATB V1.0 the planned design activities related to the different life-cycle phases are included in the Development + RAMS Plan.

D0.4.1 Development + RAMS plan

The verification of compliance to the requirements from the railway standards are included in the Gate Review process.

V1.91 Gate Review Report - Phase 1
V2.91 Gate Review Report - Phase 2
V3.91 Gate Review Report - Phase 3
V4.91 Gate Review Report - Phase 4
V5.91 Gate Review Report - Phase 5
V6.91 Gate Review Report - Phase 6
V7.91 Gate Review Report - Phase 7
V8.91 Gate Review Report - Phase 8
V9.91 Gate Review Report - Phase 9

The verification reports R*.99 have been produced per phase. The verification reports provide information on requirement coverage and traceability.

Apart from the Gate Reviews, the Safety Management activities in the system development phase include:
- Review of the FTA
- Safety and quality management plan.
- Hazard log plan and hazard log implementation
- Review and approval of the Safety Requirements (D4.2) and SIL determination.
- Organisation of HAZID sessions
- Review of the system architecture requirements and diagnostic measures.
- Internal audits
- Communication with the railway inspectorate (ILT)
- Communication with stakeholders on system requirement specifications
- Review of the module requirement specifications
- Review of the EMC measures
- Review of the diagnostic measures
- Review of the FMEAs and the CCFA.

For the modifications implemented in STM ATB V1.1 the project plans have been extended.
The Safety Management activities for STM ATB V1.1 include:
- Check of the Change Order, the authorization and the impact of the changes
- Maintaining the Hazard Log
- Reviewing system manuals
- Safeguarding of the safety organisation (role separation)
- Check for the adequacy of test plans
- Organizing functional safety/non-regression testing and review of the test results

2.7 Safety reviews

The safety reviews are included in the Gate reviews.

V1.91 Gate Review Report - Phase 1
V2.91 Gate Review Report - Phase 2
V3.91 Gate Review Report - Phase 3
V4.91 Gate Review Report - Phase 4
V5.91 Gate Review Report - Phase 5
V6.91 Gate Review Report - Phase 6
V7.91 Gate Review Report - Phase 7
V8.91 Gate Review Report - Phase 8
V9.91 Gate Review Report - Phase 9

2.8 Safety verification and validation

Safety verification and validation has been checked during all phases by means of the Checklist based Gate Reviews.

V1.91 Gate Review Report - Phase 1
V2.91 Gate Review Report - Phase 2
V3.91 Gate Review Report - Phase 3
V4.91 Gate Review Report - Phase 4
V5.91 Gate Review Report - Phase 5
V6.91 Gate Review Report - Phase 6
V7.91 Gate Review Report - Phase 7
V8.91 Gate Review Report - Phase 8
V9.91 Gate Review Report - Phase 9

The verification reports R*.99 have been produced per phase. The verification reports provide information on the requirement coverage, implementation coverage and test coverage per phase.

Apart from the Gate Reviews, the Safety Management activities in the test phase include:
- review of the hazard log mitigating measures and closure of the hazard log
- review of the 75Hz filter characteristics
- spot checks on test coverage of module tests and module integration tests
- review of the ATB decoder test plan, review of the test implementation and review of the ATB decoder test results
- review of the test results on diagnostic measures
- review of the profibus lab test results
- review of the environmental lab test results
- participation in CCB and change decisions
- specification of the track-to-train signal transfer tests and review of the test results
- specification of interface tests for ATB antenna interface of STM ATB and review of the test results
- specification and implementation of the functional system safety tests
- specification and implementation of the interface tests and test results
- review of the technical safety report
- review of system manuals.

For STM-ATB version 1.1 the safety management plan has been followed. The results of this are reported in V9.111.

2.9 Safety Justification

Safety justification is done by means of the Safety Case documents (number in the S9.x range).

2.10 System/sub-system/equipment handover

For STM ATB, version 1.0: After formal discharge of the development project team the STM ATB design will be handed over and accepted by the ERTMS-NL program. The technical documentation of the STM ATB (the so-called blueprint) together with an STM-ATB null-serie will be made available to potential suppliers under certain legal and contractual conditions, laid down in a license agreement.

For STM ATB version 1.1 an internal handover of the technical documentation will be done to the project teams responsible purchasing the STM ATB and for integration in the various NS rolling stock series.

2.11 Operation and Maintenance

Maintenance is included in document M9.4 Maintenance Manual

Requirements to Operation is documented in M9.5 User Manual

2.12 Decommissioning and disposal

Requirements to decommissioning and disposal are included in the Maintenance Manual.

M9.4 Maintenance Manual