2017:00826- Restricted

Report

Safety Assessment Report

DK-STM Generic Application version 03.00.13

Author(s)
Narve Lyngby
Ulrik Johansen

SINTEF Digital
System Safety
2021-04-08

SINTEF

SINTEF Digital

Address:
Postboks 4760 Torgarden
NO-7465 Trondheim
NORWAY
Switchboard: +47 40005100

info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

Report

Safety Assessment Report

DK-STM Generic Application version 03.00.13

KEYWORDS:
Safety; Evaluation; Railway; Signalling System; ERTMS/ETCS; STM

VERSION 8.0	**DATE** 2021-04-08
AUTHOR(S) Narve Lyngby Ulrik Johansen	
CLIENT(S) Banedanmark	**CLIENT'S REF.** Torben Hedemann Pedersen
PROJECT NO. 102004427	**NUMBER OF PAGES/APPENDICES:** 66 + 0 Appendices

ABSTRACT

Banedanmark has engaged SINTEF as an independent safety assessor ("ISA") for the STM-DK project.
The safety documentation for the DK-STM Generic Application version 03.00.13 has been assessed. SINTEF sees nothing that speaks against approving the DK-STM Generic Application version 03.00.13 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application.

PREPARED BY Narve Lyngby	SIGNATURE
CHECKED BY Robert Bains	SIGNATURE Robert Bains
APPROVED BY Maria Bartnes	SIGNATURE Maria Bartnes

REPORT NO.	**ISBN**	**CLASSIFICATION**	**CLASSIFICATION THIS PAGE**
2017:00826	-	Restricted	Restricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2015-10-30	This is an update of SINTEF report F26393 version 5.1 based on updated safety documentation. The document number is changed from SINTEF F26393 to SINTEF F27264. For technical reasons, the version of the document is identified as 1.0 instead of 6.0. For the change history of previous versions see the change log in SINTEF F26393 version 5.1.
2.0	2016-07-06	Updated according to Generic Application Safety Case version 03.00.08.
3.0	2017-02-10	Updated to cover safety qualification testing according to Generic Application Safety Case for DK-STM version 03.00.08.
4.0	2017-12-19	Updated according to Generic Application Safety Case for DK-STM version 03.00.09. The report is based on the SINTEF report F27264, v3.0. v3.0 of the report is still valid for v03.00.08 of DK-STM. It is noted that the document number for this version of the report has been changed from F27264 to 2017:00826, this due to SINTEF quality system procedures update.
5.0	2018-10-18	Updated according to Generic Application Safety Case for DK-STM version 03.00.10. This report is based on the SINTEF report 2017:00826, v4.0. The v4.0 of the report is still valid for v03.00.09 of DK-STM.
6.0	2019-02-19	Updated according to Clear Quest Record Details (CFX00414575) for DK-STM version 03.00.11. This report is based on the SINTEF report 2017:00826, v5.0. Version 5.0 of the report is still valid for v03.00.10 of DK-STM.
7.0	2020-11-23	Updated according to Clear Quest Record Details (CFX00491472, CFX00491464 and CFX00477871) for DK-STM version 03.00.12. This report is based on the SINTEF report 2017:00826, v6.0. For more details on which parts of the report that have been updated to cover the DK-STM version 03.00.12 safety assessment, see the introductory part of chapter 1. Version 6.0 of the report is still valid for v03.00.11 of DK-STM.
8.0	2021-04-08	Updated according to Clear Quest Record Details (CFX00517269 and CFX00517273) for DK-STM version 03.00.13. This report is based on the SINTEF report 2017:00826, v7.0. For more details on which parts of the report that have been updated to cover the DK-STM version 03.00.13 safety assessment, see the introductory part of chapter 1. The report at hand replaces version 7.0 of the report.

Table of contents

APPENDICES

None

1 Introduction

Banedanmark has engaged SINTEF as an independent safety assessor ("ISA") for the project "Forberedelse af togkontrollsystem STM". The project aims at developing a Danish Specific Transmission Module (STM) that will enable trains that are equipped with ETCS on-board equipment to operate on Danish lines that are equipped with the ZUB123 automatic train protection system.

The project started as a "Development project" in which a prototype generic application was developed. That prototype has been assessed by SINTEF. The project has later become a "Certification project" resulting in a generic application that has been used as a basis for specific applications.

Siemens A/S has been awarded the contract to develop and produce the generic application for the Danish STM and has submitted the *Generic Application Safety Case*[1] for the certification project.

The DK-STM version 03.00.13 is a maintenance release based on version 03.00.12, covering two change requests as described in QANote_08, ref. [130] and analysed in SafetyNote_20, ref. [131]. The safety documentation has been updated accordingly and assessed in this report. It is noted that the changes made to this report concerning the DK-STM version 03.00.13 update are fully covered by updates made in this section, the new section 3.9, the Assessment chapter 4, and the References chapter 5.

Previous versions of DK-STM have been assessed, ref. [64], ref. [66], ref. [67], ref. [69], ref. [121] and ref. [125]. The report ref. [64] was valid for version 03.00.05 of the software. Based on experience from testing, Banedanmark ("BDK") revised the System Requirements Specification and the software was updated accordingly to version 03.00.06. Some errors were detected and corrected, resulting in version 03.00.07. The Safety Case was updated accordingly and assessed in ref. [66]. Since then, Banedanmark has reworked the System Requirement Specification in order to adjust the STM functionality from the experience gained during tests on the *STM-DK*[2] version 03.00.07, resulting in SW version 03.00.08, which was assessed in [67]. Version 03.00.09, which was assessed in [69], covered the update to comply with the Unisig Baseline 3 Release 2. Version 03.00.10, which was assessed in [121], was a maintenance release covering the correction of four defects. Version 03.00.11, which was assessed in [125], was a bugfix release covering the correction of one defect. Version 03.00.12, which was assessed in [132], was a maintenance release covering the correction of one defect.

The safety analyses provided to SINTEF as basis for the assessment of v03.00.13 of DK-STM does not indicate that former released versions of the DK-STM represents any unacceptable risk related to the two change requests.

1.1 Terminology and conventions used in this report

Terms and statements that SINTEF wishes to draw special attention to are underlined.

Quotations from external documents are given in *italics* and enclosed in quotation marks. An ellipsis (…) is used where part(s) of the quoted text are omitted.

For SINTEF's evaluations of the claims made in the safety documentation, the following terms are used:

Acceptable
If an assessed claim is compliant with the requirements in the standards and can achieve the intended effect it is deemed acceptable. However, an assessed claim can also be acceptable if it can achieve the intended effect

[1] Also denoted *Safety Case* and *GASC* in the report at hand, all terms being synonyms and referenced as ref. [1].

[2] It is noted that the STM-DK and DK-STM are considered as synonym terms, both used in documentation from the manufacturer and also the ISA.

but is not (fully) compliant with the requirements in the standards; in such cases, an explanation is provided in the assessment for the relevant claim.

Tolerable
If an assessed claim is not compliant with the requirements in the standards but does not have a detrimental effect on safety or suitability for use, it is deemed tolerable.

In all other cases an Intermediate/Permanent Application Condition or Reservation (see below) will be given.

Reservation
In cases where evidence is insufficient or missing, the conclusion of this report will be based on the assumption that such evidence can and will be supplied at a later time. Reservations are closed when the necessary evidence has been submitted for assessment and the assessment confirms that the assumption was correct. If a Reservation cannot be closed (i.e. acceptable evidence is not submitted), the conclusion in this report is no longer valid.

In addition, if SINTEF sees possibilities for future improvement, Recommendations can be given. They are intended as aids for future safety work and have no influence on the conclusion in this report.

2 The assessment process

The assessment follows the CENELEC standards:

EN 50126-1:1999	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (ref. [22])
EN 50129:2003	Railway applications - Safety related electronic systems for signalling (ref. [23])
EN 50128:2001[3]	Railway applications - Software for railway control and protection systems (ref. [24])

These require a structured safety case as a foundation for an assessment. The assessor's task is according to EN 50129 (ref. [23]) 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 its intended purpose*".

2.1 SINTEF's assessment procedure

SINTEF has examined documentation that Siemens A/S has submitted. The process is iterative: when the first documents have been examined, if it becomes evident that updates are necessary or further documents have to be looked into, these documents will be requested and submitted. This process is repeated until SINTEF has the impression that a sufficient amount of information has been received.

A more detailed description can be found in the preliminary assessment plan (ref. [2]) which was contractually agreed with Banedanmark and approved by the national safety authority "Trafik- Bygge- og Boligstyrelsen".

The documents have been submitted as PDF or MS Word files. Therefore, they do not all show scanned signatures for approval of released documents. SINTEF is familiar with the releasing process used by Siemens and fully accept that for the majority of the documents electronic signatures are applied.

The assessment starts with the Safety Case for the STM-DK certification project (ref. [1]) and the present report assumes that the reader is familiar with the Safety Case.

Other documents have also been considered during the assessment. The most relevant of those other documents are listed and commented in chapter 5 of the present report.

[3] EN 50128:2001 version of the standard was superseded by EN 50128:2011 at 2017-04-25, see comments in section 3.2.2

3 The Safety Case for Danish STM

3.1 Definition of System

EN 50129, clause 5.1 states:

> "*This shall precisely define or reference the system/subsystem/equipment to which the Safety Case refers, including version numbers and modification status of all requirements, design and application documentation.*"

An overall description of the Danish STM is given in the Definition of System chapter in the Safety Case (ref. [1]). The documents that have been produced within the scope of the STM-DK project are identified with their versions in the document list (DocList, ref. [21)], although this is not mentioned in the Definition of System, but specifically covered within the references section (section 0.3) of the Safety Case..

SINTEF considers the definition of system to be acceptable.

3.2 Quality Management Report

This part shall identify which quality assurance activities were planned and performed and provide evidence that they were performed in the applicable phases of the V-model. EN 50129, clause 5.2, contains "*examples of aspects that should be controlled by the quality management system and included in the quality management report:*

- *organisational structure;*
- *quality planning and procedures;*
- *specification of requirements;*
- *design control;*
- *design verification and reviews;*
- *application engineering;*
- *procurement and manufacture;*
- *product identification and traceability;*
- *handling and storage;*
- *inspection and testing;*
- *non-conformance and corrective action;*
- *packaging and delivery;*
- *installation and commissioning;*
- *operation and maintenance;*
- *quality monitoring and feedback;*
- *documentation and records;*
- *configuration management/change control;*
- *personnel competency and training;*
- *quality audits and follow-up;*
- *decommissioning and disposal.*"

The Quality Management Report addresses all the points plus a few more.

3.2.1 Preface

The preface states that the Quality Management Report "*... broadly contains the elements specified in [CLC/TR50506-2] chapter 5.2.2. (Quality management report structure).*"

SINTEF considers the preface not to be safety-related.

3.2.2 Quality Management System and the Lifecycle Model

Reference is made to the Quality Assurance Plan (QaPl, ref. [42]). The reference process applied for the STM-DK project is the PEACC+ process, which is stated to be compliant with the ISO 9001. The referenced Quality Assurance Plan shall ensure the fulfilment of the CENELEC EN 50129 and EN 50128 requirements. The Quality Assurance Plan has been internally reviewed to ensure that it fulfils its purpose and does not conflict with Siemens A/S Quality System. Siemens A/S is certified according to ISO 9001 and operates according to its QHSE Handbook (QHSE, ref. [43]).

For realisation, the 2001 and 2011 versions of the EN 50128 standard is referenced being applied. The 2011 version in relation to the 2001 version of the standard has been specifically addressed in the safety plan (SySafePl, ref. [93]). For DK-STM v03.00.10, justification that the update can be considered as a "minor change" according to EN 50128:2011, which implies that requirements in section 9.2 of the standard shall be covered, is provided in SafetyNote_17, ref. [57]. Closeout of the EN 50128:2011 section 9.2 requirements are covered in the referenced safety plan. SINTEF is confident that the 2011 version of EN 50128 has been covered satisfactorily in relation to safety. SINTEF has not identified specific issues which is considered to have implications on safety.

SINTEF considers the quality management system and the lifecycle model to be acceptable.

3.2.3 Organisational Structure

Reference is made to the Quality Assurance Plan (QaPl ref. [42]), specifically section 2.2 where EN 50129 requirements concerning Safety Organisation are covered. Document evidence for the project organisation and documentation of personnel competence, independence of roles and staff qualification are referenced (OrgComp, ref. [39]).

The organisation fulfils the requirements for independency between design, verification and validation.

SINTEF considers the organisation to be acceptable.

3.2.4 Quality Goals

Reference is made to chapter 3 of the Quality Assurance Plan (QaPl, ref. [42]), where the sub-goal concerning the maintenance project for R03.00.10 is that the STM-DK maintenance process shall be according to PEACC+. Document evidence is provided in referenced VerRep_03.00.10, ref. [104]. Reports, according to SwVerValPl, ref. [87], which proves that the process has been followed, are referenced and registered in the DocList, ref. [21]. A delta validation is performed in SyValRep_Delta_310, ref. [99]. It is concluded that the requirements from QAPl as referenced are fulfilled.

SINTEF considers documentation of quality goals to be acceptable.

3.2.5 Standards and Metrics

Reference is made to section 3.3 of the Quality Assurance Plan (QaPl, ref. [42]), where requirements related to the use of correct PEACC+ process templates and review procedure and to checking milestone report finalisation and V&V verification quality are specified. Document evidence is identified in the Document List (DocList, ref. [21]).

Monthly quality management reports are present and stored in ELO directory 162616, and signed Milestones reports are present and stored in ELO directory 12878730. For R03.00.10 monthly reports have been replaced by weekly core team meetings, this due to the project short time duration. It is concluded that the intention of the requirements from the QaPl has been fulfilled.

SINTEF considers documentation of standards and metrics to be acceptable.

3.2.6 Quality Planning and Procedures

Reference is made to chapter 2 of the Quality Assurance Plan (QaPl, ref. [42]). In addition, other plans relevant for quality assurance are identified with reference to the Document List (DocList, ref. [21]), i.e. the Organisation- and competence plan (OrgComp, ref. [39]), System Safety Plan (SySafePl, ref. [93]), Configuration Management Plan (CmPl, ref. [17]), and System Ram Plan (SyRamPl, ref. [91]). The documents have been reviewed according to document status in the Document List (DocList, ref. [21]).

Quality records of the STM-DK project are identified: Review documentation; monthly MPPT (Mobility Project Transparency Tool) report; monthly quality management report; milestone reports; verification and validation reports; test reports; and safety and quality audit reports. For R03.00.10 monthly reports have been replaced by weekly core team meetings, this due to the project short time duration.

The main guiding processes used in the project are identified with reference to where described: Document review; source code review; requirement management; configuration and change management; and PEACC+ project guideline.

SINTEF considers the quality planning and procedures to be acceptable.

3.2.7 Specification of Requirements

Reference is made to the Quality Assurance Plan (QaPl, ref. [42]), specifically section 2.2 where EN 50129 requirements concerning System Requirement Specification are covered. Document evidence for specification of requirements according to EN 50129 requirements are provided in the Safety Case and with reference to supporting documentation. The System Requirement Specification (SRS, ref. [70]) is considered to be the customer requirement specification. Supplements and clarifications of the SRS are provided in the SRS Clarification (SRSClar, ref. [71]), this as evidence for fulfilment of EN 50129 identified requirements. A Hazard Log (HazLog, ref. [31]) for the support of hazards in the project has been established.

Review of the SRSClar is documented in the DocList, ref. [21].

It is stated in the Safety Case that every requirement from the SRS has been incorporated in the SRSClar (ref. [71]) and been subject of several reviews; this is confirmed by the review protocols that have been submitted. In addition, a DOORS filter has been created to verify that all requirements from the SRS have a link to SRSClar (ref. [71]).

SINTEF considers the specification of requirements to be acceptable.

3.2.8 Design Control

Reference is made to the Quality Assurance Plan (QaPl, ref. [42]), specifically section 2.2 where EN 50129 requirements concerning apportionment of requirements and design verification and reviews are covered. The design control is supported through the PEACC+ process through review of documentation from the SRS Clarification (SRSClar, ref. [71]) to the Source Code, via System Architecture and SW Requirement Specification (SyArchSpec, ref. [88]), SW Architecture Specifications (SwArchSpecGw, ref. [72] and SwArchSpecZUB, ref. [73]) which include the SW Design Specifications, and SW Module Design Specifications. SRS Clarification (SRSClar, ref. [71]) requirements are traced down to the software module design. Verification and testing shall be according to the complete test program (TstPrg, ref. [101]). Test reports are identified. The process has been verified in VerRep_03_00_10, ref. [104].

SINTEF considers the design control to be acceptable.

3.2.9 Procurement

It is stated that "*The STM-DK will be available in the following versions ... 24VDC ... 110 VDC ... In general the Siemens A/S standard procedures for purchasing and manufacturing (procurement) are used. Siemens A/S is responsible for manufacturing (assembling), product inspection and testing.*"

SINTEF considers procurement to be acceptable.

3.2.10 Manufacturing

It is stated "*The TCC hardware is produced in a Siemens manufacturing plant according to well established processes for procurement of the necessary parts and production of vital hardware ... All other parts needed to manufacture the products ... are produced under the responsibility of Siemens A/S using the standard procedures for purchasing and manufacturing ...*"

SINTEF considers manufacturing to be acceptable.

3.2.11 Product Identification and Traceability

It is stated "*Product identification and traceability is achieved by the product number ... Each product is also assigned a unique serial number.*"

SINTEF considers product identification and traceability to be acceptable.

3.2.12 Handling and Storage

Reference is made to the Application Rules (AppRule_total, ref. [6]) for any requirements concerning the handling and storage of the STM-DK.

SINTEF considers handling and storage to be acceptable.

3.2.13 Inspection and Testing

Reference is made to section 2.6.3 "Quality Records" and 2.8.2 "Design verification and reviews" of the Quality Management Report for the development project. For the final product it is stated "*Inspection and testing in the production will follow internal procedures for production of vital equipment ...*"

SINTEF considers inspection and testing to be acceptable.

3.2.14 Non-Conformance and Corrective Actions

Reference is made to section 4.3 of the Quality Assurance Plan (QaPl, ref. [42]). Normal quality non-conformities are treated according to Mobility Process House (PH), discipline: “Quality Management in the Line, Deviations”, while nonconformities that can lead to hazards are treated as described in the Hazard Log description (HazLog, ref. [31]) and the System Safety Plan (SySafePl, ref. [93]).

Deviations, non-conformities, project changes and risks are registered separately as specified in section 4.1 in the QaPl. Project members shall participate in keeping registrations up-to-date by informing the Project Manager/Project Controller who will make a monthly follow-up on registrations. Defects in the system (software) are handled in ClearQuest as described in the Configuration Management Plan (CmPl, ref. [17]) and in the Introduction to the ClearQuest (CQIntro, ref. [20]).

SINTEF considers non-conformance and corrective actions to be acceptable.

3.2.15 Packaging and Delivery

It is stated that "*Packaging and delivery follow internal Siemens procedures for packaging of vital equipment*".

SINTEF considers packaging and delivery to be acceptable.

3.2.16 Installation

Installation is stated not to be a part of the STM-DK project; installation will not be relevant until the specific application. Reference is made to the Installation Manual (InstMan, ref. [34]); this can be regarded as preparation for future installation.

SINTEF considers installation to be acceptable.

3.2.17 Commissioning

Reference is made to documentation intended to be applicable for commissioning, i.e. the System Description (SysDescr, ref. [94]), User Manual (UserMan, ref. [102]), Installation Manual (InstMan, ref. [34]), and the Maintenance Manual (MaintMan, ref. [38]). This can be regarded as preparation for future commissioning.

SINTEF considers commissioning to be acceptable.

3.2.18 Operation and Maintenance

Operation and maintenance is stated not to be a part of the STM-DK project; operation and maintenance will not be relevant until the specific application. Reference is made to the User Manual (UserMan, ref. [102]) and the Maintenance Manual (MaintMan, ref. [38). This can be regarded as preparation of future operation and maintenance.

SINTEF considers operation and maintenance to be acceptable.

3.2.19 Quality Monitoring and Feedback

References are made to sections 2.6.3 "Quality Records", 2.8.2 "Design Verification and Review", and 2.14 "Non Conformance and Corrective Actions" of the Safety Case, corresponding to sections 3.2.6 and 3.2.14 in this report.

SINTEF considers quality monitoring and feedback to be acceptable.

3.2.20 Documentation and Records

Reference is made to sections 2.5, 2.8.2 and 2.8.3 in the Quality Assurance Plan (QaPl, ref. [42]). This concerns documentation structure traceability where documents are listed in the Document List (DocList, ref. [21]), technical documentation to be stored in ClearCase as described in the Configuration Management Plan (CmPl, ref. [17]), and administrative documentation stored in Siemens' document management system "ELO".

To ensure follow-up on a regular basis, frequent Core Team meetings have replaced the earlier use of the Quality Checklist (ref. [37]). The weekly meetings also include the CCB (Change Control Board) Meeting – where the changes and defects reported in ClearQuest are handled.

SINTEF considers the documentation and records to be acceptable.

3.2.21 Configuration Management/Change Control

Reference is made to section 2.8.1 in the Quality Assurance Plan (QaPl, ref. [42]) concerning software configuration control, specifying that ClearCase shall be used according to description in the Configuration Management Plan (CmPl, ref. [17]).

Software releases are documented in the Software Release Note (SwRelNote, ref. [85]) and practical realization of configuration control is implemented in the CmCtrlSheet, ref. [16].

SINTEF considers configuration management and change control to be acceptable.

3.2.22 Risk Management

Reference is made to section 4.3 in the Quality Assurance Plan (QaPl, ref. [42]) concerning dealing with non-conformities. Deviations, non-conformities, project changes and risks are registered in QualityMaster reports. To ensure follow-up on a regular basis, frequent Core Team meetings have replaced the earlier use of the Quality Checklist (ref. [37]). The weekly meetings also include the CCB (Change Control Board) Meeting – where the changes and defects reported in ClearQuest are handled.

Refer also to section 3.2.14 of this report.

3.2.22.1 Compliance with the Common Safety Method

It is noted that the verification of compliance with the Common Safety Method (CSM) as provided in this report cannot be regarded to follow the formal CSM process according to the referenced regulation. However, the verification of the safety requirements as done in the following are considered to be coverable according to the regulation.

Commission Regulation (EU) 402/2013 (ref. [113]), including the amendment (EU) 2015/1136 (ref. [114]), defines a common safety method (CSM) on risk evaluation to be applied "*to any change of the railway system in a Member State ... when ... the change is considered to be significant ...*". The development of the Danish STM can be regarded as a significant change of the railway system in the sense of the regulation.

The Safety Case does not address the regulation other than referring to it, but compliance with the regulation is implicitly given through compliance with the CENELEC standards, thereby adhering to the principle of "Codes of practice" for fulfilment of the CSM regulation.

The regulation specifies general principles applicable to the risk management process in its annex 1. These are considered in the following:

Table 1: Fulfilment of CSM requirements acc. to refs. [113] and [114]

Annex I Paragraph	Definition	Verification
1.1.1	*The risk management process shall start from a definition of the system under assessment and comprise the following activities:*	Definition of system is given in the Safety Case (ref. [1]), chapter 1.
1.1.1(a)	*the risk assessment process, which shall identify the hazards, the risks, the associated safety measures and the resulting safety requirements to be fulfilled by the system under assessment*	This is defined in the Hazard Log (HazLog, ref. [31]), chapters 3, 6 and section 7.3.
1.1.1(b)	*demonstration of the compliance of the system with the identified safety requirements; and*	This is done through the System Validation Report (SyValRep, ref. [95]) and the delta validation reports (SyValRep-Delta_307, ref. [96]), (SyValRep-Delta_308, ref. [97]), (SyValRep-Delta_309, ref. [98], and SyValRep-Delta_310, ref. [99]).
1.1.1(c)	*management of all identified hazards and the associated safety measures*	This is defined in the Hazard Log (HazLog, ref. [31]), chapters 3 and 6.
	This risk management process is iterative and is depicted in the diagram of the Appendix. The process ends when compliance of the system with all the safety requirements necessary to accept the risks linked to the identified hazards is demonstrated.	
1.1.2	*The risk management process shall include appropriate quality assurance activities and be carried out by competent staff. It shall be independently assessed by one or more assessment bodies.*	This is covered by the Quality Management Report and the Hazard Log (HazLog, ref. [31]), section 2.1 and chapter 5. The independent assessment requirement is covered by the assessment report at hand.
1.1.3	*The proposer[4] in charge of the risk management process shall maintain a hazard record in accordance with point 4.*	This is covered by the Hazard Log (HazLog, ref. [31]), chapter 6.
1.1.4	*The actors who already have in place methods or tools for risk assessment may continue to apply them if such methods or tools are compatible with the provisions of this Regulation and subject to the following conditions:*	See below.
1.1.4(a)	*the risk assessment methods or tools are described in a safety management system which has been accepted by a national safety authority in accordance with Article 10(2)(a) or Article 11(1)(a) of Directive 2004/49/EC; or*	This is covered by the Hazard Log (HazLog, ref. [31]), chapter 4. The safety management system is implicitly accepted by the national safety authority when it accepts the safety assessment report.

[4] The role of the "proposer" is in this "codes of practice" approach regarded to be represented by the Safety Manager, see HazLog, ref. [31]), section 5.1

Annex I Paragraph	Definition	Verification
1.1.4(b)	*the risk assessment methods or tools are required by a TSI or comply with publicly available recognised standards specified in notified national rules.*	This is covered by the Hazard Log (HazLog, ref. [31]), chapter 4. There are currently no notified national rules concerning methods and tools.
1.1.5	*Without prejudice to civil liability in accordance with the legal requirements of the Member States, the risk assessment process shall fall within the responsibility of the proposer. In particular the proposer shall decide, with agreement of the actors concerned, who will be in charge of fulfilling the safety requirements resulting from the risk assessment. The safety requirements assigned by the proposer to those actors shall not go beyond the scope of their responsibility and domain of control. This decision shall depend on the type of safety measures selected to control the risks to an acceptable level. The demonstration of compliance with the safety requirements shall be conducted in accordance with point 3.*	This is covered by the Hazard Log (HazLog, ref. [31]), section 7.2.
1.1.6	*The first step of the risk management process shall be to identify in a document, to be drawn up by the proposer, the different actors' tasks, and their risk management activities. The proposer is responsible for coordinating close collaboration between the different actors involved, according to their respective tasks, in order to manage the hazards and their associated safety measures.*	This is covered by the Hazard Log (HazLog, ref. [31]).
1.1.7	*Evaluation of the correct application of the risk management process falls within the responsibility of the assessment body.*	This is covered by the assessment report at hand.
1.2.1	*For each interface relevant to the system under assessment and without prejudice to specifications of interfaces defined in relevant TSIs, the rail-sector actors concerned shall cooperate in order to identify and manage jointly the hazards and related safety measures that need to be handled at these interfaces. The management of shared risks at the interfaces shall be coordinated by the proposer.*	This is not applicable for a generic application. It will be relevant for the specific application, see the comment after the end of this table.
1.2.2	*If, in order to fulfil a safety requirement, an actor identifies the need for a safety measure that it cannot implement itself, it shall, after agreement with another actor, transfer the management of the related hazard to the latter in accordance with the process set out in point 4.*	This is not applicable for a generic application. It will be relevant for the specific application, see the comment after the end of this table.
1.2.3	*For the system under assessment, any actor who discovers that a safety measure is non-compliant or inadequate is responsible for notifying it to the proposer, who shall in turn inform the actor implementing the safety measure.*	This is covered by the Hazard Log (HazLog, ref. [31]), sections 3.8 and 5.1.
1.2.4	*The actor implementing the safety measure shall then inform all the actors affected by the problem either within the system under assessment or, as far as known by the actor, within other existing systems using the same safety measure.*	This is covered by the Hazard Log (HazLog, ref. [31]), sections 3.8 and 5.1.
1.2.5	*When agreement cannot be reached between two or more actors it is the responsibility of the proposer to find a solution.*	This is covered by the Hazard Log (HazLog, ref. [31]), sections 3.8 and 5.1.
1.2.6	*When a requirement in a notified national rule cannot be fulfilled by an actor, the proposer shall seek advice from the relevant competent authority.*	SINTEF has no information about notified national rules that are applicable to the STM-DK.
1.2.7	*Independently from the definition of the system under assessment, the proposer is responsible for ensuring that the risk management covers the system itself and its integration into the railway system as a whole.*	This is covered by the Hazard Log (HazLog, ref. [31]), section 5.1.

Annex I Paragraph	Definition	Verification
2.1.1	*The risk assessment process is the overall iterative process that comprises:* *(a) the system definition;* *(b) the risk analysis including the hazard identification;* *(c) the risk evaluation.* *The risk assessment process shall interact with hazard management according to point 4.1.*	This is covered by the Safety Case (ref. [1]) and its referenced documents, including the Hazard Log (HazLog, ref. [31]).
2.1.2	*The system definition should address at least the following issues:* *(a) system objective (intended purpose);* *(b) system functions and elements, where relevant (including e.g. human, technical and operational elements);* *(c) system boundary including other interacting systems;* *(d) physical (interacting systems) and functional (functional input and output) interfaces;* *(e) system environment (for example energy and thermal flow, shocks, vibrations, electromagnetic interference, operational use);* *(f) existing safety measures and, after the necessary relevant iterations, definition of the safety requirements identified by the risk assessment process;* *(g) assumptions that determine the limits for the risk assessment.*	This is covered by the chapter 1 of the Safety Case (ref. [1]).
2.1.3	*A hazard identification shall be carried out on the defined system, in accordance with point 2.2*	See paragraphs 2.2.x below
2.1.4	*The risk acceptability of the system under assessment shall be evaluated by using one or more of the following risk acceptance principles:* *(a) the application of codes of practice (point 2.3);* *(b) a comparison with similar systems (point 2.4);* *(c) an explicit risk estimation (point 2.5).* *In accordance with the general principle referred to in point 1.1.5, the assessment body shall refrain from imposing the risk acceptance principle to be used by the proposer.*	The "*application of codes of practice*" (alternative a) is used, with reference to the CENELEC standards. The system, as described in the Safety Case (ref. [1]), has been assessed by SINTEF in the assessment report at hand.
2.1.5	*The proposer shall demonstrate in the risk evaluation that the selected risk acceptance principle is adequately applied. The proposer shall also check that the selected risk acceptance principles are used consistently.*	This is covered by the Safety Management Report (chapter 3) of the Safety Case (ref. [1]).
2.1.6	*The application of these risk acceptance principles shall identify possible safety measures that make the risk(s) of the system under assessment acceptable. Among these safety measures, those selected to control the risk(s) shall become the safety requirements to be fulfilled by the system. Compliance with these safety requirements shall be demonstrated in accordance with point 3.*	This is covered by the Hazard Log (HazLog, ref. [31]) section 3.8, and the Hazard Log Report (HazLogRep, ref. [32]).
2.1.7	*The iterative risk assessment process is considered to be completed when it is demonstrated that all safety requirements are fulfilled and no additional reasonably foreseeable hazards have to be considered.*	This is covered by the Hazard Log (HazLog, ref. [31]) section 3.6, and the Hazard Log Report (HazLogRep, ref. [32]).

Annex I Paragraph	Definition	Verification
2.2.1	*The proposer shall systematically identify, using wide-ranging expertise from a competent team, all reasonably foreseeable hazards for the whole system under assessment, its functions where appropriate and its interfaces.* *All identified hazards shall be registered in the hazard record in accordance with to point 4.*	This is covered by the Hazard Log (HazLog, ref. [31]) sections 3.1, 3.8 and 6.1, and chapter 5.
2.2.2	*To focus the risk assessment efforts upon the most important risks, the hazards shall be classified according to the estimated risk arising from them. Based on expert judgement, hazards associated with a broadly acceptable risk need not be analysed further but shall be registered in the hazard record. Their classification shall be justified in order to allow independent assessment by an assessment body.*	This is covered by the Hazard Log (HazLog, ref. [31]) sections 3.3 and 3.4, and the Hazard Log Report (HazLogRep, ref. [32]).
2.2.3	*As a criterion, risks resulting from hazards may be classified as broadly acceptable when the risk is so small that it is not reasonable to implement any additional safety measure. The expert judgement shall take into account that the contribution of all the broadly acceptable risks does not exceed a defined proportion of the overall risk.*	This is covered by the Hazard Log (HazLog, ref. [31]) section 3.4 and chapter 7.
2.2.4	*During the hazard identification, safety measures may be identified. They shall be registered in the hazard record in accordance with point 4.*	This is covered by the Hazard Log (HazLog, ref. [31]) section 3.1.
2.2.5	*The hazard identification only needs to be carried out at a level of detail necessary to identify where safety measures are expected to control the risks in accordance with one of the risk acceptance principles referred to in point 2.1.4. Iteration may be necessary between the risk analysis and the risk evaluation phases until a sufficient level of detail is reached for the identification of hazards.*	This is covered by the Hazard Log (HazLog, ref. [31]) section 3.3, and the Hazard Log Report (HazLogRep, ref. [32]).
2.2.6	*Whenever a code of practice or a reference system is used to control the risk, the hazard identification can be limited to:* *(a) verification of the relevance of the code of practice or of the reference system;* *(b) identification of the deviations from the code of practices or from the reference system.*	This is covered by the Safety Case (ref. [1]), supported by the assessment report at hand.
2.3.1	*The proposer, with the support of other involved actors, shall analyse whether one, several or all hazards are appropriately covered by the application of relevant codes of practice.*	This is covered by the Hazard Log (HazLog, ref. [31]) chapter 7.
2.3.2	*The codes of practice shall satisfy at least the following requirements:* *(a) They must be widely acknowledged in the railway domain. If this is not the case, the codes of practice will have to be justified and be acceptable to the assessment body;* *(b) They must be relevant for the control of the considered hazards in the system under assessment. Successful application of a code of practice for similar cases to manage changes and control effectively the identified hazards of a system in the sense of this Regulation is sufficient for it to be considered as relevant;* *(c) Upon request, they must be available to assessment bodies for them to either assess or, where relevant, mutually recognise, in accordance with Article 15(5), the suitability of both the application of the risk management process and of its results.*	This is covered by the Safety Case (ref. [1]), worked out in accordance with applicable requirements of the CENELEC standards EN 50126, 50128 and 50129, assessed in the report at hand.

Annex I Paragraph	Definition	Verification
2.3.3	*Where compliance with TSIs is required by Directive 2008/57/EC and the relevant TSI does not impose the risk management process established by this Regulation, the TSIs may be considered as codes of practice for controlling hazards, provided requirement (b) of point 2.3.2 is fulfilled.*	The (EU) 2016/919 version of the CCS TSI mandates use of the Common Safety Method as specified by the Commission Implementing Regulation (EU) 402/2013 (ref. [113]), now including amendment (EU) 2015/1136 (ref. [114])), but contains no conditions concerning how the regulation (e.g. which principle) is to be applied.
2.3.4	*National rules notified in accordance with Article 8 of Directive 2004/49/EC and Article 17(3) of Directive 2008/57/EC may be considered as codes of practice provided the requirements of point 2.3.2 are fulfilled.*	SINTEF has no information about notified national rules that are applicable to the STM-DK.
2.3.5	*If one or more hazards are controlled by codes of practice fulfilling the requirements of point 2.3.2, then the risks associated with these hazards shall be considered as acceptable. This means that:* *(a) these risks need not be analysed further;* *(b) the use of the codes of practice shall be registered in the hazard record as safety requirements for the relevant hazards.*	This is covered by the Technical Safety Report (chapter 4 in the Safety Case ref. [1]), and the Hazard Log Report (HazLogRep, ref. [32]).
2.3.6	*Where an alternative approach is not fully compliant with a code of practice, the proposer shall demonstrate that the alternative approach pursued leads to at least the same level of safety.*	Not applicable.
2.3.7	*If the risk for a particular hazard cannot be made acceptable by the application of codes of practice, additional safety measures shall be identified by applying one of the two other risk acceptance principles.*	This is covered by the Hazard Log (HazLog, ref. [31]) section 3.8.
2.3.8	*When all hazards are controlled by codes of practice, the risk management process may be limited to:* *(a) the hazard identification in accordance with point 2.2.6;* *(b) the registration of the use of the codes of practice in the hazard record in accordance with point 2.3.5;* *(c) the documentation of the application of the risk management process in accordance with point 5;* *(d) an independent assessment in accordance with Article 6.*	For a), b) and c), see the respective identified points 2.2.6, 2.3.5 and 5. For d), concerning the requirement of an independent assessment, this is fulfilled by the assessment report at hand.
2.4.1	*The proposer, with the support of other involved actors, shall analyse whether one, several or all hazards are appropriately covered by a similar system that could be taken as a reference system.*	**Concerns the "reference system" principle.** **Not applicable, CSM is applied according to the "codes of practice" principle.**
2.4.2	*A reference system shall satisfy at least the following requirements:* *(a) it has already been proven in-use to have an acceptable safety level and would therefore still qualify for approval in the Member State where the change is to be introduced;* *(b) it has similar functions and interfaces as the system under assessment;* *(c) it is used under similar operational conditions as the system under assessment;* *(d) it is used under similar environmental conditions as the system under assessment.*	See above.

Annex I Paragraph	Definition	Verification
2.4.3	*If a reference system fulfils the requirements listed in point 2.4.2, then for the system under assessment:* *(a) the risks associated with the hazards covered by the reference system shall be considered as acceptable;* *(b) the safety requirements for the hazards covered by the reference system may be derived from the safety analyses or from an evaluation of safety records of the reference system;* *(c) these safety requirements shall be registered in the hazard record as safety requirements for the relevant hazards.*	See above.
2.4.4	*If the system under assessment deviates from the reference system, the risk evaluation shall demonstrate that the system under assessment reaches at least the same safety level as the reference system, applying another reference system or one of the two other risk acceptance principles. The risks associated with the hazards covered by the reference system shall, in that case, be considered as acceptable.*	See above.
2.4.5	*If at least the same safety level as the reference system cannot be demonstrated, additional safety measures shall be identified for the deviations, applying one of the two other risk acceptance principles.*	See above.
2.5.1	*If the hazards are not covered by one of the two risk acceptance principles laid down in points 2.3 and 2.4, the demonstration of risk acceptability shall be performed by explicit risk estimation and evaluation. Risks resulting from these hazards shall be estimated either quantitatively or qualitatively, or when necessary both quantitatively and qualitatively, taking existing safety measures into account.*	**Concerns the "explicit risk estimation" principle. Not applicable, CSM is applied according to the "codes of practice" principle.**
2.5.2	*The acceptability of the estimated risks shall be evaluated using risk acceptance criteria either derived from or based on requirements contained in Union legislation or in notified national rules. Depending on the risk acceptance criteria, the acceptability of the risk may be evaluated either individually for each associated hazard or the combination of all hazards as a whole considered in the explicit risk estimation.* *If the estimated risk is not acceptable, additional safety measures shall be identified and implemented in order to reduce the risk to an acceptable level.*	See above.
2.5.3	*If the risk associated with one hazard or a combination of several hazards is considered acceptable, the identified safety measures shall be registered in the hazard record..*	See above.
2.5.4	*The proposer shall not be obliged to perform additional explicit risk estimation for risks that are already considered acceptable by the use of codes of practice or reference systems.*	See above.

Annex I Paragraph	Definition	Verification
2.5.5	*Where hazards arise as a result of failures of functions of a technical system, without prejudice to points 2.5.1 and 2.5.4, the following harmonised design targets shall apply to those failures:* *(a) where a failure has a credible potential to lead directly to a catastrophic accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be highly improbable.* *(b) where a failure has a credible potential to lead directly to a critical accident, the associated risk does not have to be reduced further if the frequency of the failure of the function has been demonstrated to be improbable.* *The choice between definition (23) and definition (35) shall result from the most credible unsafe consequence of the failure.*	See above.
2.5.6	*Without prejudice to points 2.5.1 and 2.5.4, the harmonised design targets set out in point 2.5.5 shall be used for the design of electrical, electronic and programmable electronic technical systems. They shall be the most demanding design targets that can be required for mutual recognition.* *They shall neither be used as overall quantitative targets for the whole railway system of a Member State nor for the design of purely mechanical technical systems.* *For mixed technical systems composed of both a purely mechanical part and an electrical, electronic and programmable electronic part, hazard identification shall be carried out in accordance with point 2.2.5. The hazards arising from the purely mechanical part shall not be controlled using the harmonised design targets set out in point 2.5.5.*	See above.
2.5.7	*The risk associated with the failures of functions of technical systems referred to in point 2.5.5 shall be considered as acceptable if the following requirements are also fulfilled:* *(a) Compliance with the applicable harmonised design targets has been demonstrated;* *(b) The associated systematic failures and systematic faults are controlled in accordance with safety and quality processes commensurate with the harmonised design target applicable to the technical system under assessment and defined in commonly acknowledged relevant standards;* *(c) The application conditions for the safe integration of the technical system under assessment into the railway system shall be identified and registered in the hazard record in accordance with point 4. In accordance with point 1.2.2, these application conditions shall be transferred to the actor responsible for the demonstration of the safe integration.'*	See above.
2.5.8	*The following specific definitions shall apply in reference to the harmonised quantitative design targets of technical systems:* *(a) The term "directly" means that the failure of the function has the potential to lead to the type of accident referred to in point 2.5.5 without the need for additional failures to occur;* *(b) The term "potential" means that the failure of the function may lead to the type of accident referred to in point 2.5.5;*	See above.

Annex I Paragraph	Definition	Verification
2.5.9	*Where the failure of a function of the technical system under assessment does not lead directly to the risk under consideration, the application of less demanding design targets shall be permitted if the proposer can demonstrate that the use of barriers as defined in Article 3(34) allows the same level of safety to be achieved.*	See above.
2.5.10	*Without prejudice to either the procedure specified in Article 8 of Directive 2004/49/EC, or Article 17(3) of Directive 2008/57/EC of the European Parliament and of the Council (*), a more demanding design target than the harmonised design targets laid down in point 2.5.5 may be requested for the technical system under assessment, through a notified national rule, in order to maintain the existing level of safety in the Member State. In the case of additional authorisations for placing in service of vehicles, the procedures of Articles 23 and 25 of Directive 2008/57/EC shall apply.*	See above.
2.5.11	*Where a technical system is developed on the basis of the requirements set out in point 2.5.5, the principle of mutual recognition is applicable in accordance with Article 15(5).* *Nevertheless, if for a specific hazard the proposer can demonstrate that the existing level of safety in the Member State where the system is being used can be maintained with a design target that is less demanding than the harmonised design target, then this less demanding design target may be used instead of the harmonised one.*	See above.
2.5.12	*The explicit risk estimation and evaluation shall satisfy at least the following requirements:* *(a) the methods used for explicit risk estimation shall reflect correctly the system under assessment and its parameters (including all operational modes);* *(b) the results shall be sufficiently accurate to provide a robust basis for decision-making. Minor changes in input assumptions or prerequisites shall not result in significantly different requirements.*	See above.
3.1	*Prior to the safety acceptance of the change, fulfilment of the safety requirements resulting from the risk assessment phase shall be demonstrated under the supervision of the proposer.*	This is covered by the approval process for the STM-DK as agreed with the national safety authority.
3.2	*This demonstration shall be carried out by each of the actors responsible for fulfilling the safety requirements, as decided in accordance with point 1.1.5.*	See above.
3.3	*The approach chosen for demonstrating compliance with the safety requirements as well as the demonstration itself shall be independently assessed by an assessment body.*	This is covered by the assessment report at hand.
3.4	*Any inadequacy of safety measures expected to fulfil the safety requirements or any hazards discovered during the demonstration of compliance with the safety requirements shall lead to reassessment and evaluation of the associated risks by the proposer in accordance with point 2. The new hazards shall be registered in the hazard record in accordance with point 4.*	This is covered by the Hazard Log (HazLog, ref. [31]) sections 3.8 and 7.2, supported by the approval process for the STM-DK as agreed with the national safety authority.

Annex I Paragraph	Definition	Verification
4.1.1	*Hazard record(s) shall be created or updated (where they already exist) by the proposer during design and implementation until acceptance of the change or delivery of the safety assessment report. A hazard record shall track the progress in monitoring risks associated with the identified hazards. Once the system has been accepted and is in operation, the hazard record shall be further maintained by the infrastructure manager or the railway undertaking in charge of the operation of the system under assessment as an integrated part of its safety management system.*	This is covered by the Hazard Log (HazLog, ref. [31]) section 3.8, and the Hazard Log Report (HazLogRep, ref. [32]).
4.1.2	*The hazard record shall include all hazards, together with all related safety measures and system assumptions identified during the risk assessment process. It shall contains a clear reference to the origin of the hazards and to the selected risk acceptance principles and clearly identify the actor(s) in charge of controlling each hazard.*	This is covered by the Hazard Log (HazLog, ref. [31]) chapter 3.
4.2	*Exchange of information* *All hazards and related safety requirements that cannot be controlled by one actor alone shall be communicated to another relevant actor in order to find jointly an adequate solution. The hazards registered in the hazard record of the actor who transfers them shall only be regarded as controlled when the evaluation of the risks associated with these hazards is made by the other actor and the solution is agreed by all concerned.*	Not applicable to the generic application; see however the comment after the end of this table.
5.1	*The risk management process used to assess the safety levels and compliance with safety requirements shall be documented by the proposer in such a way that all the necessary evidence showing the suitability of both the application of the risk management process and of its results are accessible to an assessment body.*	This is covered by the assessment report at hand.
5.2	*The documentation produced by the proposer under point 5.1 shall at least include:* *(a) description of the organisation and the experts appointed to carry out the risk assessment process;* *(b) results of the different phases of the risk assessment and a list of all the necessary safety requirements to be fulfilled in order to control the risk to an acceptable level.* *(c) evidence of compliance with all the necessary safety requirements;* *(d) all assumptions relevant for system integration, operation or maintenance, which were made during system definition, design and risk assessment.*	Part (a) is covered by the Hazard Log (HazLog, ref. [31]). Part (b) is the subject of the Hazard Log Report (HazLogRep, ref. [32]). Part (c) is covered by Safety Verification and Validation (see section 3.3.8 of the assessment report at hand), Assurance of Correct Functional Operation (see section 3.4.2) and Safety Qualification Tests (see section 3.4.6). Part (d) is covered by Quality Planning and Procedures (see section 3.2.6 of the assessment report at hand), Specification of Requirements (see section 3.2.7), Design Control (see section 3.2.8) and Operation and Maintenance (see sections 3.2.18 and 3.3.11).
5.3	*The assessment body shall establish its conclusion in a safety assessment report as defined in Annex III.*	This is covered by the assessment report at hand.

With reference to paragraph 1.2.1 of Annex 1 to Commission Regulation (EU) 402/2013 (ref. [113]) (see above) the following statement is made in ref. [117]: "*SRACs identified during development of the DK-STM generic application that could not be mitigated within the project were handed over to various parties via the GASC and the application rules document. On request from Banedanmark all rules are now assembled into one single excel sheet, which is handed over to Bdk. ...*".

For this assessment additional hazards have been transferred to Banedanmark in ACKNOWL_BANE, ref. [4].

SINTEF considers this acceptable evidence for coordination of hazard management with the responsible organisations for the on-board systems that interface with a specific application.

3.2.23 Personnel Competency and Training

Reference is made to section 2.7 in the Quality Assurance Plan (QaPl, ref. [42]) concerning competencies, where competencies of project members are documented in the Organisation and Documentation of Personnel Competence (OrgComp, ref. [39]). The document specifies the roles, responsibilities and required competencies. Proof of competencies is documented separately due to requirements in the personal data law. To ensure follow-up on a regular basis, frequent Core Team meetings have replaced the earlier use of the Quality Checklist (ref. [37]). The weekly meetings also include the CCB (Change Control Board) Meeting – where the changes and defects reported in ClearQuest are handled.

SINTEF considers the personnel competency and training to be acceptable.

3.2.24 Quality Audits and Follow-up

Reference is made to section 4.4 in the Quality Assurance Plan (QaPl, ref. [42]) concerning internal audits. No internal audits are planned for the project. It is the quality- and environmental management function at Siemens A/S which plans and performs internal audits.

An internal audit has been performed (IntAudit_01, ref. [35]), and a safety audit (SINTEF_01, ref. [58]) and quality audits (SINTEF_04, ref. [61], SINTEF_11, ref. [65] and SINTEF_14, ref. [68]) have been performed by the ISA/NoBo.

There were no issues for follow-up.

SINTEF considers the quality audits and follow-up to be acceptable.

3.2.25 Decommissioning and Disposal

It is stated that "*Disposal of the components of the Train Control Computer must be done according to the standard 2012/19/EU (WEEE, Waste Electrical and Electronic Equipment)*". There is no mentioning if there are any special considerations not covered by the referenced standard that should be known when the system is decommissioned. Such conditions should be identified and documented as early as possible. This gives rise to the following:

> **Recommendation 1.** Any special considerations to be taken during decommissioning and disposal that are already known should be described for the finalisation of the STM-DK in the Generic Application Safety Case.

3.2.26 Review of Quality Management System by Top Management

The issue is stated not to be a part of the STM-DK project.

The issue is not a requirement according to EN 50129; SINTEF considers it to be a part of normal quality monitoring and feedback (see section 3.2.19).

3.2.27 Customer Satisfaction

Reference to customer evaluations is provided in the Safety Case.

The issue is not a requirement according to EN 50129; SINTEF considers it to be a part of normal quality monitoring and feedback (see section 3.2.19).

3.2.28 Conclusion

Based on the Quality Management Report it is concluded that the quality management of the STM-DK project has a sufficient coverage and maturity for a SIL4 project. Reference is also made to the conclusion in the VerRep_03_00_10, ref. [104].

SINTEF considers the conclusion to be acceptable.

3.3 Safety Management Report

This report shall document the safety activities that have been performed in order to ensure the necessary safety management during the life cycle. EN 50129, clause 5.3, states which topics shall be addressed, viz.:

1. *Safety life cycle*
2. *Safety organisation*
3. *Safety plan*
4. *Hazard log*
5. *Safety requirements specification*
6. *System/sub-system/ equipment design*
7. *Safety reviews*
8. *Safety verification and validation*
9. *Safety justification*
10. *System/sub-system/equipment handover*
11. *Operation and maintenance*
12. *Decommissioning and disposal*

The Safety Management Report addresses all these points.

SINTEF considers this to be acceptable.

3.3.1 Safety Life Cycle

EN 50129, clause 5.3.2 states:

> "*The safety management process shall consist of a number of phases and activities, which are linked to form the safety life-cycle; this should be consistent with the system life-cycle ...*"

Reference is made to the PEACC+ process which covers phases 4 through 7 of the CENELEC lifecycle. The remaining phases are covered by the System Verification and Validation Plan (SyVerValPl, ref. [100]), the Software Verification and Validation Plan (SwVerValPl, ref. [87]) and the System RAM Plan (SyRamPl, ref. [91]).

SINTEF considers the safety life cycle to be acceptable.

3.3.2 Safety Organisation

EN 50129, clause 5.3.3 states:

> "*The safety management process shall be implemented under the control of an appropriate safety organisation, using competent personnel assigned to specific roles. ... An appropriate degree of independence shall be provided between different roles ...*"

The safety organisation is a part of the project organisation, which is documented in Organisation and Documentation of Personnel Competence (OrgComp, ref. [39]). The software validator and system validator are independent of the project manager.

SINTEF considers the safety organisation to be acceptable.

3.3.3 Safety Plan

EN 50129, clause 5.3.4 states:

> "*A Safety Plan shall be drawn up at the start of the lifecycle. ... The Safety Plan shall be updated and reviewed if subsequent alterations or additions are made to the original system/subsystem/equipment.*"

Reference is made to current version of the Safety Plan (SySafePl, ref. [93]). An earlier version was assessed and approved by SINTEF (see SINTEF_02, ref. [59]). The currently applicable version was evaluated with

DK-STM v03.00.09 in SINTEF_15, ref. [69]. This considers to fulfils the applicable requirements for a Safety Plan as stated in EN 50126 and EN 50129 and is suitable for its intended use.

SINTEF considers the Safety Plan to be acceptable.

3.3.4 Hazard Log

EN 50129, clause 5.3.5 states:

> "*A Hazard Log shall be created and maintained throughout the safety lifecycle ... The Hazard Log shall be updated if any modification or alteration is made to the system, subsystem or equipment.*"

EN 50126, clause 6.3.3.3 requires:

> "*Hazard Log shall include details of:*
>
> *a) the aim and purpose of the Hazard Log.*
> *b) each hazardous event and contributing components.*
> *c) likely consequences and frequencies of the sequence of events associated with each hazard.*
> *d) the risk of each hazard.*
> *e) risk tolerability criteria for the application.*
> *f) the measures taken to reduce risks to a tolerable level, or remove, the risk for each hazardous event.*
> *g) a process to review risk tolerability.*
> *h) a process to review the effectiveness of risk reduction measures.*
> *i) a process for on-going risk and accident reporting.*
> *j) a process for management of the Hazard Log.*
> *k) the limits of any analysis carried out.*
> *l) any assumptions made during the analysis.*
> *m) any confidence limits applying to data used within the analysis.*
> *n) the methods, tool and techniques used.*
> o) *the personnel, and their competencies, involved in the process.*"

Reference is made to the Hazard Log, which has been established in the SharePoint site. Hazards from the customer Banedanmark have now been transferred to Banedanmark, (ACKNOWL_BANE, ref. [4]), and have now been closed in the DK-STM hazard log. Reference is made to the description of the use of the Hazard Log (HazLog, ref. [31]).

A Hazard Log Report has been submitted (HazLogRep, ref. [32]) that reports the status of "*safety relevant entries*" in the ClearQuest database as per 2017-11-28. All 22 hazards are "*Closed*".

SINTEF considers this to be acceptable.

3.3.5 Safety Requirements Specification

EN 50129, clause 5.3.6 states:

> "*The specific safety requirements for each system/subsystem/equipment, including safety functions and safety integrity, shall be identified and documented in the Safety Requirements Specification.*"

Reference is made to the Risk Analyses (Risk-an, ref. [44] and HHGB_RISC_AN, ref. [33]) that was part of the foundation of the requirements specification (SRS, ref. [70]).

SINTEF considers the safety requirements specification to be acceptable.

3.3.6 System and Subsystem Design

EN 50129, clause 5.3.6 states:

> "*This phase of the life-cycle shall create a design which fulfils the specified operational and safety requirements. A top-down, structured design methodology shall be used, with rigorously controlled and reviewed documentation.*"

The system has been designed according to the V-model supported by the EN 50126 and EN 50128 standards. This has been ensured through the support of the model in the PEACC+ process. Figure 5 in the Safety Management Report illustrates how the V-model is supported, covered by reviews and testing at each level in the model.

The Safety Case covers explicitly the Cenelec phases 1, 2 and 3; the Requirement phase; the Architecture phase; the SW product development phase; HW product development phase; the Integration phase; and the Validation phase; including specific documentation references for each phase. DK-STM v03.00.10 is a maintenance release where no updates related to requirements are needed.

SINTEF considers this to be acceptable.

3.3.7 Safety Audits and Reviews

EN 50129, clause 5.3.8 states:

> "*Safety reviews shall be carried out at appropriate stages in the lifecycle. Such reviews shall be specified in the Safety Plan and their results fully documented.*"

Six safety reviews are reported in the Safety Case, each describing its objective and including documentation evidence. Reported findings are either closed in earlier versions of the Safety Case or are further elaborated within the current version of the Safety Case.

A safety audit has been performed by the assessor (SINTEF_01, ref. [58]) with no issues to follow-up (see also section 3.2.24)

In addition, it is stated that "*...individual objects in DOORS have been evaluated for safety relevance*" and "*...safety relevant issues have been considered in the project via the defect management tool, ClearQuest.*". No safety relevant issue in ClearQuestStatus, ref. [15], has been reported. The one non-safety entry from DK-STM v03.00.09 assessment has now been closed, ref. [99].

SINTEF considers the safety audits and reviews that have been performed to be acceptable.

3.3.8 Safety Verification and Validation

EN 50129, clause 5.3.9 states:

> "*The Safety Plan shall include or reference plans for verifying that each phase of the life-cycle satisfies the specific safety requirements identified in the previous phase, and for validating the completed system/subsystem/equipment against its original Safety Requirements Specification.*
>
> *These activities shall be carried out and fully documented ...*"

Safety verification and validation is considered to be an integrated part of the verification and validation processes carried out in the STM-DK project. The processes are defined in the Software Verification and Validation Plan (SwVerValPl, ref. [87]), in the System Verification and Validation Plan (SyVerValPl, ref. [100]), and in the Quality Assurance Plan (QaPl, ref. [42]).

Reference is made to section 3.6 in the Safety Management Report for the main verification and validation reports.

Only the System Validation Report (SyValRep, ref. [95]) and the delta validation reports (SyValRep-Delta_307, ref. [96], SyValRep-Delta_308, ref. [97], SyValRep-Delta_309, ref. [98], and SyValRep-

Delta_310, ref. [99]) have been reviewed by SINTEF with respect to identifying additional safety issues which have not already been covered. The System Validation Report (SyValRep, ref. [95]) evaluates rules coming from the Software Validation Report (ref. [86]). These rules are not included in the application rules (AppRules, ref. [5]) but they are all covered by existing rules or other validation activities. The delta validation report for the 03.00.07 version (SyValRep-Delta_307, ref. [96]) identifies 4 new rules and 4 new constraints, 2 modified rules, 1 deleted rule and 6 deleted constraints with respect to the System Validation Report (SyValRep, ref. [95]). The delta validation report for the 03.00.08 version (SyValRep-Delta_308, ref. [97]) identifies 3 new rules and 3 new constraints, 2 modified rules, 4 deleted rule and 5 deleted constraints with respect to the System Validation Report (SyValRep, ref. [95]). The delta validation report for the 03.00.09 version (SyValRep-Delta_309, ref. [98]) identifies no rules and 3 constraints, 2 changed rules and constraints, 5 deleted rules and no deleted constraints. The delta validation report for the 03.00.10 version (SyValRep-Delta_310, ref. [99]) identifies no new rules and 3 constraints, 2 changed rules and constraints, and 7 deleted rules.

They are addressed in the Technical Safety Report; see sections 3.4.2 and 3.4.5.

SINTEF considers the safety verification and validation to be acceptable.

3.3.9 Safety Justification

EN 50129, clause 5.3.10 states:

> "*The evidence that the system/sub-system/equipment meets the defined conditions for safety acceptance shall be presented in a structured safety justification document known as the Safety Case ...*"

The justification of adequate safety for the STM-DK is provided in the Generic Application Safety Case (ref. [1]).

SINTEF considers the safety justification to be acceptable.

3.3.10 System Handover

EN 50129, clause 5.3.11 states:

> "*Prior to handover of the system/sub-system/equipment to a railway authority, the conditions for safety acceptance and safety approval ... shall be satisfied, including submission of the Safety Case and the Safety Assessment Report.*"

Within the frame of the STM-DK project the handover to the customer is specified in section 3.10 in the Safety Management Report. Reference is made to Bills of Material (BOM_BGR_24V, ref. [11] and BOM_BGR_110V, ref. [10]) and the user manuals (UserMan ref. [102], InstMan ref [34], SysDescr ref. [94] and MaintMan ref. [38]), and Applicationrules ref. [5].

SINTEF considers the system handover to be acceptable.

3.3.11 Operation and Maintenance

EN 50129, clause 5.3.12 states:

> "*Following handover, the procedures, support systems and safety monitoring ... shall be adhered to.*"

The Safety Management Report makes reference to the users' manual (UserMan, ref. [102]) and the maintenance manual (MaintMan, ref. [38]).

SINTEF considers this to be acceptable.

3.3.12 Decommissioning and Disposal

EN 50129, clause 5.3.13 states:

> "*At the end of the operational life of a system, its decommissioning and disposal shall be carried out in accordance with the measures defined in the Safety Plan and in Section 5 of the Technical Safety Report (part of the Safety Case).*"

It is stated that "*Disposal of the components of the Train Control Computer must be done according to the standard 2012/19/EU (WEEE, Waste Electrical and Electronic Equipment)* ", see also section 3.2.25 and Recommendation 1.

SINTEF considers this to be acceptable.

3.4 Technical Safety Report

The CENELEC standard EN 50129 identifies in clause 5.4 the following topics for a technical safety report:

1. *Introduction (design overview)*
2. *Assurance of correct functional operation*
3. *Effects of faults*
4. *Operation with external influences*
5. *Safety-related application conditions*
6. *Safety qualification tests*

These points are all addressed in the Technical Safety Report.

3.4.1 Introduction

EN 50129, clause 5.4 states:

> "*This section shall provide an overview description of the design, including a summary of the technical safety principles that are relied on for safety and the extent to which the system/subsystem/equipment is claimed to be safe ...*"

The Danish STM is exclusively based on the Train Control Computer (TCC) hardware and software platform. The TCC has been validated and approved (see also section 3.5 below). The gateway software and adaptations to the ZUB123 software are developed according to the requirements in EN 50128 (ref. [24]) for a SIL4 application. The test suite shall contain the same tests as for the existing, approved ZUB123 system and then demonstrate that the Danish STM achieves the same results as the ZUB123.

This means that effects of faults as described in section 4.3 in the Technical Safety Report, corresponding to section 3.4.3 of this report, are handled by the TCC platform.

SINTEF considers the technical safety principles to be acceptable.

3.4.2 Assurance of Correct Functional Operation

EN 50129, clause 5.4 states:

> "*This section shall contain all evidence necessary to demonstrate correct operation of the system/subsystem/equipment under fault-free normal conditions ... in accordance with the specific operational and safety requirements.*"

Assurance of correct functional operation is separated into different parts in the Technical Safety Report as summarised in the following:

System architecture is described by the Basic TCC System Architecture, the Application Hardware configuration, and the System Architecture. TCC is a safe SIL4 computer according to EN 50129 with a main computer module VE5 which realises a complete 2v2 system and a number of peripheral modules which realise input and output interfaces. Reference is made to detailed documentation. The Application Hardware configuration, the actual hardware configuration used in the STM-DK, is shown in Figure 7 in the Technical Safety Report. Verification of correct configuration is done in the System Validation Report (SyValRep, ref. [95]) and the delta validation reports (SyValRep-Delta_307, ref. [96], SyValRep-Delta_308, ref. [97], SyValRep-Delta_309, ref. [98] and SyValRep-Delta_310, ref. [99]). The system architecture is shown in Figure 8 in the Technical Safety Report and is explained in detail in the System Architecture Specification (SyArchSpec, ref. [88]) and in the System Description (SysDescr, ref. [94]). Interfaces between the system architecture and its environment are described separately.

Definition of interfaces differentiates between safety relevant system interfaces and non-safety relevant interfaces. Safety relevant system interfaces are: Emergency brake, Antenna A and B, Profibus interface, Isolation switch and Power supply. The Service-PC, Human-Machine interface and interface to remanent memory are not listed, but described in the same sub-section as the named safety related interfaces. The safety aspects for each of these interfaces are covered in the Technical Safety Report, and specifically by safety notes (ref. [47] to [56]), application rules (AppRule, ref. [5]) that apply, and relevant requirements (SRSClar, ref. [71]).

For the Human-Machine Interface it is important that this actually is implemented in the EVC computer which interfaces to the STM-DK via the Profibus interface. From version 03.00.08 the customized interface was applied as described in SafetyNote_12, ref. [55]. The Human Machine interface is described in details in UserMan, ref. [102]. Requirement to MTBF is forwarded to the EVC manufacturer via AppRule 71.

Fulfilment of the SRS Clarification (SRSClar, ref. [71]) is demonstrated in the System Validation Report (SyValRep, ref. [95]) and the delta system validation reports (SyValRep-Delta_307, ref. [96]) and (SyValRep-Delta_308, ref. [97] , SyValRep-Delta_309, ref. [98], and SyValRep-Delta_310, ref. [99]). See the comments in chapter 5 of the report at hand concerning ref. [95], [96], [97], [98] and [99] for more details.

Fulfilment of the Safety Requirement Specification (chapter 9 in SRSClar, ref. [71]) is demonstrated in the System Validation Report (SyValRep, ref. [95]) and the delta system validation reports (SyValRep-Delta_307, ref. [96], SyValRep-Delta_308, ref. [97], SyValRep-Delta_309, ref. [98], and SyValRep-Delta_310, ref. [99]). Some of these requirements are however directed to the Safety Case. Fulfilment of these is covered in section 4.2.4 in the Technical Safety Report. Additional rules from the system validation are also covered there.

Assurance of correct hardware functionality is based on using the validated and assessed TCC platform; using a validated hardware/software configuration; ensuring the fulfilment of all applicable application rules; and performing testing as specified. Document evidence or justification is provided for each of the issues in the Technical Safety Report. Reference is made to the integration tests (SwHwIntTstRep ref. [77] and SyIntTstRep ref. [89].

Assurance of correct software functionality is based on correct function of the Gateway, ZUB123 and TCC components, and the complete STM-DK as a component. For each of the basic components justification is provided with respect to development and validation aspects, and for STM-DK the justification is based on analyses and testing as specified.

SINTEF considers the assurance of correct functional operation to be acceptable.

3.4.3 Effects of Faults

EN 50129, clause 5.4 states:

> "*This section shall demonstrate that the system/subsystem/equipment continues to meet its specified safety requirements, including the quantified safety target, in the event of random hardware faults.*"

Effects of faults are separated into different parts in the Technical Safety Report as summarized in the following:

Concerning *Effect of single faults*, *Independence of items*, *Detection of single faults*, *Effects of multiple faults* and *Defence against Systematic Faults*: The Technical Safety Report section 4.3 claims that by using the TCC platform and fulfilling the application rules for the platform as covered by the related safety cases, all of these situations will be handled satisfactorily. This is considered to be acceptable since both the TCC platform and the STM-DK are developed according to EN 50129 SIL4 requirements.

For *Action following detection (including retention of safe state)*, whenever a fault is detected the STM-DK will enter the failure mode FA. This state cannot be left until the STM-DK has been powered off and powered on again.

SINTEF considers the effects of faults to be acceptably handled.

3.4.4 Operation with External Influences

EN 50129, clause 5.4 states:

> "*This section shall demonstrate that when subjected to the external influences defined in the System Requirements Specification, the system/sub-system/equipment*
>
> - *continues to fulfil its specified operational requirements,*
> - *continues to fulfil its specified safety requirements (including fault conditions).*"

Operation with external influences is separated into different parts. The aspects *Climatic conditions*; *Mechanical conditions*; *Altitude*; *Electrical conditions (on vehicles)*; and *Protection against unauthorized access* are all covered through application rules (AppRule, ref. [5]); the rules are divided into groups called "*type of rule*" such as "*non-functional*", "*climatic*", "*installation*" etc. and individual rules can have more than one type.

SINTEF considers operation with external influences to be acceptably handled.

3.4.5 Safety-Related Application Conditions, SRACs

EN 50129, clause 5.4 states:

> "*This section shall specify ... the rules, conditions and constraints which shall be observed in the application of system/subsystem/equipment.*"

Safety-related application conditions have been transferred to the DOORS module AppRules and are listed in the Safety Case (ref. [1]) grouped according to configuration, system build, operation and maintenance, operational safety monitoring and decommissioning and disposal. Some of them are covered by the installation and maintenance manuals (InstMan, ref. [34] and MaintMan, ref. [38]).

SINTEF considers handling of safety-related application conditions to be acceptably handled.

3.4.6 Safety Qualification Tests

This section shall contain evidence to demonstrate successful completion, under operational conditions, of the safety qualification tests. EN 50129, clause 5.4 chapter 6 demands safety qualification tests as described in Annex B.6 (normative). Section B.6.1 describes the requirements:

> "*The extent and duration of the Safety Qualification Tests shall be agreed between the railway authority and the safety authority, and shall be justified having regard to the degree of novelty and complexity associated with the system/sub-system/equipment.*
>
> *Because completion of the Safety Qualification Tests is contained within the Safety Case, the safety of the system is not fully assured during the test period. Therefore appropriate precautions, procedures and monitoring shall be provided, to ensure safety of the railway during the test period...*"

For previous releases of this report (v1.0 and 2.0) safety qualification tests have been covered by application rules as identified in relevant Safety Case.

SQT was performed and documented with version 3.0 of the report, based on early planning, ref. [115], and the documentation of the test specification, performance and approval, ref. [116].

Four ATC errors were reported, all documented and analysed in ref. [116] and considered by SINTEF not to have safety impact.

The conclusion from the testing documented in ref. [116] was, quoted: "*the DK-STM in Baseline 3 is just as reliable as in baseline 2.3.0d and does not generate more errors than the present ZUB 123 ATC mobile installation*".

It is noted that the testing was done with version 03.00.07 of the DK-STM. This implies that experience testing for DK-STM versions 03.00.08 and 03.00.09 was not explicitly covered by the performed SQT.

SINTEF considers that the planning, specification, performance and documentation of the SQT are according to the requirements as referenced above.

The application conditions related to the SQT were considered closed with respect to the SQT aspect as documented in v3.0 of this report.

For DK-STM v03.00.09 no further activities concerning SQT has been reported. It has been stated by Siemens that SQT is not within the scope for v03.00.09. The relevant application rules for SQT has been deleted, which has been done in full cooperation with Banedanmark (reported in clarification email from Siemens).

For DK-STM v03.00.10 no further activities concerning SQT has been reported.

SINTEF considers handling of safety qualification testing to be acceptable.

3.5 Related Safety Cases

EN 50129, clause 5.1 states:

> "*This shall contain references to the Safety Cases of any sub-systems or equipment on which the main Safety Case depends.*
>
> *It shall also demonstrate that all the safety-related application conditions specified in each of the related sub-system/equipment Safety Cases are*
>
> *either fulfilled in the main Safety Case,*
>
> *or carried forward into the safety-related application conditions of the main Safety Case.*"

Reference is made to the safety cases for legacy ATC and the TCC platform. The SRACs coming from those safety cases are all addressed and either closed (with reference to acceptable documentation), covered by application rules or passed on as SRACs to the specific application. See also section 3.4.5 above.

The previous version of this report (SINTEF_15, ref. [69]) is also addressed. There was no reservations in that report, only one Recommendation which now has been dealt with, ref section 5.7 in the Safety Case.

SINTEF considers the handling of safety related application conditions from the components resp. sub-systems to be acceptable.

3.6 Conclusion

EN 50129, clause 5.1 states:

> "*This shall summarise the evidence presented in the previous parts of the safety case, and argue that the relevant system/subsystem/equipment is adequately safe, subject to compliance with the specified application conditions.*"

The conclusion for the STM-DK project states:

> *"This GASC demonstrates that the DK-STM generic application is sufficiently safe, with the conditions listed below*".

The following conditions (not identified other places in the Generic Application Safety Case (ref. [1])) are listed:

Installation and maintenance:

> *#COND-DK-STM-GASC-007#: Rules and directions prescribed in installation and maintenance manuals must be observed.*

Infrastructure:

> *#COND-DK-STM-GASC-008#: SRACs exported to Banedanmark via the application rules document, [AppRule], relating to infrastructure as specified in Section 4.5 must be fulfilled.*

EVC:

> *#COND-DK-STM-GASC-009#: SRACs exported to the ETCS onboard equipment exported via [AppRule] must be complied with.*

SINTEF considers the conclusion to be acceptable.

3.7 DK-STM maintenance update from version 03.00.10 to version 03.00.11

This section covers the safety assessment related to the DK-STM maintenance update from version 03.00.10 to version 03.00.11.

The update process followed by the manufacturer Siemens is described in QANote_06, ref. [119], and the performed safety analysis related to the one error correction to be done is documented in SafetyNote_18, ref. [120].

The defect is described in the Defect and Change Management System CHAMPFX, where early details of the description also are included in the references QANote_06. The defect was discovered during a "tillysningskørsel" with DK-STM version 03.00.09 installed in the MQ4118 train, where the defect relates to the DK-STM handling of an invalid balise passing. The intermediate conclusion concerning safety performed in QANote_06 is that the defect represents no safety impact but may have minor impact on availability.

The bugfix process to follow is described in the referenced QANote_06, where the DK-STM version 03.00.10 referenced Quality Assurance Plan and System Safety Plan are referenced as guide lines for the update process, and where the V-model according to EN 50128 is to be followed. The in QANote_06 referenced Verification Report, System Validation Report and Generic Application Safety Case for DK-STM version 03.00.10, are considered still to be valid together with the provided DK-STM version 03.00.11 update documentation.

All details concerning the follow-up related to the development process for the correction of the defect is documented in the ClearQuest Record Details, ref. [122], covering the separate parts: Submission, Analysis, CCB handling, Solution, Verification and Validation.

A separate safety analysis SafetyNote_18 has been performed as referenced above, concluding that the defect is not classified to be safety relevant as the brakes will be activated caused by a balise error detection. The proposed error correction requires one line of code to be modified. This, according to the EN 50128:2011 can be considered as a "minor change"[5]. The proposed solution implies that the architecture and the status of requirements remain unchanged, and that application rules and interface towards the EVC are not affected. The SafetyNote_18 concludes, quoted: "*The analysis done for the defects concludes that non-safety related change of the defects constitutes a minor change in the software which speaks for a bugfix under maintenance release of STM version 03.00.11*".

CCB decision concerning the handling of the defect states, quoted: "*It has been decided to remedy this defect with a new version R.03.00.11. No new features – or alteration of features – will be implemented in the R.03.00.11.*". This implies that there are no changes to be made in addition to the one defect correction as described is the scope for the DK-STM version 03.00.11 update.

The "Solution" part of the referenced ClearQuest Record Details describes in detail, both in relation to the source code and the corresponding BAB (generated code file).

The "Verification" part of the referenced ClearQuest Details describes two steps: (i) Retesting with identical environment and train movement as when the error occurred; and (ii) Test with Siemens test system, running on target hardware. Detailed test results are referenced, and both tests where concluded to be as expected and ok, also referenced to be sufficient by the Validator. In addition to the above referenced two tests, both source-code review and a complete Unit Test of the GW part of DK-STM has been performed.

The "Validation" part of the referenced ClearQuest Details includes the Validator's evaluation, including his conclusion, quoted: "*In summary correct implementation and verification of the change was demonstrated*".

SINTEF endorses the referenced documentation of the DK-STM version 03.00.11 update with respect to the assessment of the safety, having no additional comments related to the completeness and correctness of the referenced documentation.

[5] The handling of "minor change" according to EN 50128:2011 has been covered in the DK-STM version 03.00.10 referenced System Safety Plan, ref. section 3.2.2 in the corresponding Safety Assessment Report [121].

3.8 DK-STM maintenance update from version 03.00.11 to version 03.00.12

This section covers the safety assessment related to the DK-STM maintenance update from version 03.00.11 to version 03.00.12.

The update process followed by the manufacturer Siemens is described in QANote_07, ref. [123], and the performed safety analysis related to the one error correction and two change requests to be done are documented in SafetyNote_19, ref. [124].

The defect and change requests are described in the Defect and Change Management System CHAMPFX, where early details of the description also are included in the references QANote_07.

The defect (CFX00491472) was discovered during the test of STM-DK software. The defect is present in all released STM-DK software versions. The defect occurs when two train units are driving from starting station through other stations to an end station the front train unit then ends with a Y term saved. This Y term shall persist through shunting and a Cab close/open operation, but not if the train has been in either modes

- Sleeping (SL), or
- None leading (NL).

The solution is that while in SL or NL it will be simulated that the Cab in the other end is shortly occupied, which means the Y term is deleted.

Also, two change requests (CFX00491464 and CFX00477871) from the customer is planned to be handled in the new maintenance release R.03.00.12. These changes are:

- a modification in the text presented to the driver through the DMI, to display “*ATC: Indtast ATC data*".
- a supervision function of the gap between Vest and Vmax (since in the ETCS system has been discovered to in some case to provide the STM-DK with an unsafe estimated speed), and if exceeding the defined threshold, the STM-DK is to issue a warning for the driver.

The bugfix process to follow is described in the referenced QANote_07, where the DK-STM version 03.00.10 referenced Quality Assurance Plan and System Safety Plan are referenced as guidelines for the update process, and where the V-model according to EN 50128 is to be followed. The in QANote_07 referenced Verification Report, System Validation Report and Generic Application Safety Case for DK-STM version 03.00.10, are considered still to be valid together with the provided DK-STM version 03.00.11 and 03.00.12 update documentation.

All details concerning the follow-up related to the development process for the correction of the defect and the change requests are documented in the ClearQuest Record Details, refs. [126], [127] and [128], covering the separate parts: Submission, Analysis, CCB handling, Solution, Verification and Validation.

A separate safety analysis SafetyNote_19, ref. [124], has been performed as referenced above, stating for the defect that "*In order to correct the 1 defect 100-line codes are changed to the existing 29988, the modification therefore adds 0,033% new line codes to the Gateway software. The change introduces no new requirements and the system architecture remains unchanged and SIL components are unaffected. The change will therefore mainly be done on right side of the v-model with existing change procedures*". For the two changes, it is stated that "*In order to introduce these 2 changes 121-line codes are added to the existing 29988, the modification therefore adds 0,4% new line codes to the Gateway software. The change adds a clarification of requirement to the system and will therefore follows the V-model as defined in the Quality Note. As there is no change in the architecture and the SIL components the integrity of safety is therefore kept intact*". The SafetyNote_19 concludes based on this that "*…the changes of the STM-DK constitutes a minor change in the software which speaks for a maintenance release of STM version 03.00.12. The revealed error has been fixed in the DK-STM 03.00.12 software, which will be released 4th quarter of 2020.*"

The "Solution" part of the referenced ClearQuest Record Details describes in detail the implementation of the solutions.

The "Verification" part of the referenced ClearQuest Details describes the verification process and refers to the verification statement by software integration verifier Mr. Volker Andreas from ESE (ref. [129]): "*…software changes introduced to Release R03.00.12 of the STM-DK Gateway software Change Request Verified by*

- *CFX00491472 DMIButtonStateMachine_083*
- *CFX00491464 TrainDataEntry_003*
- *CFX00477871 Odometer_014, Odometer_015*

received adequate testing. Test results as reported by "Software Integration Test Report Gateway, G81001-X3107-U034-26" the demonstrated correct implementation. Related change requests considered complete".

The "Validation" part of the referenced ClearQuest Details includes the Validator's evaluation, including his conclusion, quoted: "*Verification ok. Validation is documented in G81001-X3107-U547-09 Close defect.*".

SINTEF endorses the referenced documentation of the DK-STM version 03.00.12 update with respect to the assessment of safety, having no additional comments related to the completeness and correctness of the referenced documentation.

The summary and conclusions of the DK-STM version 03.00.12 safety assessment is found in chapter 4.

3.9 DK-STM maintenance update from version 03.00.12 to version 03.00.13

This section covers the safety assessment related to the DK-STM maintenance update from version 03.00.12 to version 03.00.13. Two change requests from the customer are planned to be handled in the new maintenance release R.03.00.13 (CFX00517269 and CFX00517273).

The update process followed by the manufacturer Siemens is described in QANote_08, ref. [130], and the performed safety analysis related to the two change requests to be done are documented in SafetyNote_20, ref. [131].

The defect and change requests are described in the Defect and Change Management System CHAMPFX, where early details of the description also are included in the referenced QANote_08.

Change request CFX00517269; previously Banedanmark had requested a change (CFX00477871 [128]) implemented in the previous STM-DK 03.00.12 release. The change was for STM-DK to monitor the gap between Vest and Vmax. Further description of the change is described in the SafetyNote_19 [124]. However, after some test runs Banedanmark has realized that ETCS would more often provide wrong Vest values due to slip/slide conditions, which affects the operation. Based on the above discovery Banedanmark has together with Alstom made an analysis of the slip/slide data, with the conclusion that STM-DK instead of monitoring the gap between Vest and Vmax should monitor the gap between Vmin and Vmax, while still using Vest. This is in order to filter out wrong alarms due to slip/slide. The hazard workshop also concluded that STM-DK activation of Service Brake after 6 minutes shall be removed as it is the driver's responsibility. The hazard workshop concluded that there are no identified hazards related to this change in the STM-DK.

Change request CFX00517273; related to the DK-STM baseline 2.3, it is experienced activation of emergency brakes in operation with the Vectron locomotive, due to the redundant DMI display Where the permissible reconnection time (1.8s) of the DK-STM in most cases is too short for this switch-over for redundant DMI display, and in such cases the DK-STM will trigger an emergency brake. Based on the analysis from the Vectron locomotives and experience in other projects, the design solution is for the STM-DK to have an increase of the permissible reconnection time to 5 seconds instead of the 1.8 to comply with the redundant DMI setup in the Vectron Locomotives. Based on hazard workshop it was concluded that the change of the reconnection time from 1.8s to 5s has no negative impact on the safe operation of the vehicle as the train is still under control of the STM-DK in these extra 3.2s.

The process to follow is described in the referenced QANote_08, where the DK-STM version 03.00.10 referenced Quality Assurance Plan and System Safety Plan are referenced as guidelines for the update process, and where the V-model according to EN 50128 is to be followed. The in QANote_08 referenced Verification Report, System Validation Report and Generic Application Safety Case for DK-STM version 03.00.10, are considered still to be valid together with the provided DK-STM version 03.00.11, 03.00.12 and 03.00.13 update documentation.

All details concerning the follow-up related to the development process for the correction of the change requests are documented in the ClearQuest Record Details, refs. [133] and [134], covering the separate parts: Submission, Analysis, CCB handling, Solution, Verification and Validation.

A separate safety analysis SafetyNote_20, ref. [131], has been performed as referenced above, stating for the change requests that "*In order to introduce these 2 changes 205-line codes are added to the existing 29988, the modification therefore adds 0,7% new line codes to the Gateway software. The change adds a clarification of requirement to the system and will therefore follows the V-model as defined in the Quality Note. The changes listed in this safety note does not affect the interfaces towards the EVC, why the interface remains unchanged. As there is no change in the architecture and the SIL components the integrity of safety is therefore kept intact.*". The SafetyNote_20 concludes based on this that "*The analysis done for software change and update concludes that the changes of the STM-DK constitute a minor change*[6] *in the software which speaks for a minor maintenance release of STM version 03.00.13. The changes to the DK-STM 03.00.13 software, will be released 2nd quarter of 2021*". Hence also, the Hazard Log is not affected by this maintenance update, based on the conclusion of the safety analysis in the SafetyNote_20, ref. [131].

The "Solution" part of the referenced ClearQuest Record Details describes in detail the implementation of the solutions.

The "Verification" part of the referenced ClearQuest Details provides an overview of verification activities done for STM version 03.00.13.

The "Validation" part of the referenced ClearQuest Details refers to new System Validation Report, updated for STM version 03.00.13 (ref. [135]). The Validation report concludes that " *The system STM-DK fulfils all requirements to meet its intended use. The system STM-DK with software version 03.00.13 is suitable to operation under consideration of the rules and constraints listed in chapter 9 and the requirements listed in "Table 25 List of changed evaluation on inapplicable requirements". The system STM-DK is suitable for the use with ETCS systems of UNISIG Baseline 2 and UNISIG Baseline 3*".

SINTEF endorses the referenced documentation of the DK-STM version 03.00.13 update with respect to the assessment of safety, having no additional comments related to the completeness and correctness of the referenced documentation.

The summary and conclusions of the DK-STM version 03.00.13 safety assessment is found in chapter 4.

[6] The handling of "minor change" according to EN 50128:2011 has been covered in the DK-STM version 03.00.10 referenced System Safety Plan, ref. section 3.2.2 in the corresponding Safety Assessment Report [121].

4 Assessment

The changes concerning the upgrade for DK-STM from v03.00.12 to v03.00.13 have been described in "Update process for maintenance release R.03.00.13" in QANote_08, ref. [130] and in "Analysis for the DK-STM changes, DK-STM 03.00.13" in SafetyNote_20, ref. [131], and the corresponding performed maintenance update process has been documented in the ClearQuest Record Details, refs. [133] and [134].

The safety documentation for the DK-STM Generic Application has been assessed, ref. section 3.9. SINTEF sees nothing that speaks against approving the DK-STM Generic Application version 03.00.13 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application.

4.1 Application Conditions, Reservations and Recommendations

There are no Application Conditions, no Reservations and one Recommendation in the present report. The recommendation is recapitulated below:

5 References

The following documents have been used as the basis for assessment. Unless otherwise stated in the comments, the documents can be regarded as acceptable.

The Safety Case (ref. [1]) uses alphanumeric acronyms rather than numbers for references; in order to facilitate traceability, the acronyms are included (without braces) in the following list above the document name.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
1. GASC	G81001-X3107-U405-08	08.00	2018-09-28	The DK-STM v03.00.10 Generic Application Safety Case, which represents the basis for the assessment carried out in this report. Updates with this version of the Safety Case are identified in chapter 1 of the Safety Case.
2. Prosjekttilbud Assessment for dansk STM	90513001-STMDK	1.0	2007-12-07	This contains a description of the assessment activities to be performed during the project. It is included as an integral part of the contract between Banedanmark and SINTEF and has been accepted by Trafikstyrelsen as an acceptable assessment plan.
Safety Case References				
3. AnwRgl*	See GASC references	-	-	Application rules exported from the TCC platform. These have been covered in chapter 5 of the GASC.
4. ACKNOWL_BANE	ELO Ref: 1583345 & 1584769	-	-	Emails from Banedanmark to Siemens which confirms that the hazards HAZ001, HAZ002 and HAZ003 has been transferred to Banedanmark and closed for the DK-STM hazard log.
5. AppRule, Application Rules	G81001-X3107-L005-09	09	2017-11-10	The document states the rules that must be followed to use the STM-DK application in safety related train installations. The sources for the rules which are covered are specified for each rule, and rules are classified according to type.
6. AppRule_total STM-DK Application Rules, Baseline 3.0	-	-	-	This is a reference to the DOORS module that contains all the application rules and is evidently a file path; the file has not been submitted. SINTEF considers it to be of only informational value and will not assess it.
7. ATCSpec ATC Systemspecifikation	G81001-K3118-U002-*	H	2002-07-31	This is a set of documents that together constitute the specification of the Danish ATC system ZUB 123/LZB-DSB
8. BANE_SRACS	Banedanmark official acknowledgement of approval of all application rules. ELO ref: 1584922			Email from Banedanmark to Siemens which confirms that the application rules as identified in the GASC and its referenced documents are accepted by Banedanmark.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
9. Bane	Fjernbane Onboard Baseline 3 Hazard Record SP-FB-FOB-006263			The document keeps application conditions transferred from DK-STM to Banedanmark as documented in ref. [BANE_SRACS], where the reference includes an extract of relevant information from this reference.
10. BOM_BGR_110V 2v2-subrack, ZUB123-STM, 110V -TCC	S25160-C2001-A127	B	2012-04-13	This is a Bill of Material for the 110 Volt sub-rack.
11. BOM_BGR_24V 2v2-subrack, ZUB123-STM, 24V -TCC	S25160-C2001-A252	B	2012-04-13	This is a Bill of Material for the 24 Volt sub-rack.
12. CandD Concept and Definition	Z123STM/1_CaD	1.3	2008-07-09	This document describes the concept and boundaries for the ZUB123-STM. It is generated from a DOORS database.
13. CE_Declar EC Declaration of Conformity	PM1 A6Z00032036605/B	000	2016-02-17	This is an updated version of the CE declaration created especially for STM -STM including the antenna interface modules Tasse5/Uebgen5. The previous version of the EC Declaration is accompanied by a "statement of Opinion" from the Notified Body EMCCert DR RAŠEK GmbH in accordance with the R&TTE Directive 1999/5/EC. The statement concerns the components TASSE5-sub-assembly S25391-B111-A2 and UEBGENS5-sub-assembly S25391-B112-A2 which according to the GASC 03.00.08 are still applicable.
14. CERT_116	Contract no. SP 16025 STM-DK Certification ART CERT-116	-	-	Siemens agreement with Banedanmark concerning the DK-STM upgrade to version 03.00.09. The detailing of the changes are described in ref. [SafetyNote_14].
15. ClearQuestStatus	-	-	2018-10-02	This is an extract of safety relevant issues in the ClearQuest database. It identifies one item, one with status "*postponed*" (CFX00355544). The "*postponed*" issue is a change request not yet being ordered. The issues have impact on safety. For v03.00.10 the status is reported updated at date 2018-10-02 in the Safety Case, now holding none safety related entities.
16. CmCtrlSheet Configuration Management	G80001-X3107-U513-07	09	2018-10-01	This is a document that identifies versions and baselines of documents and modules for a release of the STM-DK software. The document has been updated to version 09 covering DK-STM v03.00.10.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
17. CmPl Configuration Management Plan	G80001-X3107-U003-03	03	2014-01-20	This is the Configuration Management Plan for the STM-DK certification project. It addresses • CM administration • CM activities • Software, building and releasing • User access rights to CM data • Data backup and archiving • Changing configurations
18. CompList Documentation of Personnel Competence – List of CV's	G81001-X3107-U401-06	06	-	This document is not submitted due to data privacy regulations, but can be made available on request. SINTEF considers this to be acceptable.
19. CppStyleGuide C++ Programming Style Guide	G80001-X3107-R005-01	01	2009-12-08	This is a coding standard for writing C++ code for the STM ZUB123. It states "*The rules and guidelines defined in this document apply to code running on the STM ZUB123 itself. They do not apply to test code and software tools used for development, de-bugging or diagnostics later in the product life cycle.*" It is based on the C++ coding standard for the SIMIS Basis system.
20. CQIntro Introduction to CHAMPfx / ClearQuest	G81001-X3107-U031-01	01	2010-07-01	This is a description of the change management process that is implemented with IBM Rational ClearQuest. It defines the roles and contains step-by-step instructions for each activity.
21. DocList Document List and Document Control	G81001-X3107-L001-08	09	2018-10-01	This is a complete list of documents produced in the project, including their actual version and release status. The document has been updated to version 09 covering DK-STM v03.00.10.
22. EN 50126 Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	EN 50126-1	-	Sep 1999	These are the standards against which the assessment has been performed. They require a structured safety case as a basis for assessment.
23. EN 50129 Railway Applications – Safety Related Electronics Systems for Signalling	EN 50129	-	Feb 2003	
24. EN 50128 Railway Applications – Communications, Signalling and Processing Systems – Software for Railway Control and Protection Systems	EN 50128	-	Mar 2001	Only clause 9.2 Software Maintenance from the 2011 version of EN 50128 is applied; it is equivalent to clause 16 of the 2001 version.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
25.	GASC_Cert_R03.00.01	G81001-X3107-U405-03	03	2014-08-09	Generic Application Safety Case, STM-DK Certification, Release 03.00.01 This is the Generic Application Safety Case for the baseline 3.0 version of the STM with version 03.00.01 of the software. It has been assessed by SINTEF; see ref. [63].
26.	GASC_Cert_sw03.00.05 GASC	G81001-X3107-U405-04	04	2015-03-09	Generic Application Safety Case, STM-DK Certification, Release 03.00.05. This is the Generic Application Safety Case for the baseline 3.0 version of the STM with version 03.00.05 of the software. It has been assessed by SINTEF; see ref. [64].
27.	GASC_Cert_R03.00.07	G81001-X3107-U405-05	05	2015-08-28	Generic Application Safety Case, STM-DK Certification, Release 03.00.07 This is the Generic Application Safety Case for the baseline 3.0 version of the STM with version 03.00.07 of the software. It has been assessed by SINTEF; see ref. [66].
28.	GASC_Cert_R03.00.08	81001-X3107-U405-06	06	2016-06-10	Generic Application Safety Case, STM-DK Certification, Release 03.00.08 This is the Generic Application Safety Case for the baseline 3.0 version of the STM with version 03.00.08 of the software. It has been assessed by SINTEF; see ref. [67].
29.	GASC_Cubicle GASC for the STM cubicle	G81002-E3134-U002-*[7]	-	-	This reference is included because the Safety Case states "*The safety case at hand acts as an input document to the safety case for the STM cubicle …*". This Safety Case is subject to a separate assessment.
30.	Glossary Siemens AG – Glossary	G81001-X3107-L001-01	01	2012-04-13	This is a list of terms with their definitions. For terms coming from subsets of standards the source is identified.
31.	HazLog, Hazard Log STM-DK	G81001-X3107-U008-03	03.01	2012-04-13	The Hazard Log is the operative basis for the on-going safety management. The system safety representative uses the Hazard Log to perform, track and document his tasks. It is also considered as a constituent part of the Safety Case to prove that all necessary activities to identify risks, to reduce risks and to control risk have been applied to the system to be developed. The process for Hazard Log Management is described in chapter 3 of the document.
32.	HazLogRep Report per 2017-11-28 from ClearQuest STM-DK project	-	-	2017-11-28	This is a report of hazards in the ClearQuest database of date 2017-11-28. All hazards are "*Closed*".

[7] *: covers both A and B

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
33. HHGB_RISK_AN Helsingor-Hornbæk-Gilleleje Banen Risk Analysis	G81001-X3107-U569-01.00	01.00	2016-02-10	Risk analysis performed in preparation to the introduction of new ATP train type for DK-STM with customized ATP functionality on ATP infrastructure. A risk evaluation work-shop has been performed, where the outcome identifies a set of hazards and defines proper mitigations.
34. InstMan STM-DK Installation Manual	IN 655.00 Q2962	1.09	2017-08-14	This is the installation manual for installing the STM-DK as an add-on to an ETCS system. It addresses • Decommissioning of ATC ZUB123 • General rules and procedures, specifically referring to application rules • Electric interfaces and diagrams • Configuration of STM-DK • Functional test • Diagnosis
35. IntAudit_01 Siemens Auditrapport	IMO-2010-03	-	2010-06-15	The Internal Audit report (in Danish language) covers aspects as: Review process; inspections; requirement management; planning and reporting; risk handling; and document control. One problem report concerning inspections has been issued. According to the Quality Management Report there are no issues to follow-up.
36. ISO 9001Cert Certificate of approval	CPN00016312	-	2018-09-03	This is a certificate of approval of the management system of Siemens A/S, Ballerup, according to ISO 9001:2015, ISO 14001:2015 and OHSAS 18001:2007. It is valid until 2021-09-02. The certificate has been renewed for DK-STM v03.00.10 maintenance update.
37. KS_Chekliste Quality Checklist	G81001-X3107-L007-01	01.06	2012-04-13	This is a filled-in checklist covering management activities from regular inspections addressing quality assurance, safety management, risk control, resource control, project management and software configuration. However, in the Certification project frequent Core Team meetings have replaced the use of this [KS_Chekliste]. These meetings also include the CCB (Change Control Board) Meeting – where the changes and defects reported in ClearQuest are handled.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
38. MaintMan STM-DK Vedligeholdsmanual	VN 655.00 Q4433	3.01	2017-06-09	This is the maintenance manual for STM-DK. It addresses • Maintenance o including competency of personnel, tools, repair etc. • Diagnosis via LED on circuit boards o For TCC modules and external components • Diagnosis via PC • Appendices o Maintenance form sheet o Error reporting form sheet o Error diagnosing
39. OrgComp Organisation and Documentation of Personnel Competence	G81001-X3107-U404-07	07	2018-09-24	The Organisation and Documentation of Personnel Competence for the STM-DK project. This document documents the competence of everyone participating in the STM-DK certification project, including the mapping of roles in the project with standard roles according to what is required, and shows the project organisation. The document has been updated to version 07, covering updates of roles and organization diagram applicable for DK-STM v03.00.10.
40. Pascal86 Hinweise Programmierung Pascal86 ZUB123/LZB-DSB	A25441-X0020-R007-02-35	02	1995-09-25	This is a coding standard for writing Pascal-86 code. It requires the validated compiler Pascal-86 X311 to be used.
41. QANote_05 Update process for maintenance release R.03.00.10	QANote_05	01	2017-07-17	The document is new for the DK-STM v03.00.10 maintenance update. The document describes the update process to follow. There are four defects (CFX00393997, CFX00393988, CFX00393972 and CFX00396034) which have been discovered during testing with DK-STM v03.00.09 which shall be corrected. The document states the "safety relevant assessment is set to "no"" and the impact on availability is considered to be "minor", caused by possible unintended emergency break to occur. No new features or alteration of features shall be implemented.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
42. QaPl Quality Assurance Plan	G81001-X3107-U400-03	03	2017-06-20	Quoted from section 1.5: "*This quality assurance plan ...:* - *Applies to all activities within the framework of the project's quality assurance that are to be carried out at the system | hardware level and at the software level during the certification.* - *Is valid for all staff members and organisational units participating in the project.* - *Is valid for the whole duration of the project* *This document is intended to ensure the definite scheduling of those measures, methods, tools, responsibilities, supplier QA measures, verifications and resources required for the compliance with the normative requirements for quality assurance in the project.*" The plan covers specifically: Process, methods and tools; Q objectives and Q metrics; Verification activities; Assessments of previous validation tests; and Non development activities in the certification project.
43. QHSE-HB Kvalitet, Miljø og Arbejdsmiljø – Siemens A/S	-	-	2013-08-13	This is a printout from the intranet based quality, health and safety handbook at Siemens A/S. The individual components date from May 1999 to March 2015
44. Risk-an ZUB123-STM Risk analyses	G81001-V3118-U014-B	B	2008-07-08	This is the risk analysis from phase 3 (Risk Analysis) according to the CENELEC lifecycle. It contains a system overview and fault tree analyses and FMECAs and addresses amongst other things RAM and safety requirements (derived from FMECA), hazard identification and classification.
45. RMPlan RM-Plan Guide	A6Z00002541903	D	2013-12-27	This is a DOORS report that contains the requirement management guideline. It addresses • Work Products of Requirements Management • Traceability • Test and Validation of Requirements • Structures in DOORS • Corresponding Topics
46. SafeRew_01 Safety review STM-DK development	MOL-PE	-	2011-11-10	This is the minutes of an internal safety review consisting of walk throughs of a risk analysis, the Hazard Log and an analysis of the DMI interface. It is only intended for internal use and can be regarded as evidence that reviews have been performed.
47. SafetyNote_01 THR for the STM-DK	SafetyNote_01	01.00	2011-10-01	This documents fulfilment of the requirement that the hazard rate shall be less than $10^{-8}h^{-1}$.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
48. SafetyNote_02 Safety analysis concerning the DMI	SafetyNote_02	01	2012-07-09	This documents "*compliance with safety requirements for STM-DK operation using EVC-DMI*".
49. SafetyNote_03 SERIO5 remanent memory CRC polynomial	SafetyNote_03	01.00	2012-06-01	This verifies that the chosen generator polynomial is sufficient to detect random changes in the safety relevant data.
50. SafetyNote_04 CRC polynomial SSL and STL	SafetyNote_04	01.00	2012-06-15	This documents fulfilment of requirements for the CRC polynomial in the Safe Link Layer (SLL) and the Safe Time Layer (STL, which depends on the SSL).
51. SafetyNote_05 Safety of STM-DK for speed up to 210 km/h	SafetyNote_05	01.00	2012-06-01	This demonstrates that "*the safety of the train is not jeopardized at 210 km/h*".
52. SafetyNote_07 Review of Safety Requirements' traceability	SafetyNote_07	05	2016-05-23	Purpose of document is to report on a traceability study of Safety Requirements carried out by the Safety Manager in March-May 2016 as part of the development process for the new software version 03.00.08. The traceability work is documented in an excel sheet embedded in the document.
53. SafetyNote_08 TASSE5/UEBGEN test interval	SafetyNote_08	01	2013-11-21	This document provides justification for the choice of 48 hours as interval for the TASSE5/UEBGEN test procedures.
54. SafetyNote_10 Note on TIU timeout specifications	SafetyNote_10	02	2016-06-06	Safety note outlines the risks related to delay of signals communicated via the TIU connection between the Alstom EVC and STM-STM. The corresponding hazard is deemed highly improbable.
55. SafetyNote_12 Development process for STM-DK version 03.00.08	SafetyNote_12	05	2016-04-15	Safety note describes the development work to be done at Siemens and the implications for the approval and certification process in the update of the STM-DK software version 03.00.07 to version 03.00.08. The actual functional changes in version 03.00.08 are identified.
56. SafetyNote_14 Development process for DK-STM version 03.00.09	SafetyNote_14	-	2017-05-29	Purpose of this safety note is to describe the development work related to updating the current version of STM-DK software version 03.00.08 to the new version 03.00.09 to be done at Siemens and the implications for the approval and certification process.
57. SafetyNote_17 Analysis for the DK-STM defects, DK-STM R.03.00.10	SafetyNote_17	01	2018-09-20	The document is new for the DK-STM v03.00.10 maintenance update. It describes and analyses the safety consequences of the four defects to be corrected with the DK-STM v03.00.10. None of the defects have been classified to be safety relevant, and consequences for correction implementation imply no change of system architecture, requirements and application conditions, and only a minor change of the software.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
58. SINTEF_01 Safety Management Audit of Siemens AS Ballerup 5th October 2010	SINTEF F16778	1.0	2010-10-13	The Safety Audit performed by SINTEF focused on safety aspects according to CENELEC EN 50126 and EN 50128. No nonconformities and one recommendation concerning the Quality Assurance Plan were issued. The plan was updated to version 03 with respect to the audit recommendation. In the mean-time it is issued as version 04.01 (see ref. [42]).
59. SINTEF_02 Comments on STM-DK "System Safety Plan"	90C26703-NOT-2009-01	5.0	2010-05-31	This is SINTEF's evaluation of the Safety Plan for the STM-DK development project. It concludes "*The submitted safety plan fulfils the applicable requirements for a safety plan ... the documents can be considered acceptable.*"
60. SINTEF_03 Comments on STM-DK "Software Validation and Verification Plan"	90C26703-NOT-2010-01	1.1	2011-05-03	This is SINTEF's evaluation of the software V&V plan. It concludes "*The software validation and verification plan alone does not fulfil all the requirements as defined in EN 50128. ... The System and Software Quality Assurance Plan ... has also been assessed and is considered to be acceptable with respect to fulfilment of the requirements of EN 50128. ... the Software Validation and Verification Plan can therefore be approved.*"
61. SINTEF_04 Quality Management Audit of Siemens AS, Ballerup 6th September 2011	SINTEF F20834	1.0	2011-11-04	The Quality Management Audit performed by SINTEF focused on quality management requirements according to the certification of the STM-DK as a CCS constituent according to the EU Interoperability Directive on railway. No nonconformities or recommendations were issued. It must however be noted that only requirements considered to be relevant for the STM-DK prototype project were covered.
62. SINTEF_08 Safety Assessment Report STM-DK Generic Application Safety Case with supplements	SINTEF F26198	4.1	2014-06-30	This is the assessment of the Generic Application Safety Case after information closing reservations in the previous report (ref. [118]) had been submitted and dynamic testing had been performed. It concludes "*SINTEF sees nothing that speaks against approving use of the STM-DK generic application as a basis for specific applications that are not intended for commercial traffic, provided the reservations in the safety case are satisfactorily closed and the application conditions from the STM-DK generic application safety case and this assessment report are fulfilled by the specific application.*"

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
63. SINTEF_09 Safety Assessment Report STM_DK Generic Application (Baseline 3.0)	SINTEF F26393	5.0	2014-10-14	This is the initial issue of the report at hand, valid for SW version 03.00.01. It concluded "*The safety documentation for the STM-DK generic application is evidently not yet completed so that a final recommendation concerning approval to use the STM-DK generic application as a basis for specific applications cannot yet be given. The final documentation will have to close the reservations in the safety case and this assessment report satisfactorily, and the application conditions from the STM-DK generic application safety case and this assessment report must be fulfilled by the specific application.*"
64. SINTEF_10 Safety Assessment Report STM_DK Generic Application (Baseline 3.0)	SINTEF F26393	5.1	2015-06-25	This is a previous issue of the report at hand, being SINTEF's assessment of the STM-DK Generic Application SW version 03.00.05. It concluded "*The safety documentation for the STM-DK generic application has been assessed. SINTEF sees nothing that speaks against approving that the STM-DK generic application for use in specific applications provided the reservations in this report are closed and the application conditions in the safety case are fulfilled by the specific application.*" There were two reservations: "*Reservation 1: The Delta System Validation report shall be submitted for assessment and approved.* *Reservation 2: Evidence shall be provided that the software integration tests have all been passed before the GASC can be approved.*"
65. SINTEF_11 Quality Management Audit of Siemens AS, Ballerup 11th May 2015	SINTEF F26956	1.1	2015-06-15	This is an audit report that concludes: "*There is one nonconformity with the requirements of Commission Decision 2010/713/EU ... which SINTEF expects will be closed in the course of normal work as a prerequisite for issuing a Quality Management System Approval.*"
66. SINTEF_12 STM-DK Generic Application (Baseline 3.0) version 03.00.07	SINTEF F27264	1.0	2015-10-30	This is the SINTEF's assessment of the STM-DK Generic Application SW version 03.00.07.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
67. SINTEF_13 Safety Assessment Report for the STM-DK Generic Application (Baseline 3.0) Version 03.00.08	SINTEF F27264	2.0	2016-07-06	This is the SINTEF's assessment of the STM-DK Generic Application SW version 03.00.08. It concluded. "*The safety documentation for the STM-DK Generic Application has been assessed. SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.00.08 for use in specific applications with the reservations given in the Safety Case and this report and provided the application conditions in the Safety Case are fulfilled by the specific application.*" *There were two reservations:* *"Reservation 1. The SRACs as identified by the Generic Application Safety Case (ref. [1]) and its referenced documents must be formally accepted by BDK* *Reservation 2. If any SRACs as identified by the Generic Application Safety Case (ref. [1]) and its referenced documents are reworded, reclassified or redistributed the Safety Case shall be updated accordingly and submitted for reassessment.*". A separate safety assessment, concerning SQT testing, was done after the assessment of v03.00.08 of DK-STM. That assessment was reported in version 3.0 of this document.
68. SINTEF_14 Quality Management System Approval Report – DK-STM Interoperability Constituent, Baseline 3.0	SINTEF 2017:00568	1.0	2017-11-02	Covers the required QMS surveillance related to the certification of DK-STM versions 03.00.08 and 03.00.09 according to the Interoperability directive 2008/57/EC.
69. SINTEF_15 Safety Assessment Report for the STM-DK Generic Application (Baseline 3 Release 2) version 03.00.09	SINTEF 2017:00826	4.0	2017-12-19	The SINTEF Safety Assessment Report for DK-STM v03.00.09, covering the DK-STM update to comply with the Baseline 3 Release 2.
70. SRS BDK_SRS30 SRS ZUB123-STM issue 18 (baseline 16)	G81001-X3107-R243-18 Released	18 (base-line 16)	2017-05-10	This is a DOORS report that represents the Customer's System Requirement Specification for the STM-DK. Each requirement is uniquely identified by its SRS30_xxxx identifier, including a classification and approval status. Requirements are logically grouped.
71. SRSClar System Requirements Clarification	SyReqClarification	13 (base-line 14.0)	2017-06-07	This is a DOORS report that contains clarifications to the requirements in ref. [70]. It is to be regarded as a supplement to ref. [70].

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
72. SwArchSpecGw Software Architecture Specification Gateway	G81001-X3107-U024-12	12 (base-line 11.0)	2017-10-04	This is a DOORS report that contains the software architecture specification for the software component "Gateway".
73. SwArchSpecZUB Software Architecture Specification ZUB123	SwArchZUB	05	2014-12-04	This is a DOORS report that contains the software architecture specification for the software component "ZUB123".
74. SwAssRep Inspection report of safety assessment	A6Z00035256415	B	2014-08-07	This is a report from the assessment of the software validation report (ref. [86]) for normative correctness and usability. It states "*This assessment does neither evaluate the software development process nor the product software as an object of the software validation report. The fulfilment of [SUBSET 035 V2.1.1] and [SUBSET 035 V3.0.0] is no topic of this assessment.*"
75. SwBuildGuide STM-DK Building and Compiling Procedure	G81001-X3107-U517-01	01	2013-12-17	This document describes the processes to build and compile the ZUB123 components, make the gateway component and build the STM-DK product.
76. SwHwIntTstPl SW/HW Integration test specification	G81001-X3107-U032-07	07	2015-05-19	This is a DOORS report that contains the specification of the SW/HW integration tests to be performed. It is noted that it has been clarified by Siemens that the valid version shall be version 6 baseline 9, not version 7 baseline 10 as stated in the GASC version 07.
77. SwHWIntTstRep Software hardware Integration Test Report for ver. 03.00.06	G81001-X3107-U515-09	09	2015-05-29	This is the report from the validation activities according to the Software Verification and Validation Plan (ref. [87]). All tests were passed.
78. SWInstGuide Software installation guide DK_STM	G81001-X3107-U406-03	03	2015-02-24	This document describes how to install and configure the STM-DK software on its target hardware.
79. SwIntTstRepGw Software Integration Test Report Gateway	G81001-X3107-U034-25	25	2018-09-03	The document has been updated to version 25 for DK-STM v03.00.10 maintenance update, covering the addressed defect CFX00393997. This is the report from the validation activities according to the Software Verification and Validation Plan (ref. [87]). 15 requirements could not be proved by tests in the scope of the software verification. In addition, there are a number of issues listed in sections 3.1.1 and 3.1.3. Most of these are attributed to the test environment. All issues are appropriately discussed in the delta System Validation Report for 03.00.10 (ref. [99]).

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
80. SwIntTestRepZub Software Integration Test Report ZUB123	G81001-X3107-U035-13	13	2018-09-07	The document has been updated to version 13 for DK-STM v03.00.10 maintenance update, covering the addressed defects CFX00396034, CFX00393972 and CFX00393988. This is the report from the validation activities according to the Software Verification and Validation Plan (ref. [87]). All tests are passed.
81. SwIntTstSpecGw	-	-	-	A selection of UML test models referred in [SWIntTstRepGw] (ref. [79]).
82. SwIntTestSpecZub Software Integration Test Specification ZUB123	SwIntTestSpecZub	05	2015-02-25	This is a DOORS report that defines the tests to be performed for integration of the ZUB123 software.
83. SwMethods SW development, Techniques and measures acc. To EN 50128	G81001-X3107-L004-01	01	2010-12-20	This identifies and justifies the techniques and methods from EN 50128:2001 Annex A that were used in the development project.
84. SwModChkL Checklist for Software Module Review	G81001-X3107-U033-03	03	2015-02-27	This is a checklist to be used when reviewing software module documents: • Design specification • Test specification • C++ source code • Test C++ source code • Pascal86 source code • Test Pascal86 source code
85. SwRelNote STM-DK Software Release Notes	G81001-X3107-L006-25	25	2018-08-01	The document uniquely defines specific versions of the STM-DK, this by uniquely associating a specific version to both software (using a diagnosis tool) and documentation (by using ClearCase) to a specified version identifier. It is valid for the development project and identifies R03.00.10 as the latest version. It states that R03.00.09 is the "*Latest validated version*". The document has been updated to version 25 covering DK-STM v03.00.10 maintenance update.
86. SwValRep Software Validation Report	G81001-X3107-U036-05	05	2014-07-25	SINTEF notes that the report has been prepared and approved by the same person and that the change log identifies the document's date as 2014-06-30 whilst the cover sheet states 2014-07-25. A total of 12 rules and 6 constraints are defined in Section 10 and the conclusion is "*The overall result of the software validation is: the developed software is under consideration of rules and constrains from Section 10 ready to use.*"

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
87. SwVerValPl Software Verification and Validation Plan	G81001-X3107-U019-02	02.01	2011-08-15	The Software Verification and Validation Plan for the STM-DK project. The document describes the planning of software verification and software validation. The planned verification activities are limited to testing and analysis. All necessary verification activities concerning the documents with reference to tables of EN 50128 are described in the Quality Assurance Plan (ref. [42]).
88. SyArchSpec System Architecture Specification	G81001-X3107-R0004-19	19 (baseline 16.0)	2017-09-04	This is a DOORS report that describes the system architecture of the ZUB123-STM. It also contains the software requirement specifications for the software components Gateway and ZUB123. The document represents a basis for mapping the SRS Clarification (ref. [71]) to the composition of architectural components which the STM-DK consists of.
89. SyIntTstRep System Integration Test Report	G81001-X3107-U012-14	14	2018-09-11	The document has been updated to version 14 covering DK-STM v03.00.10 maintenance update, showing updated test results in chapter 3. SINTEF has verified that no new test result issues has been added with the DK-STM v03.00.10 maintenance update. This is the System Integration Test Report for STM-DK version 03.00.10. A number of tests failed or could not be performed. The corresponding requirements are all appropriately accounted for in the delta validation report SyValRep-Delta_310, ref. [99].
90. SyIntTstSpec System Integration Test Specification	G81001-X3107-U026-11	11 (baseline 16.0)	2017-11-21	This is a DOORS report that specifies the integration tests to be performed.
91. SyRamPl System RAM Plan	G81001-X3107-U006-01	01.02	2012-04-16	The purpose is to specify the activities in the development project so that the requirements is a DOORS report that is concerning reliability, availability and maintainability (RAM) can be fulfilled efficiently in the fundamental documentation. The RAM plan describes the process for fulfilling the requested RAM requirements, specifically: RAM Management; RAM Requirements and RAM Activities. RAM Requirements are referenced from the SRS Clarification (SRSClar, ref. [71]).
92. SyReqTstSpec System Requirement Test Specification	G81001-X3107-U535-7.0	7.0	2016-05-31	This is a DOORS report that specifies the tests to be performed to demonstrate fulfilment of the requirements in the SRS Clarification (ref. [71]). It has been stated by Siemens that the valid document is G81001-X3107-U535-07

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
93. SySafePl System Safety Plan	G81001-X3107-U402-03.00	03.00	2017-10-18	This is the System Safety Plan for the certification project. It defines the process for finalisation of the development project for baseline 3/UNISIG baseline 3.6 to be used in trains equipped with Alstom ETCS. The plan fulfils the applicable requirements for a Safety Plan as stated in EN 50126 and EN 50129. It refers to clause 9.2 (maintenance) of EN 50128:2011 as being applicable to the updates to the software. SINTEF considers the Safety Plan to be acceptable.
94. SysDescr STM-DK System Description	KN 655.00 Q2959	2.00	2014-11-19	The System Description for the STM-DK. The document is written in Danish language and specifically covers the aspects: General Design (including architecture, interfaces and hardware composition); STM-DK's main functions; Safety (covering both hardware and software aspects); System notifications; and List of physical components.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
95. SyValRep System Validation Report	G81001-X3107-U010-03	03	2014-08-08	SINTEF notes that the report has been prepared and approved by the same person. The main purpose with the validation in relation to the Safety Case is specifically to ensure the correct configuration of the STM-DK, and to demonstrate the fulfilment of the System Requirements, see the Technical Safety Report. The validated system consists of three main parts: The new component Gateway SW, the approved legacy ZUB123 SW and a number of already developed and assessed hardware and software components. Since the changes between the baseline 2.3.0d and baseline 3.0 versions of the system only affect the software, the other components are not revalidated. The focused aspects of the validation are: - The system changes due to adapting to baseline 3.0 - Integration of the new software components SLL and STL - Tracing of functionality changes from the SRS to the software It is claimed that fulfilment of the requirements from the SRS Clarification (ref. [71]) implies compatibility with the Unisig subsets 35, 56, 57, 58 and 59 for both baseline 2.3.0d and 3.0: "*The definition of the used baseline is done at start-up by evaluating the content of the telegram STM-2. The switching is non-reversible in normal operation and can only be reversed by a technician from Siemens.*" The results from validation are summarised in chapter 11 with the following conclusion: "*The system STM-DK fulfils all requirements to meet its intended use. The system STM-DK is suitable to operation under consideration of the rules and constraints listed in section 9 and the requirements listed in "Table 6 List of inapplicable requirements*".

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
96. SyValRep-Delta_307 Delta System Validation Report	G81001-X3107-U547-05	05	2015-08-24	This document reports supplementary validation activities for the software versions 03.00.05, 03.00.06 and 03.00.07. The validation steps are identified as: 1. Adaption of system test specification and analysis module 2. Check of all reported software changes 3. Test evaluation from software integration test reports 4. Analysis of the verification process 5. Test result evaluation from system integration test 6. Test result evaluation from system validation 7. Error recovery All changes were documented in the release note for the relevant version. The report concludes "*The system STM-DK fulfils all requirements to meet its intended use. The system STM-DK with software version 03.00.07 is suitable to operation under consideration of the rules and constraints listed in chapter 9 …*". Chapter 9 identifies 4 new rules and 4 new constraints, 2 modified rules, 1 deleted rule and 6 deleted constraints with respect to the System Validation Report (SyValRep, (ref. [95]).
97. SyValRep-Delta_308 Delta System Validation Report	G81001-X3107-U547-06	6	2016-06-09	This version of the delta validation report contains the validation activities for the software versions 03.00.05, 03.00.06, 03.00.07 and 03.00.08. Validation conclusion: "*The system STM-DK fulfils all requirements to meet its intended use. The system STM-DK with software version 03.00.08 is suitable to operation under consideration of the rules and constraints listed in ...*". The document identifies 3 new rules and 3 new constraints, 2 modified rules, 4 deleted rules and 5 deleted constraints with respect to the System Validation Report (SyValRep, ref. [95]).

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
98. SyValRep_Delta_309 Delta System Validation Report	G81001-X3107-U547-07	07	2017-11-29	This version of the delta validation report contains the validation activities for the software versions 03.00.05, 03.00.06, 03.00.07, 03.00.08 and 03.00.09. Validation conclusion: "*The system STM-DK fulfils all requirements to meet its intended use. The system STM-DK with software version 03.00.09 is suitable to operation under consideration of the rules and constraints listed in chapter 9 and the requirements listed in ...*". The document identifies none rules and 3 constraints, 2 modified rules, 7 deleted rules and none deleted constraints with respect to the System Validation Report (SyValRep, ref. [95]).
99. SyValRep_Delta_310 Delta System Validation Report	G81001-X3107-U547-08	08	2018-09-24	This is an updated document covering DK-STM v03.00.10, covering addressed defects as identified in section 3.6 of the document, and with SW update as identified in section 6.1 of the document. It is stated and has been verified that there are no rule changes for this version. This version of the delta validation report contains the validation activities for the software versions 03.00.05, 03.00.06, 03.00.07, 03.00.08, 03.00.09 and 03.00.10. Validation conclusion: " *The system STM-DK fulfils all requirements to meet its intended use. The system STM-DK with software version 03.00.10 is suitable to operation under consideration of the rules and constraints listed in chapter 9 and the requirements listed in "Table 19 List of changed evaluation on inapplicable requirements"*. The document identifies no new rules and 3 constraints, 2 modified rules, 7 deleted rules and no deleted constraints with respect to the System Validation Report (SyValRep, ref. [95]).
100. SyVerValPl System Verification and Validation Plan	G81001-X3107-U004-01.01	01.01	2010-04-08	The System Verification and Validation Plan for the STM-DK project. System validation and system verification are activities which take place on the system level of the project. The plan describes the actions in terms of validation and verification on system level, specifically covering: Assumptions; system validation; system verification; and system integration.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
101. TstPrg STM-DK Test Programme	G81001-X3107-U005-02	02	2010-10-29	The document gives an overview of the test activities that will be carried out in the STM-DK development project. The types of testing defined are: Software module tests; Software integration tests; Software / hardware integration tests; and Software requirement test (validation); System Integration tests; System requirement test (validation); Factory acceptance test (FAT); UNISIG compliance test (UCAT); and Product acceptance test (PAT).
102. UserMan STM-DK Brugermanual	SN 655.00 Q2960	10.00	2017-11-20	This is a user manual that describes how to operate STM-DK from an arbitrary ETCS DMI.
103. VerRep_03.00.09 Verification Report R 03.00.09 STM-DK Cert	G81001-X3107-U543-05	05	2017-12-01	This is a report on verification of documents that were compiled in the current phase of the project. It states that the system integration tests have been performed successfully with reference to ref. [89] and concludes "*It can be concluded, that the process leading to the released software R 03.00.09.00 has been in accordance with the [PEACC] process and therefore also in acc. To [EN 50128] concerning review, test and verification activities*".
104. VerRep_03.00.10 Verification Report R 03.00.10 STM-DK Cert	G81001-X3107-U543-06	06	2018-09-21	This is an updated document covering DK-STM v03.00.10. This is a report on verification of documents that were compiled in the current phase of the project. It states that the system integration tests have been performed successfully with reference to ref. [89] and concludes "*It can be concluded, that the process leading to the released software R 03.00.10.00 has been in accordance with the [PEACC] process and therefore also in acc. To [EN 50128] concerning review, test and verification activities*".
105. ZUB_COSNO_Des Design Specification for COSNO Task scheduler STMDK	G81001-X3107-R231-02	02	2014-12-10	This is a DOORS report that documents the design of the COSNO software modules in the STM-DK.
106. ZUb_IFtask_Des Design Specification for Interface Task STMDK	G81001-X3107-R232-05	05	2014-12-10	This is a DOORS report which "*describes the design of the InterfaceTask, which is part of the STMDK, and which is specified in the architecture for the software component "ZUB123" within the STM ZUB123*"

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
107. ZUB_COSNO_TstSpec Module Test Specification/ Protocol for the module COSNO	G81001-X3107-U231-02	02	2015-08-26	This is a DOORS report that specifies the tests to be performed for the COSNO module. The date is the printing date of the document; the date it was produced is not identified.
108. ZUBModDes Porting of ZUB123/LZB DSB to STM	G81001-X3107-U028-E	E	2009-12-15	"*This is a description of how the ZUB123/LZB DSB system software can be ported to a ZUB123/LZB DSB STM system where major functionalities are handled by the ETCS system, and the processing of ZUB123/LZB DSB balise and loop data are managed by the ZUB123/LZB DSB STM.*"
109. ZUBTrafProcDes Design Specification for the Traffical Process Tasks STMDK	G81001-X3107-R233-06	06	2016-06-27	This is a DOORS report which "*contains the design of Traffical process of ZUB123 STMDK, as specified by the architecture for the software component "ZUB123" within the STM ZUB123.*"
110. ZUBTrafProcTstSpec Traffical Process Test Specification	G81001-X3107-U233-11	11	2018-10-01	This is a DOORS report which "*describes the test of software modules contained in the package STMDK...*" The document has been updated to version 11 covering DK-STM v03.00.10 maintenance release. The update is described in ID TestSpecTrafProc-348, referring to affected defects for ZUB123.
111. ZUBTstSuiteAn Analysis of ZUB 123 Test Suite	G81001-X3107-U018-01	01	2010-09-27	This document describes the conversion of ZUB 123 interfaces to STM-DK interfaces. It contains detailed instructions for all telegrams and interfaces.
112. ZUBTstSuiteConv Converting of ZUB 123 Test Suite	G81001-X3107-U029-05	05	2014-09-09	This document describes how to convert the scripts ("*KOM-files*") from the ZUB 123 test suite to interface with the STM-DK.
113. Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009	(EU) 402/2013	-	2013-04-30	Regulation implementing the Common Safety Method (CSM) to be used as (part of) safety assessments.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
114. Commission Implementing Regulation (EU) 2015/1136 of 13 July 2015 amending Implementing Regulation (EU) No 402/2013 on the common safety method for risk evaluation and assessment	(EU) 2015/1136	-	2015-07-13	Amendment to the CSM regulation (EU) No 402/2013 above.
115. MoM, Fjernbane Onboard Safety meeting with the NSA, date 08.07.2016	-	-	2016-07-20	One issue for the meeting (ch.3) concerns the agreement, planning, performance and documentation of the Safety Qualification Test.
116. MR tra–n - DK-STM ver. 3–0 - Report for Safety Quality Test (SQT)	-	01.00	2017-01-12	The document describes the Safety Qualification Test performed with DK-STM baseline 3.0. Earlier Experience Gathering Operation (EGO) has been performed with DK-STM baseline 2.3.0d on different lines than the baseline 3.0 testing. The extent and duration of the Safety Qualification Tests have been agreed between the railway authority Banedanmark and the Danish safety authority Trafikstyrelsen. The testing has been performed with trainset MR-4021 with DK-STM version 03.00.07 installed. The summary from testing reports 8 days of driving, where the MR 4021 travelled 2420 km in 41 hours and parsing more than 1848 balises and where 1728 balises where different from each other. During testing, 4 ATC errors were detected. Each error is analysed and concluded on separately in detail in the document. Based on this SINTEF considers that none of them have any safety implications. The conclusion from the testing was that the DK-STM in Baseline 3 is just as reliable as in baseline 2.3.0d and does not generate more errors than the present ZUB 123 ATC mobile installation. SINTEF comments that the basis for testing, test specification, test performance and documentation of the results are comprehensive and precise and considered fully acceptable. It is however noted that the testing has been done with version 03.00.07 of the DK-S–M - not the latest version 03.00.08 which was covered in version 2.0 of this assessment report and still valid also for version 3.0.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
				The test specification and filled-in test protocol are included being a part of the document. Unexpected events (no.–1 - 8, were 4 are classified as ATC errors, registered in time period 10.10.20–6 - 27.10.2016), being used as input to the document, are documented separately using the template "SQT Registrering af uventede hændelser". Approval of testing is documented separately in the filled-in template "Driftsscenarier for kørsel med MR-togsæt til SQT".
117. SafetyNote_09 Analysis of assessor comments on GASC	SafetyNote_09	01	2014-05-28	This document contains Siemens responses to the reservations and application condition given in the safety assessment report for the baseline 2.3.0d GASC (ref. [118]).
118. SINTEF_06 Safety Assessment Report STM-DK Generic Application	SINTEF F25994	3.1	2014-03-13	This is the assessment of the baseline 2.3.0d version of the STM-DK Generic Application (ref. [26]). It concludes "*SINTEF sees nothing that speaks against approving use of the STM-DK generic application as a basis for specific applications, provided the reservations in the safety case and this assessment report are satisfactorily closed and the application conditions from the STM-DK generic application safety case and this assessment report are fulfilled by the specific application.*"
				Added references related to the DK-STM version 03.00.11 maintenance release update
119. Update process for bugfix release R.03.00.11	QANote_06	01	2019-01-22	The document is new for the DK-STM v03.00.11 maintenance update. The document describes the update process to follow. There is one defect (CFX00414575) which have been discovered during testing with DK-STM v03.00.09 which shall be corrected. The document states the "safety relevant assessment is set to "no"" and that the impact on availability will probably be set to "minor". No new features or alteration of features shall be implemented. The DK-STM version 03.00.11 update process will follow the "CHAMPFX – Process flow", which includes separate Submission, Analysis, Solution, Verification and Validation documentation parts.

Ref. Safety case ref. Document Name	**Document Id.**	**Ver.**	**Date**	**Comment**
120. Analysis for the DK-STM defects, DK-STM 03.00.11	SafetyNote_18	02	2019-02-06	The document is new for the DK-STM v03.00.11 maintenance update. It describes and analyses the safety consequences of the one defect to be corrected with the DK-STM v03.00.11. The defects have been classified not to be safety relevant, and consequences for correction implementation imply no change of system architecture, requirements and application conditions, and only a minor change of the software.
121. Safety Assessment Report – DK-STM Generic Application (Baseline 3.0) version 03.00.10	2017:00826	5.0	2018-10-18	This is the Safety Assessment Report covering DK-STM version 03.00.10
122. CFXRequest CFX00414575 – ClearQuest Record Details	CFX00414575	-	2019-02-11	ClearQuest Record Details related to CFX00414575. The document, including its document references, represents complete documentation for the DK-STM version 03.00.11 update. The documented process includes six parts: Main, Analysis, CCB, Solution, Verification and Validation. SINTEF evaluates the content of the referenced version of date 2019-02-11 to be complete.
				Added new references related to the DK-STM version 03.00.12 maintenance release update
123. Update process for maintenance release R.03.00.12	QANote_07 ELO1874024	01	2020-09-11	The document is new for the DK-STM v03.00.12 maintenance update. The document describes the update process to follow. There is one defect (CFX00491472) which have been discovered during testing which shall be corrected. Also, two change requests from the customer is planned to be handled in the new maintenance release R.03.00.12 (CFX00491464 and CFX00477871). The document refers to the safety note (ref. [124]) regarding safety and severity. No new features – or alteration of features – will be implemented in R.03.00.12 because of the defect. The DK-STM version 03.00.12 update process will follow the "CHAMPFX – Process flow", which includes separate Submission, Analysis, Solution, Verification and Validation documentation parts.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
124. Analysis for the DK-STM defects, DK-STM 03.00.12	SafetyNote_19	02	2020-10-07	The document is new for the DK-STM v03.00.12 maintenance update. It describes and analyses the safety consequences of the one defect to be corrected and two changes to the DK-STM v03.00.12. The analysis done for software change and update concludes that the changes of the STM-DK constitutes a minor change in the software which speaks for a maintenance release of STM version 03.00.12. The revealed error has been fixed in the DK-STM 03.00.12 software, which will be released 4th quarter of 2020.
125. Safety Assessment Report – DK-STM Generic Application (Baseline 3.0) version 03.00.11	2017:00826	6.0	2019-02-19	This is the Safety Assessment Report covering DK-STM version 03.00.11
126. CFXRequest CFX00491472 – ClearQuest Record Details	CFX00491472	-	2020-11-17	ClearQuest Record Details related to CFX00491472. The document, including its document references, represents complete documentation for the DK-STM version 03.00.12 update. The documented process includes six parts: Main, Analysis, CCB, Solution, Verification and Validation. Stated to have safety relevance, and severity is stated to be no functional impact. SINTEF evaluates the content of the referenced version of date 2020-11-17 to be complete.
127. CFXRequest CFX00491464 – ClearQuest Record Details	CFX00491464	-	2020-11-17	ClearQuest Record Details related to CFX00491464. The document, including its document references, represents complete documentation for the DK-STM version 03.00.12 update. The documented process includes six parts: Main, Analysis, CCB, Solution, Verification and Validation. Stated not to have safety relevance, and severity is stated to be no functional impact. SINTEF evaluates the content of the referenced version of date 2020-11-17 to be complete.
128. CFXRequest CFX00477871 – ClearQuest Record Details	CFX00477871	-	2020-11-19	ClearQuest Record Details related to CFX00477871. The document, including its document references, represents complete documentation for the DK-STM version 03.00.12 update. The documented process includes six parts: Main, Analysis, CCB, Solution, Verification and Validation. Stated to have safety relevance, and severity is stated to be minor impact on availability. SINTEF evaluates the content of the referenced version of date 2020-11-19 to be complete.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
129. Verification statement from software integration verifier Volker Andreas	Email from ESE (Andreas Volker) to Siemens (Steen Noergaard and Bjarne Ravnskjaer)	-	2020-11-06	Verification statement from software integration verifier Mr. Volker Andreas from ESE regarding CFX00491472, CFX00491464 and CFX00477871. The statement reads: "*…software changes introduced to Release R03.00.12 of the STM-DK Gateway software* *Change Request Verified by* - *CFX00491472 DMIButtonStateMachine_083* - *CFX00491464 TrainDataEntry_003* - *CFX00477871 Odometer_014, Odometer_015* *received adequate testing.* *Test results as reported by "Software Integration Test Report Gateway, G81001-X3107-U034-26" the demonstrated* *correct implementation.* *Related change requests considered complete.*"
				Added new references related to the DK-STM version 03.00.13 minor maintenance release update
130. Update process for maintenance release R.03.00.13	QANote_08 ELO1879046	01	2021-01-27	The document is new for the DK-STM v03.00.13 maintenance update. The purpose of the Quality Note is to describe the process for generating the new maintenance release R.03.00.13. Release R.03.00.13 is considered by Siemens to be maintenance release due to the small changes. Two change requests from the customer are planned to be handled in the new maintenance release R.03.00.13 (CFX00517273 and CFX00517269). The document refers to the safety note (ref. [131]) regarding safety and severity. The DK-STM version 03.00.13 update process will follow the "CHAMPFX – Process flow", which includes separate Submission, Analysis, Solution, Verification and Validation documentation parts.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
131. Analysis for the DK-STM changes, DK-STM 03.00.13	SafetyNote_20	02	2021-02-10	The document is new for the DK-STM v03.00.13 minor maintenance update. It describes and analyses the safety consequences of the two changes to the DK-STM v03.00.13. The analysis done for software change and update concludes that the changes of the STM-DK constitute a minor change in the software which speaks for a minor maintenance release of STM version 03.00.13. The changes to the DK-STM 03.00.13 software, will be released 2nd quarter of 2021. It is stated in the CFXs that there are no identified hazards related to CFX00517269 in the STM-DK (ref. [133]) and that the change of the reconnection time from 1.8s to 5s (CFX00517273) has no negative impact on the safe operation of the vehicle as the train is still under control of the STM-DK in these extra 3.2s (ref. [134]).
132. Safety Assessment Report – DK-STM Generic Application (Baseline 3.0) version 03.00.12	2017:00826	7.0	2020-11-23	This is the Safety Assessment Report covering DK-STM version 03.00.12
133. CFXRequest CFX00517269 – ClearQuest Record Details	CFX00517269	-	2021-03-26	ClearQuest Record Details related to CFX00517269. The document, including its document references, represents complete documentation for the DK-STM version 03.00.13 update. The documented process includes six parts: Main, Analysis, CCB, Solution, Verification and Validation. The hazard workshops (20th of January 2021) concluded that there are no identified hazards related to this change in the STM-DK. SINTEF evaluates the content of the referenced version of date 2021-03-26 to be complete.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
134. CFXRequest CFX00517273 – ClearQuest Record Details	CFX00517273	-	2021-03-29	ClearQuest Record Details related to CFX00517273. The document, including its document references, represents complete documentation for the DK-STM version 03.00.13 update. The documented process includes six parts: Main, Analysis, CCB, Solution, Verification and Validation. Based on hazard workshop (15th of December 2020) it was concluded that the change of the reconnection time from 1.8s to 5s has no negative impact on the safe operation of the vehicle as the train is still under control of the STM-DK in these extra 3.2s. SINTEF evaluates the content of the referenced version of date 2021-03-29 to be complete.
135. SyValRep System Validation Report Release 03.00.13	G81001-X3107-U547-10	10	2021-03-25	This is an updated document covering DK-STM v03.00.13, covering addressed defects as identified in section 3.9 of the document, and with SW update as identified in section 6.1 of the document. It is stated and has been verified that there are no rule changes for this version. This version of the delta validation report contains the validation activities for the software versions 03.00.05, 03.00.06, 03.00.07, 03.00.08, 03.00.09, 03.00.10, 03.00.11, 03.00.12 and 03.00.13. The document identifies no new rules and 3 constraints, 2 modified rules, 7 deleted rules and no deleted constraints with respect to the System Validation Report (SyValRep, ref. [95]). Validation conclusion: "*The system STM-DK fulfils all requirements to meet its intended use. The system STM-DK with software version 03.00.13 is suitable to operation under consideration of the rules and constraints listed in chapter 9 and the requirements listed in "Table 25 List of changed evaluation on inapplicable requirements".* *The system STM-DK is suitable for the use with ETCS systems of UNISIG Baseline 2 and UNISIG Baseline 3".*

SINTEF

Technology for a better society

www.sintef.no