SINTEF

2022:00145- Restricted

Report

Safety Assessment Report

STM-DK Generic Application version 03.01.00

Author(s)
Narve Lyngby
Ulrik Johansen

SINTEF Digital
System Safety
2022-03-02

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

STM-DK Generic Application version 03.01.00

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

VERSION
2.0

DATE
2022-03-02

AUTHOR(S)
Narve Lyngby
Ulrik Johansen

CLIENT(S)
Siemens Mobility AS

CLIENT'S REF.
Tim Moltzen

PROJECT NO.
102026384

NUMBER OF PAGES:
48

ABSTRACT
Banedanmark has engaged SINTEF as an independent safety assessor ("ISA") for the STM-DK project.
The safety documentation for the STM-DK Generic Application version 03.01.00 has been assessed. SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.01.00 for use in specific applications provided the application rules and conditions in the Safety Case are adhered to.

PREPARED BY
Narve Lyngby

SIGNATURE

CHECKED BY
Robert Bains

SIGNATURE

APPROVED BY
Maria Bartnes

SIGNATURE

REPORT NO. 2022:00145
ISBN -
CLASSIFICATION Restricted
CLASSIFICATION THIS PAGE Restricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2022-02-21	Assessment based on Generic Application Safety Case for STM-DK version 03.01.00. This report is based on the SINTEF report 2017:00826, v8.0. The v8.0 of the report is still valid for R03.00.13 of STM-DK.
2.0	2022-03-02	Updated assessment based on updated Generic Application Safety Case (version 2.0) for STM-DK version 03.01.00. The update consists of minor wording corrections in section 5.2.2 in the Safety Case.

SINTEF

Table of contents

APPENDICES

None

1 Introduction

Siemens Mobility has engaged SINTEF as an independent safety assessor ("ISA") for assessing maintenance release (R03.01.00) of the STM-DK Generic Application. The STM-DK version 03.01.00 is a maintenance release based on version 03.00.10. The complexity and consequence of the R03.01.00 maintenance task has been evaluated by Siemens Mobility as a minor maintenance task which is not safety related.

The argumentation provided in the GASC R03.00.10 [1] for which the current APIS is based on is based on documentation, V&V and test results which are from release R03.00.10 and not the latest release R03.01.00.

Siemens has decided to replace the "safety note" approach which has been used for the maintenance updates R03.00.11, R03.00.12 and R03.00.13 with a maintenance Safety Case [2] to enable a complete safety argumentation for changes implemented since last GASC and APIS. Siemens states that the scope of the maintenance Safety Case [2] is to demonstrate "validity" of the existing GASC R03.00.10 as well as documenting changes and impact caused by other maintenance releases until R03.01.00.

The following assessments has been provided for the STM-DK versions 03.00.10 to 03.00.13:

- Version 03.00.10 was assessed by SINTEF in [42]. This was a maintenance release covering the correction of four defects.
- Version 03.00.11 was assessed by SINTEF in [43]. This was a bugfix release covering the correction of one defect.
- Version 03.00.12 was assessed by SINTEF in [44]. This was a maintenance release covering the correction of one defect.
- Version 03.00.13 was assessed by SINTEF in [45]. This was a maintenance release covering 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 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 Application Condition or Reservation (see below) will be given.

Application Condition (AC):

According to EN 50129, clause 5.4, application conditions are "...rules, conditions and constraints which shall be observed in the application of the system/subsystem/equipment". An AC relate to

- issues that shall be improved at an appropriate time. A matter of concern is the amount of ACs that should block the commissioning of a system. If this is the situation, SINTEF will make it clear in the conclusion.

- rules, conditions and limitations that are valid for the system under use, and must be adhered to during the whole lifecycle.

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. [13])
EN 50129:2003	Railway applications - Safety related electronic systems for signalling (ref. [14])
EN 50128:2001/2011	Railway applications - Software for railway control and protection systems (ref. [15])

These require a structured safety case as a foundation for an assessment. The assessor's task is according to EN 50129 (ref. [14]) 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*".

The Safety Case [2] refers to "old" version of EN 50126 (1999). It is stated in the Safety Case [2] that EN50126:2017 is only required "to the extent and insofar as existing systems are being modified". Siemens has further stated that this represents a maintenance update, and in case of maintenance; only EN50126:1999, section 6.11 for maintenance is required.

The Safety Case [2] refers to "old" version of EN 50129 (2003). Explanation is not provided in the Safety Case. However, in reply to SINTEF in LooP [85], Siemens refers to chapter 1 in EN 50129:2018 [16], quote: "*This document is not applicable to existing systems, subsystems or equipment which had already been accepted prior to the creation of this document. However, so far as reasonably practicable, it should be applied to modifications and extensions to existing systems, subsystems and equipment*". Moreover, Siemens states in presentation to SINTEF [86] that section 8.3 in EN 50129:2018 [16] is applied for the project. Chapter 1 in the Safety Case [2] also states that R03.01.00 of the STM DK Generic Application is a minor maintenance release, and that it is not safety relevant. The Safety Case is thus a delta Safety Case providing safety argumentation for changes implemented since last GASC [1].

SINTEF considers that the changes made to the system in R03.00.11 to R03.01.00 could be considered as modifications. However, the maintenance upgrade or modification is considered so small that SINTEF finds this to be acceptable for the maintenance update R03.01.00.

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. [3]) which was contractually agreed with Banedanmark and approved by the national safety authority "Trafikstyrelsen".

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 [2]) and the present report assumes that the reader is familiar with the Safety Case.

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

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.*"

Reference is made in section 2 in the Safety Case for R03.01.00 [2] to section 1 of the GASC for R03.00.10 [1]. Impact on the system definition caused by the maintenance releases R03.00.11, R03.00.12, R03.00.13 and R03.01.00 are provided in chapter 2 of the Safety Case for R03.01.00 [2].

It is stated that existing description from section 1 in [1] remains valid for R03.00.10. It is further stated that R03.00.11 to R03.00.13 are classified as minor maintenance releases in [34], [35] and [36], and that the maintenance work does not change the system description provided in GASC for R03.00.10 [1]. The system definition provided for R03.00.10 in [1] is therefore considered by Siemens as valid for the maintenance release R03.00.11 to R03.00.13. SINTEF agrees with this in assessment reports [43] for R03.00.11, [44] for R03.00.12 and [45] for R03.00.13.

For R03.01.00 it is stated that [76] classifies this version as a minor maintenance release. The work is described in [76] and does not change the system description provided in GASC for R03.00.10 [1]. The GASC for R03.00.10 [1] is therefor stated by Siemens to be valid as system definition for release R03.01.00.

SINTEF considers this 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 [2] addresses all the points plus a few more.

3.2.1 Preface

The preface states that the Quality Management Report "*This section constitutes part 2 of the safety case in accordance with [EN50129] chapter 5.2.*"

The reference and structure of the Quality Management Report is according to EN 50129:2003 [14].

3.2.2 Quality Management System and the Lifecycle Model

Reference is made to the Quality Assurance Plan [30]. 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 [22].

For realisation, the 2001 and 2011 versions of the EN 50128 standard are referenced being applied. The 2011 version in relation to the 2001 version of the standard has been specifically addressed in the system and software maintenance [71]. For STM-DK R03.01.00, 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 the Safety Case [2]. Closeout of the EN 50128:2011 section 9.2 requirements are covered in the referenced system and software maintenance [71]. 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

Document evidence for the project organisation and documentation of personnel competence, independence of roles and staff qualification are referenced [25]. Proof of competencies has due to personal data laws been placed in a separate document called “Documentation of Personnel Competence – List of CVs” [10].

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

Further; SINTEF has reviewed personnel competency as part of audits of Siemens, latest in audit on the quality management system in 2020: Quality Management System Approval Report, Report No. 2017:00568, dated 2020-04-03 [37].

SINTEF considers the organisation to be acceptable.

3.2.4 Quality Planning and Procedures

Reference is made to the Quality Assurance Plan [30]. In addition, other plans relevant for quality assurance are identified with reference to the Document List [12], i.e. the Organisation- and competence plan [25], System Safety Plan [64], Configuration Management Plan [9], System Ram Plan [61], Software Verification and Validation Plan [58] and System Verification and Validation Plan [70]. The documents have been reviewed according to document status in the Document List [12].

SINTEF considers the quality planning and procedures to be acceptable.

3.2.5 Specification of Requirements

The System Requirement Specification [46] is considered to be the customer requirement specification. Supplements and clarifications of the SRS are provided in the SRS Clarification (SRSClar) [47], and it is stated that the maintenance release is based on this document.

Review of the SRSClar is documented in the Document List, ref. [12].

It is stated in the Safety Case that every requirement from the SRS has been incorporated in the SRSClar (ref. [47]) 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. [47]).

SINTEF considers the specification of requirements to be acceptable.

3.2.6 Design Control

The design control is supported through review of documentation from the SRS Clarification (SRSClar, ref. [47]) to the Source Code, via System Architecture [59] and SW Requirement Specification (included in the System Architecture) [59], SW Architecture Specifications [48] and [49] which include the SW Design Specifications, and SW Module Design Specifications. SRS Clarification (SRSClar, ref. [47]) requirements are traced down to the software module design.

It is stated that every specified test report in the Software Verification and Validation Plan [58] and the System Verification and Validation Plan [70] are present and approved. Test reports are identified and stated available in the Document list and document control [12]:

- Software Integration Test Report Gateway [52].
- Software Integration Test Report ZUB123 [53].
- Software Hardware Integration Test Report [50].
- Software Validation Report, version 03.01.00 [57].
- System Integration Test Report [60].
- System Validation Report, version 03.01.00 [66].

The process has been verified in VerRep_03.01.00 [73].

SINTEF considers the design control to be acceptable.

3.2.7 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.

3.2.8 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.

3.2.9 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.

3.2.10 Handling and Storage

Reference is made to the Application Rules [5] for any requirements concerning the handling and storage of the STM-DK.

SINTEF considers handling and storage to be acceptable.

3.2.11 Inspection and Testing

Reference is made to section 3.6.2 "Design verification and reviews" of the Quality Management Report. For the final product it is stated "*Inspection and testing in the production will follow internal procedures for production of vital equipment ...*"

Reference is also provided to section 3.7 in the Safety Case, mentioning product numbers. See sections 3.2.6 and 3.2.7 in the report at hand.

SINTEF considers inspection and testing to be acceptable.

3.2.12 Non-Conformance and Corrective Actions

Normal quality non-conformities are treated according to Mobility Process House (PH), discipline: “Quality Management in the Line, Deviations”. Defects in the system (software) are handled in ClearQuest as described in the Configuration Management Plan [9] and in the Introduction to the ClearQuest [11].

It is further stated that during CCB (Change Control Board) meetings it is checked that ClearQuest is used correctly. The actual evaluation of the ClearQuest database was done by the validation and id documented in the System Validation Report [66] and in the Software Validation Report [57]. In addition; for the R03.01.00

VE6[1] Maintenance weekly core team meetings have been used to identify non-conformancies and progress documented in the Minutes of Meetings.

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

3.2.13 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.

3.2.14 Installation

Installation is stated not to be a part of the maintenance release project. Reference is made to the Installation Manual [20].

SINTEF considers installation to be acceptable.

3.2.15 Commissioning

Reference is made to documentation intended to be applicable for commissioning, i.e.:

- System Description [65].
- User Manual [72].
- Installation Manual [20].
- Maintenance Manual [24].

SINTEF considers commissioning to be acceptable.

3.2.16 Operation and Maintenance

Operation and maintenance are stated not to be a part of the maintenance release project; operation and maintenance will not be relevant until the specific application. Reference is, however, made to the User Manual [72] and the Maintenance Manual [24].

SINTEF considers operation and maintenance to be acceptable.

3.2.17 Quality Monitoring and Feedback

References are made to sections 3.6.2 "Design Verification and Review" and 3.12 "Non Conformance and Corrective Actions" of the Safety Case, corresponding to sections 3.2.6 and 3.2.12 in this report.

SINTEF considers quality monitoring and feedback to be acceptable.

3.2.18 Documentation and Records

Reference is given to Document List and Document Control [12] for listing of all documents relevant for the project. Technical and administrative documentation are stored in the document management system "ELO" as described in the Configuration Management Plan [9].

SINTEF considers the documentation and records to be acceptable.

[1] The VE6 board are a COTS product with an existing approval for use on the TCC 4.1 platform.

3.2.19 Configuration Management/Change Control

It is stated that ClearCase (ChampFx) is used for change control, and reference is provided to the project specific Configuration Management Plan [9].

Software releases are documented in the Software Release Note [56] and practical realization of configuration control is implemented in the Configuration Management Control Sheet [8].

The Configuration Management Plan [9] has been reviewed and review documentation is stored in ELO according to [12].

SINTEF considers configuration management and change control to be acceptable.

3.2.20 Risk Management

Deviations, non-conformities, project changes and risks are registered in MPPT (Mobility Project Transparency Tool). MPPT (Mobility Project Transparency Tool), with list of risks is used in the project and updated every month via monthly reports to the steering committee.

To ensure follow-up on a regular basis, weekly Core Team meetings are conducted. 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 3.2.12 of this report.

SINTEF considers this to be acceptable.

3.2.21 Personnel Competency and Training

The competencies of the project members are documented in Organisation and Documentation of Personnel Competence [25]. The document specifies the roles, responsibilities and required competencies. Proof of competencies is documented separately in Documentation of Personnel Competence - List of CV's [10].

SINTEF considers the personnel competency and training to be acceptable.

3.2.22 Quality Audits and Follow-up

No internal audits have been performed in the maintenance release project. It is, though, stated that a risk assessment has been done by the quality manager in the project (QMiP) based on the following points:

- The QMiP is involved in all aspects of the quality assurance activities daily
- Weekly core team meetings with the participation of the Project, the Project Manager, the Safety Manager, the QMiP, the Architect and the Designer are held discussing all relevant issues
- Registration and handling of issues in the clearquest system (ChampFx)
- Conduction milestone meetings with milestone reports
- Checking and reporting the activities in the Verification Report [73]

Leading to the conclusion by Siemens that this may constitute an adequate substitute for an actual quality audit.

SINTEF as NoBo also performed a remote audit on the quality management system in 2020: Quality Management System Approval Report, Report No. 2017:00568, dated 2020-04-03 [37].

There were no issues for follow-up.

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

3.2.23 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 STM-DK 03.01 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.

3.3 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 Case makes a general reference to the GASC for STM-DK R03.00.10 [1], covering the safety management performed until (and including) R03.00.10. It is further stated that the safety management report in the GASC for STM-DK R03.00.10 [1] is valid for R03.00.10 and demonstrate compliance with the System Safety Plan [64] for the development project until R03.00.10. The GASC for STM-DK R03.00.10 [1] was assessed by SINTEF as ISA in [42].

It is further stated that all releases after R03.00.10 and until R03.01.00 are maintenance releases which follows a separate safety process for maintenance which does not change the processes of the System Safety Plan [64] or the results of the safety management documented in the safety management report of the GASC for STM-DK R03.00.10 [1].

Additional evidence of safety management performed for maintenance releases R03.00.11 to R03.01.00 are provided in the Safety management Report chapter of the Safety Case [2], and the assessment is provided in the sections below.

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 ...*"

Maintenance release R03.00.11 to R03.00.13

Safety argumentation for the maintenance releases R03.00.11, R03.00.12 and R03.00.13 is given in the Quality Notes [27], [28] and [29], and the Safety Notes [34], [35] and [36].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that the safety lifecycle for maintenance release R03.01.00 are defined in section 3 of the Maintenance Safety Plan for STM Maintenance release 03.01 [63]. Compliance with the safety life-cycle in section 3 of [63] is documented in section 4.3 in the Safety Case. See section 3.3.3 in the report at hand.

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 ...*"

Maintenance release R03.00.11 to R03.00.13

Safety organisation for each maintenance releases has been managed by update of Organisation and Documentation of Personnel Competence [25] for each release.

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

The safety organisation is a part of the project organisation, which is documented in Organisation and Documentation of Personnel Competence [25]. 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.*"

Maintenance release R03.00.11 to R03.00.13

Safety argumentation for the maintenance releases R03.00.11, R03.00.12 and R03.00.13 is given in the Quality Notes [27], [28] and [29], and the Safety Notes [34], [35] and [36].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

Reference is made to Maintenance Safety Plan for STM Maintenance release 03.01 [63], which has been commented by SINTEF in LooP [85]. SINTEF considers this document to fulfil the applicable requirements for a Safety Plan as stated in EN 50126 and EN 50129 and is suitable for its intended use.

An overview of activities of the safety program for R03.01.00, including references to resulting documentation of the activities, are provided in the Safety Case [2].

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.*"

Maintenance release R03.00.11 to R03.00.13
Safety argumentation for the maintenance releases R03.00.11, R03.00.12 and R03.00.13 is given in the Quality Notes [27], [28] and [29], and the Safety Notes [34], [35] and [36].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that Maintenance release R03.01.00 includes correction of defects as well as implementation of minor changes, and that the analysis demonstrates that the task is a minor maintenance release which is not safety relevant. It is therefore concluded by Siemens that no significance evaluation and hazard workshop have been needed and no new hazards have been identified. The existing hazard log from release R03.00.10 ([17] and [18]) is therefore unchanged. Reference is also provided to consequence evaluation [77] and the complexity evaluation included in the change description [76].

SINTEF considers this to be acceptable. However, the last revision of the Hazard Log is from 2017. It is stated in EN 50129: "*The Hazard Log shall be updated if any modification or alteration is made to the system, subsystem or equipment*". Hence:

Recommendation STM-DK 03.01 2: The Hazard Log should be updated when changes are made to the system even though no new hazards are identified.

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.*"

Maintenance release R03.00.11 to R03.00.13
It is stated that the maintenance task is minor, non-safety related, and no hazards were identified. The maintenance releases have therefore no changes to the existing safety requirements contained in Customer's Requirement Specification, [46]. The GASC for STM-DK R03.00.10 [1] section 3.5 therefore remains unchanged.

Maintenance release R03.01.00

It is stated that the maintenance task is minor, non-safety related, and no hazards were identified. The maintenance releases have therefore no changes to the existing safety requirements contained in Customer's Requirement Specification, [46]. The GASC for STM-DK R03.00.10 [1] section 3.5 therefore remains unchanged.

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.*"

Maintenance release R03.00.11 to R03.00.13

It is stated that R03.00.11 to R03.00.13 is classified as a maintenance task and not as a system/subsystem design task. The maintenance release of R03.00.11 to R03.00.13 has resulted in maintenance update of some of the design documents referenced in section 3.6 in the GASC for STM-DK R03.00.10 [1].

Maintenance release R03.01.00

It is stated that R03.01.00 is classified as a maintenance task and not as a system/subsystem design task. The maintenance release of R03.01.00 has resulted in maintenance update of some of the design documents referenced in section 3.6 in the GASC for STM-DK R03.00.10 [1].

It is further stated that the maintenance releases from R03.00.10 to R03.01.00 where all minor and not safety related. The safety argumentation in the GASC for STM-DK R03.00.10 [1] is therefore stated to be still valid for the updated design documentation when used together with this document. Reference is given to the Configuration Management Control Sheet [8] for a complete list of valid design document versions. The Configuration Management Control Sheet [8] also identifies which documents have been updated for this release.

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.*"

Maintenance release R03.00.11 to R03.00.13

It is stated that no safety audits are performed (or expected) for minor non safety related maintenance.

Maintenance release R03.01.00

It is stated that no safety audits are performed (or expected) for minor non safety related maintenance.

It is also stated that review of documents includes the safety manager which ensures compliance with the safety requirements and safety process.

SINTEF considers this to be tolerable.

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 ..."

Maintenance release R03.00.11 to R03.00.13

It is stated that planning of validation and verification for the maintenance releases R03.00.11, R03.00.12 and R03.00.13 is covered by the Quality Notes [27], [28] and [29]. It is further stated that the result of verification was documented in the CHAMP FX system together with the documentation of the change. Result of the

validation was documented as “add-on” to the existing validation in the System Validation Report [68] and [69].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

For the maintenance release R03.01.00, it is stated that Verification and Validation has been implemented in compliance with the Verification and validation plans [58] and [70]. Verification is documented in [73] and validation is documented in [66] and [57]. The verification and validation for R03.01.00 supersedes all previous verification and validation. Reference is given to Configuration Management Control Sheet [8], providing a list of updated verification and validation documentation.

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 ...*"

Maintenance release R03.00.11 to R03.00.13

It is stated that justification for not safety related changes is provided in the safety notes [34], [35] and [36]. Section 3.9 of the GASC for STM-DK R03.00.10 [1] is therefore stated to remain unchanged.

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that justification for not safety related change is provided in the consequence evaluation [77]. Section 3.9 of the GASC for STM-DK R03.00.10 [1] is therefore stated to remain unchanged.

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.*"

Maintenance release R03.00.11 to R03.00.13

It is stated that there were no changes to handover documentation. Section 3.10 of the GASC for STM-DK R03.00.10 [1] is therefore stated to remain unchanged.

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that changes to handover documentation were identified in the consequence evaluation [77]. Handover documentation listed in the GASC for STM-DK R03.00.10 [1] will remain unchanged but will in some cases be updated to newer versions as identified in the Configuration Management Control Sheet [8]. It is also stated that this document will be added to the list of handover documentation.

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.*"

It is stated that the existing description in the GASC for STM-DK R03.00.10 [1] is unchanged and remains valid.

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 the existing description in the GASC for STM-DK R03.00.10 [1] is unchanged and remains valid. See also section 3.2.23.

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*

The safety Case makes a general reference to the GASC for STM-DK R03.00.10 [1], covering the technical safety performed until (and including) R03.00.10. It is stated that maintenance releases after R03.00.10 and until R03.01.00 are minor maintenance releases which are all evaluated as not safety related. The technical safety report in the GASC for STM-DK R03.00.10 [1] is therefore stated valid for R03.01.00 when used together with the GASC for R03.01.00 [2]. The GASC for STM-DK R03.00.10 [1] was assessed by SINTEF as ISA in [42].

The purpose of the technical safety report in the Safety Case [2] is to supplement the existing technical safety report in the GASC for STM-DK R03.00.10 [1] with safety argumentation covering updates of documentation, V&V and test performed during the non-safety related maintenance releases R03.00.11, R03.00.12, R03.00.13 and R03.01.00.

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 ...*"

It is stated that the existing description in the GASC for STM-DK R03.00.10 [1] is unchanged and remains valid.

It is described in the GASC for STM-DK R03.00.10 [1] that 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. [15]) 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 in the Safety Case [2], 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:

3.4.2.1 System architecture description

Maintenance release R03.00.11 to R03.00.13
It is stated that the maintenance releases did not include update of System Architecture Specification [59]. Instead the System Architecture Specification [59] changes were verified and managed as „add on“ via CHAMP FX and validated in the Validation Reports [68] and [69].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that R03.01.00 includes updates of the System Architecture Specification [59] containing “clean up” from release R03.00.11 to R03.00.13 as well as new changes defined for the R03.01.00 update.

The changes are defined in the System Change Description [76] and includes updated TCC software and replacement of VE5 by new VE6 hardware. The System Architecture Specification [59] has been reviewed and verified as described in section 3.6 in the Safety Case [2], see section 3.2.6 in the report at hand.

The update of application rules for safe use of the updated TCC platform has been imported to the System Architecture Specification [59] and the completeness of the System Architecture Specification [59] regarding requirements from TCC and input documents has been validated and confirmed in the System Validation Report [66].

3.4.2.2 Definition of interfaces

Maintenance release R03.00.11 to R03.00.13
It is stated that the maintenance releases include minor changes related to the interface to the DMI. The changes where verified and managed as „add on“ via CHAMP FX and validated in [68] and [69].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that R03.01.00 includes minor updates related to the interfaces (new TCC release, change to PEGEL level for antenna and display of failure codes on DMI). The updates are defined in the System Change Description [76] and are evaluated by Siemens as minor and not safety related. It is further stated that these updates have lead to update of the User Manual [72] regarding failure codes and an update of TCC conditions of use as defined in the Condition of Use [79].

3.4.2.3 Fulfilment of the System Requirements Specification

Maintenance release R03.00.11 to R03.00.13
It is stated that the maintenance releases did not include update of the system requirement specification [46] or the DOORS requirements clarification module [47]. Instead the changes where verified and managed as „add on“ via CHAMP FX and validated in [68] and [69].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that R03.01.00 includes updates of the system requirement specification [46] or the DOORS requirements clarification module [47] containing “clean up” update of all changes from release R03.00.11 to R03.00.13 as well as changes made for R03.01.00. Note; as stated in section 3.3.5 in the report at hand, no changes are made to the existing safety requirements. The update of the clarification module [47] has been reviewed and verified as described in section 3.6 in the Safety Case [2], see section 3.2.6 in the report at hand.

Fulfilment of requirements is validated and confirmed by the Validator mainly via links from the System Requirement Test Specification [62] as documented in the System Validation Report [66].

3.4.2.4 Fulfilment of the Safety Requirement Specification

Maintenance release R03.00.11 to R03.00.13
It is stated that maintenance release R03.00.11 to R03.00.13 was evaluated by Siemens as not safety related. There are therefore no changes to the safety requirements contained in the system requirement specification [46] or the DOORS requirements clarification module [47]. The existing description in the GASC for STM-DK R03.00.10 [1] is therefore unchanged and remains valid.

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance releases are assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that R03.01.00 is evaluated by Siemens as not safety related. There are therefore no changes to the safety requirements contained in the system requirement specification [46] or the DOORS requirements clarification module [47]. The existing description in the GASC for STM-DK R03.00.10 [1] is therefore unchanged and remains valid.

Reference is further provided to section 5.5 in the Safety Case (Safety-Related Application Conditions (SRACs)) [2], see section 3.4.5 in the report at hand.

3.4.2.5 Assurance of correct hardware functionality

Maintenance release R03.00.11 to R03.00.13
It is stated that there are no hardware changes to the maintenance release R03.00.11 to R03.00.13.

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance release is assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that Release R03.01.00 includes Introduction of hardware board VE6. The VE6 board are a COTS product with an existing approval for use on the TCC 4.1 platform. It is further stated that the refurbishment of hardware VE6 is not a change but a hardware maintenance task. This is demonstrated in the Consequence Evaluation [77] and confirmed in the System Change Description [76]. Besides the replacement of VE5 by VE6 there are no other changes to the hardware compared to release R03.00.10.

3.4.2.6 Assurance of correct software functionality

Maintenance release R03.00.11 to R03.00.13
It is stated that minor non safety maintenance corrections has been made to the gateway software. Changes, review and verification where documented as „add on“ via CHAMP FX. Assurance of correct functionality was confirmed via validation in [68] and [69].

It is further stated that there are no changes to the ZUB123 or TCC software components in maintenance release R03.00.11 to R03.00.13

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for each maintenance release is assessed by SINTEF in [43], [44] and [45].

Maintenance release R03.01.00

It is stated that minor non safety maintenance corrections have been implemented to the gateway software. The software architecture specification for the gateway [48] has therefore been updated. The source code files are stated verified and tested as specified in the Checklist for Software Module Review [55] and as documented

in the Verification Report for R03.01.00 [73]. Correct function of the Gateway component is verified in the Software Integration Test Report [52]. Assurance of correct function is confirmed by validation in the Software Validation Report [57].

It is further stated that minor non safety maintenance corrections have been implemented to the ZUB123 software. The software architecture specification for the ZUB [49] has therefore been updated. The source code files are verified and tested as documented in the Verification Report for R03.01.00 [73]. Correct function of the Gateway component is verified in the Software Integration Test Report [53]. This is confirmed by software validation in the Software Validation Report [57].

It is also stated that TCC software components of TCC release 1.3 has been updated to TCC release 4.1 [79]. The TCC software components are stated to be standard modules validated and assessed with accompanying SRAC. All relevant SRAC from the Condition of Use [79] are found in DOORS [4] and linked from the System Architecture Specification [59]. All changes to the SRAC in System Architecture Specification [59] are identified and can be found in section 5.5.2.2 in the Safety Case [2], see section 3.4.5 in the report at hand. This is confirmed by validation in the System Validation Report [66].

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.*"

It is stated that the existing description in the GASC for STM-DK R03.00.10 [1] remains valid for release R03.00.11, R03.00.12, R03.00.13 and R03.01.00.

SINTEF considers this to be acceptable.

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)."*

It is stated that the existing description in the GASC for STM-DK R03.00.10 [1] remains valid for release R03.00.11, R03.00.12, R03.00.13 and R03.01.00.

SINTEF considers this to be acceptable.

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.*"

Changes to the Safety Related Application Conditions (SRACs) which shall be fulfilled by the STM-DK are listed in the Safety Case (ref. [2] grouped in Safety Related Application Conditions (SRACs) which shall be fulfilled by the STM-DK Specific Application (section 5.5.1 in the Safety Case [2]) and Safety Related Application Conditions (SRACs) which shall be fulfilled by the STM-DK Generic Application (section 5.5.2 in the Safety Case [2]). The lists assemble SRACs from the Application Rules [5] which are changed, deleted or new when comparing release R03.01.00 with R03.00.10.

Safety Related Application Conditions (SRACs) which shall be fulfilled by the STM-DK specific application are maintained and documented via the DOORS module Application Rules [5].

Safety Related Application Conditions (SRACs) which shall be fulfilled by the STM-DK generic application are maintained and documented via the DOORS modules Application rules exported from the TCC 4.1 [4] and System Architecture Specification [59]. In addition to the two DOORS modules there are also SRAC for the Generic Application which are defined in the following two documents System Validation Report [66] and legacy ATC Safety Case [6].

All changes to the SRAC for generic application from release R03.00.11 to R03.01.00 has been validated in the System Validation Report [66] and are documented in the sections 5.5.2.1 to 5.5.2.6 in the Safety Case [2].

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 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 the assessment report for the STM-DK from SINTEF ([38] and [39]) safety qualification tests have been covered by application rules as identified in relevant Safety Case.

SQT was performed and documented in the assessment report from SINTEF [40], based on early planning, ref. [83], and the documentation of the test specification, performance and approval, ref. [84].

Four ATC errors were reported, all documented and analysed in [84] and considered by SINTEF in the assessment report [40] not to have safety impact.

The conclusion from the testing documented in ref. [84] was, quoted: "*the STM-DK 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 STM-DK. This implies that experience testing for STM-DK versions after R03.00.07 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 the assessment report from SINTEF [40].

No further activities concerning SQT has been reported for STM-DK versions R03.00.09 to R03.01.00. The relevant application rules for SQT have been deleted, which according to Siemens has been done in cooperation with Banedanmark.

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."

It is stated that the related safety cases in section 5 in the GASC for STM-DK R03.00.10 [1] are not affected by any of the maintenance releases R03.00.10 and until R03.01.00. Section 5 of the GASC for STM-DK R03.00.10 [1] therefore remains unchanged.

It is, however, stated that the related safety cases from the TCC Platform have been updated because maintenance release R03.01.00 uses an updated TCC platform (TCC 4.1). However, reference is made to section 5.5.2.1 in the Safety Case [2] for description of all updates to the TCC SRACs, see section 3.4.5 in the report at hand.

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:

" For maintenance upgrade from R03.00.13 to R03.01.00 it is demonstrated that the maintenance is implemented in compliance with the maintenance safety plan [MaintSafePl] and the quality plan [QaPl]. It is shown that the STM-DK maintenance upgrade R03.01.00 has a minor complexity with a non safety classification of the consequence. This classification is demonstrated in [SyChngDesc] for the complexity evaluation and in [ConEval] for consequence evaluation. Analysis of impact on the existing safety argumentation in [GASC_Cert_R03.00.10] has been completed and demonstrate that the safety argumentation in [GASC_Cert_R03.00.10] remains valid for R03.01.00 when considered together with the maintenance release addressed in this maintenance GASC.

For previous maintenance upgrade R03.00.11, R03.00.12 and R03.00.13 an analysis of impact on the existing safety argumentation in [GASC_Cert_R03.00.10] has been performed by identifying updates, documents and validation performed for the maintenance releases. The impact analysis has shown that all outstanding document updates and (delta)V&V now has been included into the R03.01.00 documents and that the 3 maintenance releases all are classified as not safety related.

For the R03.01.00 maintenance release the complete safety argumentation is therefore comprised by the following two documents:

- *STM-DK R03.00.10, For safety development and upgrade of STM-DK, [GASC_Cert_R03.00.10] (Argumentation for safety of STM-DK)*
- *STM-DK R03.01.00, For non safety related maintenance of STM-DK from R03.00.10 to R03.01.00. (Argumentation for not affecting safety of the STM-DK*".

No conditions are given in the Safety Case [2].

SINTEF considers the conclusion to be acceptable.

4 Assessment

The maintenance upgrade of STM-DK from R03.00.10 to R03.01.00 have been described in the Safety Case for STM-DK R03.01.00 [2].

Compliance with the Cenelec (EN 50126 [13], EN 50128 [15] and EN 50129 [14]) requirements for R03.00.10 is assessed by SINTEF in [42], and the maintenance releases R03.00.11, R03.00.12 and R03.00.13 are assessed by SINTEF in [43], [44] and [45].

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 03.01.00 for use in specific applications provided the application rules and conditions in the Safety Case are adhered to.

4.1 Application Conditions, Reservations and Recommendations

There are no Application Conditions, no Reservations and two Recommendations in the present report. They are listed below:

Recommendation STM-DK 03.01 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.

Recommendation STM-DK 03.01 2: The Hazard Log should be updated when changes are made to the system even though no new hazards are identified.

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. [2]) 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 STM-DK R03.00.10 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.	Maintenance GASC STM Maintenance release R03.01	G81001-X3107-U420-01	2.0	2022-02-28	The purpose of this Maintenance GASC is to demonstrate the safety of the minor maintenance release R03.01.00. This maintenance GASC is a add on the existing GASC covering R3.00.10. and is valid for STM-DK version 03.01.00. SINTEF comments: The GASC is assessed in the report at hand.
3.	ISA and NoBo assessment plan for STM-DK 03.01.00	102026384-NOT-2022-01	1.0	2022-02-18	This contains a description of the assessment activities to be performed during the project.
4.	AnwRglTCC	ZUB123STM/Z123 STM_INT/ 20_Arch/30_SysComp/Anwenderregeln	-	-	Application rules exported from the TCC 4.1.
5.	AppRule, Application Rules	G81001-X3107-L005-10	10	2022-02-01	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.	ATCSpec ATC Systemspecifikation	G81001-K3118-U002-H	H	2002-07-31	This is a set of documents that together constitute the specification of the Danish ATC system ZUB 123/LZB-DSB

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
7.	CE_Declar	A6Z08110407235	000	2016-02-17	EC-Declaration of conformity, Basissystem TCC 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 Safety Case [2] are still applicable.
8.	CmCtrlSheet Configuration Management Control Sheet	G80001-X3107-U513-11	11	2022-01-31	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 11 covering STM-DK R03.01.00.
9.	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
10.	CompList Documentation of Personnel Competence – List of CV's	G81001-X3107-U401-08	08	-	This document is not submitted due to data privacy regulations, but can be made available on request. SiNTEF has, however, reviewed personnel competency as part of audits of Siemens, latest in audit on the quality management system in 2020: Quality Management System Approval Report, Report No. 2017:00568, dated 2020-04-03 [37]. SINTEF considers this to be acceptable.
11.	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.
12.	DocList Document List and Document Control	G81001-X3107-L001-11	11	2022-02-14	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 11 also covering STM-DK R03.01.00 VE6.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
13.	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 STM-DK are developed and updated, and against which the assessment has been performed. They require a structured safety case as a basis for assessment.
14.	EN 50129 Railway Applications – Safety Related Electronics Systems for Signalling	EN 50129	-	Feb 2003	
15.	EN 50128 Railway Applications – Communications, Signalling and Processing Systems – Software for Railway Control and Protection Systems	EN 50128	-	2001 2011	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.
16.	EN 50129 Railway Applications – Safety Related Electronics Systems for Signalling	EN 50129	-	Feb 2018	
17.	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.
18.	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*".
19.	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 STM-DK 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.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
20.	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
21.	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.
22.	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 ISO 45001:2018. It is valid until 2024-09-02.
23.	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.

24.	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

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
25. OrgComp Organisation and Documentation of Personnel Competence	G81001-X3107-U404-09	09	2021-08-05	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 09, covering updates of roles and organization diagram applicable for STM-DK R03.01.00 VE6.
26. QANote_05 Update process for maintenance release R.03.00.10	QANote_05	01	2017-07-17	The document is new for the STM-DK R03.00.10 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 STM-DK R03.00.09 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.
27. QANote_06 Update process for maintenance release R.03.00.11	QANote_06	01	2019-01-22	The document is new for the STM-DK R03.00.11 maintenance update. The document describes the update process to follow. There is one defect (CFX00414575) which have been discovered during testing with STM-DK R03.00.09 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 STM-DK 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
28.	QANote_07 Update process for maintenance release R.03.00.12	QANote_07	01	2020-09-11	The document is new for the STM-DK R03.00.12 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. [35]) regarding safety and severity. No new features – or alteration of features – will be implemented in R.03.00.12 because of the defect. The STM-DK version 03.00.12 update process will follow the "CHAMPFX – Process flow", which includes separate Submission, Analysis, Solution, Verification and Validation documentation parts.
29.	QANote_08 Update process for maintenance release R.03.00.13	QANote_08	01	2021-01-27	The document is new for the STM-DK R03.00.13 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. [36]) regarding safety and severity. The STM-DK 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
30.	QaPl Quality Assurance Plan	G81001-X3107-U400-04	04	2021-08-12	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 for release 03.01.00.* *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.
31.	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.
32.	RMPlan RM-Plan Guide	A6Z00002541903	G	2017-03-03	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
33.	SafetyNote_17 Analysis for the STM-DK defects, STM-DK R.03.00.10	SafetyNote_17	01	2018-09-20	The document is new for the STM-DK R03.00.10 maintenance update. It describes and analyses the safety consequences of the four defects to be corrected with the STM-DK R03.00.10. 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
34.	SafetyNote_18 Analysis for the STM-DK defects, STM-DK R.03.00.11	SafetyNote_18	02	2019-02-06	The document is new for the STM-DK R03.00.11 maintenance update. It describes and analyses the safety consequences of the one defect to be corrected with the STM-DK R03.00.11. 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.
35.	SafetyNote_19 Analysis for the STM-DK defects, STM-DK R.03.00.12	SafetyNote_19	02	2020-10-07	The document is new for the STM-DK R03.00.12 maintenance update. It describes and analyses the safety consequences of the one defect to be corrected and two changes to the STM-DK R03.00.12. 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 STM-DK 03.00.12 software.
36.	SafetyNote_20 Analysis for the STM-DK defects, STM-DK R.03.00.13	SafetyNote_20	02	2021-02-10	The document is new for the STM-DK R03.00.13 minor maintenance update. It describes and analyses the safety consequences of the two changes to the STM-DK R03.00.13. 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 STM-DK 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 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.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
37.	SINTEF_16 Quality Management System Approval Report	SINTEF 2017:00568	4.0	2020-04-03	The purpose for the update of this report from v3.0 to v4.0 is to document a QMS surveillance audit for the STM-DK covering versions 03.00.08 to 03.00.11.00. The report concludes: "*…Consequently, the quality work performed in conjunction with the design, production and final product inspection and testing of the STM-DK Interoperability Constituent, versions 03.00.08, 03.00.09, 03.00.10 and 03.00.11/03.00.11.00, fulfils the requirements to a module CH1 Quality Management System Approval Certificate according to the guidelines of the NB-Rail RFU-STR-001 Content of issued certificate*."
38.	SAR_R03.00.07	SINTEF F27264	1.0	2015-10-30	The SINTEF Safety Assessment Report for STM-DK R03.00.07, covering the STM-DK update to comply with the Baseline 3 Release 2.
39.	SAR_R03.00.08	SINTEF F27264	2.0	2016-07-06	The SINTEF Safety Assessment Report for STM-DK R03.00.08. A separate safety assessment, concerning SQT testing, was done after the assessment of R03.00.08 of STM-DK. That assessment was reported in version 3.0 of this document. The assessment report concludes: "*SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.00.08 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application.…* *…There are no Application Conditions, two Reservations and one Recommendation in the present report* *Reservation 1. The SRACs as identified by the Generic Application Safety Case and its referenced documents must be formally accepted by BDK.* *Reservation 2. If any SRACs as identified by the Generic Application Safety Case and its referenced documents are reworded, reclassified or redistributed the Safety Case shall be updated accordingly and submitted for reassessment.*"

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
40. SAR_R03.00.08 SQT	SINTEF F27264	3.0	2017-02-10	Updated to cover safety qualification testing according to Generic Application Safety Case for STM-DK version 03.00.08. The assessment report concludes: "*SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.00.08 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application.* *With version 3.0 of this report, the Safety Qualification Tests (SQT) has been performed as documented in section 3.4.6. As stated in section 3.4.6, it is noted that train installation applied was based on STM-DK version 03.00.07…* *…There are no Application Conditions, two Reservations and one Recommendation in the present report* *Reservation 1. The SRACs as identified by the Generic Application Safety Case and its referenced documents must be formally accepted by BDK.* *Reservation 2. If any SRACs as identified by the Generic Application Safety Case and its referenced documents are reworded, reclassified or redistributed the Safety Case shall be updated accordingly and submitted for reassessment.*"
41. SAR_R03.00.09	SINTEF F27264	4.0	2017-12-19	The SINTEF Safety Assessment Report for STM-DK R03.00.09. The assessment report concludes: "*SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.00.09 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application…* *…There are no Application Conditions, no Reservations and one Recommendation in the present report* "
42. SAR_R03.00.10	SINTEF 2017:00826	5.0	2018-10-18	The SINTEF Safety Assessment Report for STM-DK R03.00.10. The assessment report concludes: "*SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.00.10 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application…* *…There are no Application Conditions, no Reservations and one Recommendation in the present report* "

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
43.	SAR_R03.00.11	SINTEF 2017:00826	6.0	2019-02-19	The SINTEF Safety Assessment Report for STM-DK R03.00.11. The assessment report concludes: "*SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.00.11 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application…* *…There are no Application Conditions, no Reservations and one Recommendation in the present report* "
44.	SAR_R03.00.12	SINTEF 2017:00826	7.0	2020-11-23	The SINTEF Safety Assessment Report for STM-DK R03.00.12. The assessment report concludes: "*SINTEF sees nothing that speaks against approving the STM-DK Generic Application version 03.00.12 for use in specific applications provided the application rules and conditions in the Safety Case are fulfilled by the subsequent specific application…* *…There are no Application Conditions, no Reservations and one Recommendation in the present report* "
45.	SAR_R03.00.13	SINTEF 2017:00826	8.0	2021-04-08	The SINTEF Safety Assessment Report for STM-DK R03.00.13. The assessment report concludes: "*SINTEF sees nothing that speaks against approving the STM-DK 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…* *…There are no Application Conditions, no Reservations and one Recommendation in the present report* "
46.	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.
47.	SRSClar System Requirements Clarification	SyReqClarification	15 (base-line 14.0)	2021-07-14	This is a DOORS report that contains clarifications to the requirements in ref. [46]. It is to be regarded as a supplement to ref. [46]. SINTEF comments: The GASC refers to version 13 baseline 14.0, whilst received document is version 15 baseline 14.0. SINTEF assumes that this is a typing error in the Safety Case, and the assessment uses version 15 baseline 14.0 as basis for the assessment.

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
48. SwArchSpecGw Software Architecture Specification Gateway	G81001-X3107-U024-13	20 (base-line 11.0)	2021-10-15	This is a DOORS report that contains the software architecture specification for the software component "Gateway".
49. SwArchSpecZUB Software Architecture Specification ZUB123	G81001-X3107-U025-07	20 (base-line 6.0)	2021-10-22	This is a DOORS report that contains the software architecture specification for the software component "ZUB123".
50. 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. [58]). All tests were passed.
51. 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.
52. SwIntTstRepGw Software Integration Test Report Gateway	G81001-X3107-U034-25	28	2021-12-14	The document has been updated to version 28 for STM-DK R03.01.00 maintenance update, covering the Change Request CFX00517269. This is the report from the validation activities according to the Software Verification and Validation Plan (ref. [58]). 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 03.01.00 (ref. [66]).
53. SwIntTestRepZub Software Integration Test Report ZUB123	G81001-X3107-U035-15	15	2022-01-11	The document has been updated to version 15 for STM-DK R03.01.00 maintenance update. This is the report from the validation activities according to the Software Verification and Validation Plan (ref. [58]). All tests are passed. SINTEF comment: version 13 is referred in the Safety Case [2]. The document is updated for R03.01.00 in v15. SINTEF considers this to be a typing error.
54. SwIntTestSpecZub Software Integration Test Specification ZUB123	G81001-X3107-U027-07	07	2022-01-27	This is a DOORS report that defines the tests to be performed for integration of the ZUB123 software.
55. 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

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
56.	SwRelNote STM-DK Software Release Notes	G81001-X3107-L006-25	29	2022-01-03	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 R03.01.00 VE6 as the latest version. It states that R03.01.00 is the "*Latest validated version*". SINTEF comment: version 25 is referred in the Safety Case [2]. The document is updated for R03.01.00 in v29. SINTEF considers this to be a typing error.
57.	SwValRep Software Validation Report	G81001-X3107-U036-07	07	2022-01-17	A total of 5 rules and 2 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*."
58.	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. [30]).
59.	SyArchSpec System Architecture Specification	G81001-X3107-R004-19	20 (base-line 18.0)	2021-10-04	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. [47]) to the composition of architectural components which the STM-DK consists of.
60.	SyIntTstRep System Integration Test Report	G81001-X3107-U012-14	19	2022-01-11	The document has been updated to version 19 covering STM-DK R03.01.00 maintenance update, showing updated test results in chapter 3. SINTEF has verified that no new test result issues has been added with the STM-DK R03.01.00 maintenance update. This is the System Integration Test Report for STM-DK version 03.01.00. A number of tests failed or could not be performed. The corresponding requirements are all appropriately accounted for in the delta validation report SyValRep, ref. [66].

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
61.	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. [47]).
62.	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. [47]). It has been stated by Siemens that the valid document is G81001-X3107-U535-07
63.	MaintSafePl Maintenance Safety Plan STM Maintenance release R03.01	G81001-X3107-U410-02	02	2022-01-06	This Safety Plan defines the safety process relevant for maintenance upgrade of STM-DK R03.01 supporting new VE6 hardware and minor software improvements. The document is a add on to the existing safety plan [64] and does therefore only describe activities which are relevant for the maintenance upgrade, and which are not covered by the existing safety plan.
64.	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.
65.	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
66.	SyValRep System Validation Report	G81001-X3107-U010-05	05	2022-01-27	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. The components Gateway SW and Legacy ZUB123 SW have a separate software validation report that approves the correct behaviour of these components and confirms the operational use of the components. All other components are already assessed and are checked during the system integration tests. It is claimed that fulfilment of the requirements from the SRS Clarification (ref. [47]) 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 5 List of inapplicable requirements*".

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
67.	SyValRep_Delta_08 Delta System Validation Report	G81001-X3107-U547-08	08	2018-09-24	This is an updated document covering STM-DK R03.00.10, 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. [66]).
68.	SyValRep_Delta_09 Delta System Validation Report	G81001-X3107-U547-09	09	-	This is an updated document covering STM-DK R03.00.11 and R03.00.12, 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, 03.00.10, 03.00.11 and 03.00.12.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
69.	SyValRep_Delta_10 Delta System Validation Report	G81001-X3107-U547-10	10	2021-03-25	This is an updated document covering STM-DK R03.00.13, 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”.
70.	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.
71.	SySwMaintPl System and Software Maintenance Plan	G81001-X3107-U050-01	01	2021-09-30	This document describes the maintenance measures of the system STM-DK. This maintenance plan covers the requirements for maintenance measures as listed in EN50128:2011 Chap. 9.2. for changes of software on safe computer systems.
72.	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.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
73.	VerRep_03.01.00 Verification Report R 03.01.00 VE6, STM-DK Cert	G81001-X3107-U543-07	07	2021-12-14	This is an updated document covering STM-DK R03.01.00. 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. [60] and concludes "*It can be concluded, that the process leading to the released software R 03.01.10 has been in accordance with [EN 50128] concerning review, test and verification activities*". SINTEF comments: The conclusion state that the "…released software R 03.01.10…". However, the released software version is R03.01.00. SINTEF considers this to be a typing error.
74.	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.
75.	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.
76.	SyChngDesc System change description	G81001-X3107-U586-02	02	2022-01-10	System change description, Release 03.01.00 VE6 SINTEF comments: The Safety Case refers to version 01, whilst SINTEF has received updated version 02 of the document. SINTEF considers this to be a typing error in the Safety Case, and the assessment is based on version 02.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
77.	ConEval Consequence evaluation	G81001-X3107-U583-03	3.0	2022-01-07	The purpose of this “consequence evaluation” is to clarify if the changes will need a significance evaluation that might require involvement of specialist from Banedanmark and CSM-RA assessment. The evaluation concludes that: "*The STM-DK upgrade to R03.01.00 is according to the consequence evaluation in section 2 a change to the “railway system” and not safety related. Therefore, no CSM-RA assessment or significance evaluation is expected at the railway level.*"
78.	MOM_22120221	-	-	2021-12-22	STM DK Assessment, mail to Narve.Lyngby@sintef.no: 22.12.2021; 10:45 Presentation&mom, 22-12-2021.pdf
79.	TCC_Rel_4.1 Conditions of Use	A6Z00042980629/ PM1/000/A	A	2020-01-20	The purpose of this document is to fully describe TCC Release 4.1 to the extent that it refers to lower-level public documentation in the form of interfaces and also directly contains any additional information that may be missing. This missing information may be, for example, conditions from lower-level assessment reports.
80.	TCC_SYS_GUT Abschlussbericht zur Begutachtung des Systems "TCC 4.1"	A6Z00043606209/ PM2/000/A	-	2020-01-22	This inspection report considers all components of the overall TCC Rel. 4.1 system and deals with the requirements and restrictions as well as the interface conditions of these components. The report concludes that: "During the assessment, no deviations from the fulfillment of the goals and requirements regarding generic components of the standards EN 50128:2001 and EN 50129:2003 could be determined."
81.	SW_Inst_Proc	IN 655.00 Q5019	01.00	2022-01-31	This technical note describes the tools and process for updating the software of the STM-DK when installed in a vehicle and with VE6 in the subrack.
82.	Glossary	G81001-X3107-L002-01	-	2022-02-15	Glossary
83.	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.
84.	MR tra–n – STM-DK ver. 3–0 – Report for Safety Quality Test (SQT)	-	01.00	2017-01-12	The document describes the Safety Qualification Test performed with STM-DK baseline 3.0. Earlier Experience Gathering Operation (EGO) has been performed with STM-DK 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

Ref. Safety case ref. Document Name	Document Id.	Ver.	Date	Comment
				the railway authority Banedanmark and the Danish safety authority Trafikstyrelsen. The testing has been performed with trainset MR-4021 with STM-DK 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 STM-DK 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. 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".
85. LooP STM-DK R03.01	102026384-NOT-2021-01	2.0	02.03.2022	There are no remaining open points.
86. STM meeting 05.10.2021	-	-	05.10.2021	Presentation from STM meeting 05.10.2021.

Technology for a better society

www.sintef.no