Report

Safety Assessment Report

DK-STM Cubicle

Author(s):

Narve Lyngby

Report No:

2022:00579 - Restricted

Client:

Siemens Mobility A/S

SINTEF Digital
Postal address:
Postboks 4760 Torgarden
7465 Trondheim, Norway
Switchboard: +47 40005100
info@sintef.no

Enterprise /VAT No:
NO 919 303 808 MVA

Report

Safety Assessment Report

DK-STM Cubicle

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

VERSION
1.0

DATE
2022-06-29

AUTHOR(S)
Narve Lyngby
Ulrik Johansen

CLIENT(S)
Siemens Mobility A/S

CLIENT'S REFERENCE
Peter Bomholt

PROJECT NO.
102026384

NO. OF PAGES/APPENDICES
26

SUMMARY
Siemens Mobility A/S has engaged SINTEF as an independent safety assessor ("ISA") for the DK-STM Cubicle project. The changes concerning the upgrade for DK-STM Cubicle from VE5 to VE6, including updated standards, have been described in a separate Safety Note for STM-DK Cubicle VE6. This Safety Note, including referenced documentation, has been assessed. It relies also on the existing GASC for the DK-STM cubicle, which has been assessed by SINTEF.

SINTEF has the impression that the submitted safety documentation provides the correct status of the safety condition of the STM-DK Cubicle VE6. SINTEF has not found any evidence to the contrary that the system can be used as a SIL 4 system in accordance with CENELEC EN 50126-1:1999 and EN 50129:2003, and finds that the safety and quality management and technical safety are taken care of in the project.

In the opinion of SINTEF, the submitted safety documentation provides a basis for recommending that the STM-DK Cubicle VE6 can be used for future specific applications.

PREPARED BY
Narve Lyngby

SIGNATURE

CHECKED BY
Robert Bains

SIGNATURE

APPROVED BY
Maria Bartnes

SIGNATURE

REPORT NO.
2022:00579

ISBN
-

CLASSIFICATION
Restricted

CLASSIFICATION THIS PAGE
Restricted

Document history

VERSION	DATE	VERSION DESCRIPTION
1.0	2022-06-29	This is an update of SINTEF report F27049 version 1.0.1 based on updated safety documentation. The document number is changed from SINTEF F27049 to 2022:00579. For technical reasons, the version of the document is identified as 1.0 instead of 2.0. For the change history of previous versions see the change log in SINTEF F27049 version 1.0.1.

Table of contents

APPENDICES

None

1 Introduction

Siemens Mobility A/S has engaged SINTEF as an independent safety assessor ("ISA") for the project STM-DK Cubicle VE6 update.

The DK-STM is based on standard modules from the Siemens TCC platform and housed in a standard 19" subrack. The subrack is, however, not suitable for mounting on-board and there are application conditions that require an enclosure and filtering of supply voltage. Therefore, a cubicle for housing the STM-DK has been developed.

In the STM-DK Cubicle (G81002-E3134-H024 + H072 + H110), the STM-DK Subrack (G81002-E3135-H024+ H110) is used as the active part. Until now, the CPU-board in the STM-DK Subrack (G81002-E3134) was VE5 (S25391-B90-X23-.*). Due to obsolescence, VE5 will be replaced by VE6 (S25391-B90-X26-.*), ref. [48].

Previous versions of STM-DK Cubicle have been assessed in ref. [42] and ref. [40]. The report ref. [42] was valid for STM-DK Cubicle with VE5 CPU-board. Due to two updated documents being part of the STM DK Cubicle Safety Case which relates to the update of DK-STM Generic Application Software to version 03.00.09, an updated assessment was performed by SINTEF in ref. [40]. The STM-DK Cubicle with VE6 CPU-board is considered by Siemens as a minor update. It is stated that the original STM-DK Cubicle SRS (ref. [34]) has not changed, therefore there are no new customer requirements. The Safety Note (ref. [48]) therefore focus on the impact of changed legislation/standards and the impact of using the CPU board VE6 instead of VE5. Hence; the Safety Note (ref. [48]) addresses if relevant standards/regulation have changed respectively if the VE6 complies with the updated requirements. It is noted that the changes made to this report concerning the STM-DK Cubicle with VE6 CPU-board update are fully covered by updates made in this section, chapter 2, the new section 3.7, the Assessment chapter 4, and the References chapter 5.

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 of the quoted text is omitted.

The word chapter is used to reference parts of the safety case documents; the word section is used to reference parts of this report.

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

Acceptable
If an assessed claim is substantially (or fully) compliant with the requirements in the standards and can achieve the intended effect it is deemed acceptable.

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:
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*".

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 will be 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. [3])
EN 50126-1:2017	Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) (ref. [56])
EN 50129:2003	Railway applications - Safety related electronic systems for signalling (ref. [4])
EN 50129:2018	Railway applications - Safety related electronic systems for signalling (ref. [57])

These require a structured safety case as a foundation for an assessment. The assessor's task is according to EN 50129 (ref. [57]) the "*...process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the product is fit for its intended purpose in relation to safety* ".

The Safety Note (ref. [48]) refers to "old" version of EN 50126 (1999). It is stated in the Safety Note (ref. [48]) that EN50126:2017 is only required "*to the extent and insofar as existing systems are being modified*". Siemens has further stated that as the replacement of VE5A with VE6 in the STM-DK Subrack, is the only update for the STM-DK Cubicle, it is also considered a maintenance update of the STM_DK Cubicle, not a modification/extension.

The Safety Note (ref. [48]) refers to "old" version of EN 50129 (2003). Siemens refers in the Safety Note to chapter 1 in EN 50129:2018 (ref. [57]), 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*". The Safety Note (ref. [48]) also states that the replacement of VE5A with VE6 in the STM-DK Subrack, is the only update for the STM-DK Cubicle, it is also considered a maintenance update of the STM_DK Cubicle, not a modification/extension, and that it is not safety relevant. SINTEF does, however, consider this to be a modification, but finds the handling by Siemens to be tolerable.

2.1 SINTEF's assessment procedure

SINTEF has examined documentation that Siemens AS 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. [5]) which was contractually agreed with Banedanmark and approved by the national safety authority Trafikstyrelsen.

The documents have been submitted as PDF or 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 can accept that for the majority of the documents electronic signatures are indicated.

The assessment starts with the safety case for the DK-STM cubicle project (ref. [1] plus [2] and [37]) and the present report assumes that the reader is familiar with the safety case.

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

3 The Safety Case for DK-STM cubicle

The preliminary version of the safety case (assessed in the previous version of this report) contained a number of "*Conditions*" which correspond to reservations in the sense of this report. The current version of the safety case documents acceptable closure of most of them; those that are not closed are retained as application conditions.

SINTEF considers this to be acceptable.

3.1 Definition of System

EN 50129, clause 5.1 states:

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

An overall description of the DK-STM cubicle is given in chapter 1 of the safety case (ref. [1]) and reference is made to the system description (SysDes_cubicle ref. [36]). The documents that have been produced within the scope of the DK-STM project are identified with their versions in the document list (DocList, ref. [13]) and the cubicle specific drawings are listed in the drawings list (DocList_cubicle ref. [14])

SINTEF therefore considers the definition of system to be acceptable.

3.2 Quality Management Report

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

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

The quality management report refers to the DK-STM generic application safety case (GASC_Cert ref. [16]) for details and only addresses cubicle specific activities.

Reference is made to the cubicle specific requirements in the quality assurance plan (QaPl ref. [27]) and lists the status of the cubicle specific quality goals. Two are still pending; they relate to documentation and are not considered to be safety critical.

SINTEF considers this to be acceptable.

3.3 Safety Management Report

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

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

The safety management report addresses all these points.

SINTEF considers this to be acceptable.

3.3.1 Safety life cycle

EN 50129, clause 5.3.2 states:

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

It is stated that the project spans phases 1 through 7 of the CENELEC lifecycle. In addition, the installation and maintenance manuals (InstMan_cubicle ref. [21] resp. MaintMan_cubicle ref. [25]) have been prepared for future phases.

SINTEF considers the safety life cycle to be acceptable.

3.3.2 Safety organisation

EN 50129, clause 5.3.3 states:

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

The safety organisation is a part of the project organisation, which is documented in Organisation and Documentation of Personnel Competence (OrgComp ref. [26]). The validator is independent of the project manager.

SINTEF considers the safety organisation to be acceptable.

3.3.3 Safety Plan

EN 50129, clause 5.3.4 states:

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

Reference is made to the cubicle specific Safety Plan (SafePln_cubicle ref. [32]) which fulfils the applicable requirements for a safety plan as stated in EN 50126 and EN 50129 and is considered suitable for its intended use.

SINTEF considers the safety plan to be acceptable.

3.3.4 Hazard log

EN 50129, clause 5.3.5 states:

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

EN 50126, clause 6.3.3.3 requires:

"*Hazard Log shall include details of:*

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

Reference is made to the hazard log, which has been established in the SharePoint site. Reference is made to the description of the use of the hazard log (HazLog, ref. [17]).

A hazard log report has been submitted (HazLogRep ref. [18]) that reports the status of "*safety relevant entries*" in the ClearQuest database as per 2015-08-26. All hazards are "*Resolved*" or "*Closed*".

SINTEF considers this to be acceptable.

3.3.5 Safety requirements specification

EN 50129, clause 5.3.6 states:

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

Reference is made to the DK_STM GASC (GASC_Cert ref. [16]) and the hazard workshop report (RiskAn_cubicle ref. [31]).

SINTEF considers the safety requirements specification to be acceptable.

3.3.6 System Design

EN 50129, clause 5.3.6 states:

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

The system has been designed according to the V-model supported by the EN 50126 and EN 50128 standards. This has been ensured through the support of the model in the PEACC+ process. Reference is

made to the requirements specification (SRS_cubicle ref. [34]) and the hardware design specification (DesSpec_cubicle ref. [12]) and the Application rules (AppRule_cubicle, ref. [8]).

It is mentioned that the installation and maintenance manuals will be updated to include adjustments due to application rules and a reservation "*#COND-Cubicle STM-DK GASC-003#*" is given that addresses this.

It is stated that "... *DK-STM must successfully pass a number of qualification tests. This is already stated in [GASC_Cert]. The tests are not part of the cubicle project but the results will also verify the correct cubicle functionality.*"

SINTEF considers this to be acceptable.

3.3.7 Safety verification and validation

EN 50129, clause 5.3.9 states:

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

Safety verification and validation is considered to be an integrated part of the verification and validation processes carried out in the DK-STM project as described in the DK-STM GASC (GASC_Cert ref. [16]).

SINTEF considers the safety verification and validation to be acceptable.

3.3.8 Safety Justification

EN 50129, clause 5.3.10 states:

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

The justification of adequate safety for the DK-STM cubicle is provided in the GASC for the STM cubicle (ref. [1]).

SINTEF considers the safety justification to be acceptable.

3.3.9 System handover

EN 50129, clause 5.3.11 states:

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

Within the frame of the DK-STM project the handover to the customer is specified in chapter 3.9 in the safety management report. Reference is made to the user documents (AppRule_cubicle ref. [8], InstMan_cubicle ref [21], SysDes_cubicle ref. [36] and MaintMan_cubicle ref. [25]).

SINTEF considers the system handover to be acceptable.

3.3.10 Operation and maintenance

EN 50129, clause 5.3.12 states:

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

The safety management report makes reference to the maintenance manual (MaintMan_cubicle ref. [25]).

SINTEF considers this to be acceptable; see also section 3.3.6.

3.3.11 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 "*There are no special requirements concerning decommissioning and disposal*".

SINTEF considers this to be acceptable.

3.4 Technical Safety Report

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

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

These points are all addressed in the technical safety report (TSR_cubicle ref. [37]).

Since the TSR does not address the validator's findings (in ValRep_cubicle, ref. [39]) they are addressed in the safety case. All three are acceptably closed.

3.4.1 Introduction

EN 50129, clause 5.4 states:

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

The TSR (TSR_cubicle ref. [37]) does not contain an overview description of the design; an overview is, however, included in the definition of system (see section 3.1 in this report). The technical safety principles are also indirectly identified in the definition of system.

SINTEF considers this to be tolerable.

3.4.2 Assurance of correct functional operation

EN 50129, clause 5.4 states:

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

Assurance of correct functional operation is separated into different parts in the technical safety report as summarised in the following:

System architecture is shown through the following Figure 1:

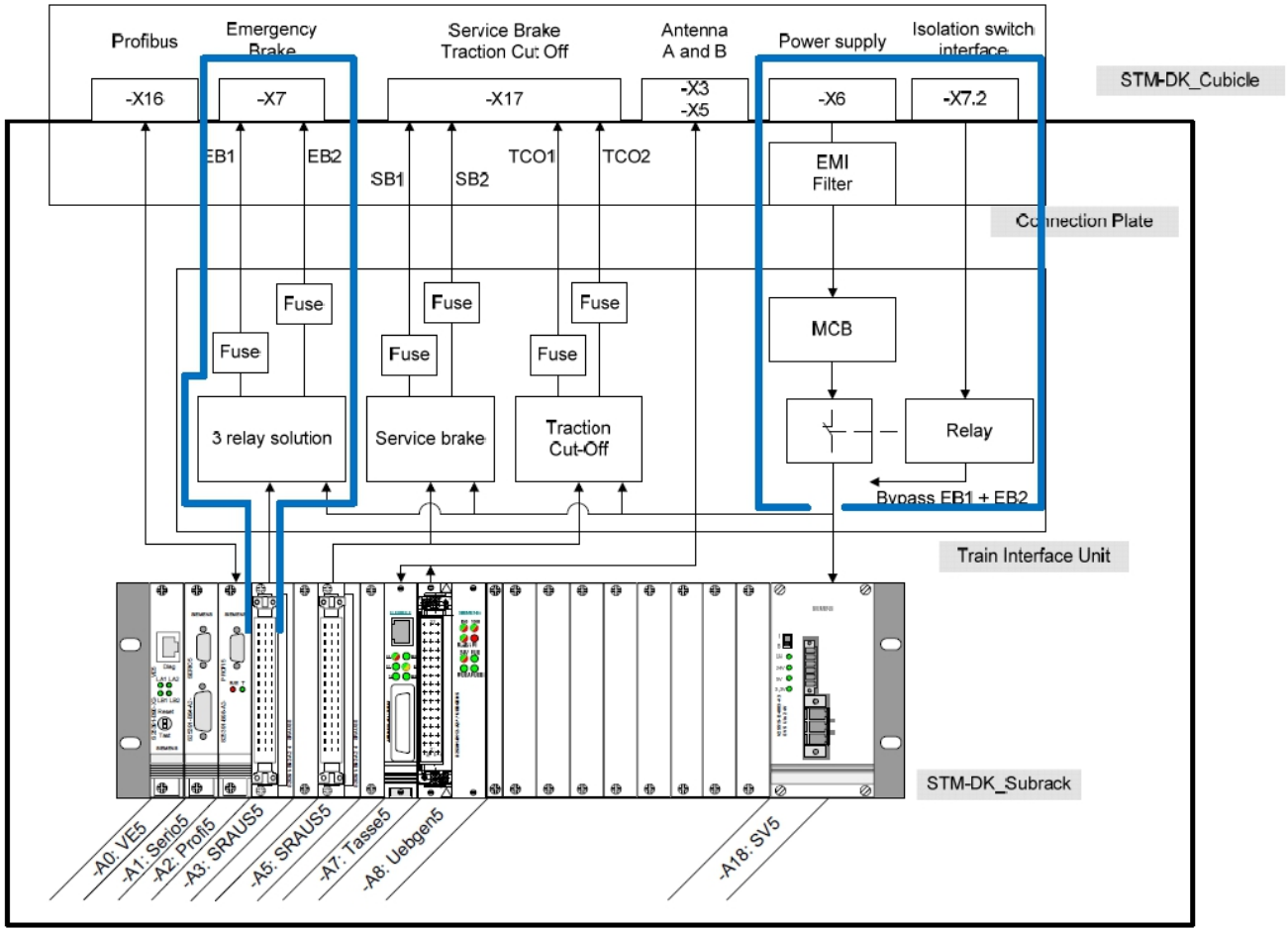

Figure 1 Overview of the DK-STM cubicle (from ref. [37])

The blue lines delimit the safety related parts.

Definition of interfaces identifies man-machine interfaces as outside the scope of the TSR, and internal and external system interfaces (identified as "-Xn" in Figure 1 above).

Fulfilment of System Requirements Specification (SRS_cubicle, ref. [34]) is shown in the validation report (ValRep_cubicle, ref. [39]).

Fulfilment of the Safety Requirement Specification (SRS_cubicle, ref. [34] and RiskAn, ref. [31]) is demonstrated in the validation report (ValRep ref. [39]).

Assurance of correct hardware functionality makes reference to the DK_STM GASC (GASC_Cert ref. [16]) and is demonstrated in the validation report (ValRep ref. [39]).

Assurance of correct software functionality is not relevant because the DK-STM cubicle does not contain software.

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.*"

For effects of faults FMEAs are given for each of the safety related parts of the cubicle (see blue boundaries in Figure 1). Independence of items is demonstrated through detailed calculations. Detection of single faults is covered by the FMEAs. For effects of multiple faults a fault tree analysis is included. The resulting failure rates are within the limits for SIL 4.

SINTEF considers the effects of faults to be acceptably handled.

3.4.4 Operation with external influences

EN 50129, clause 5.4 states:

"*This section shall demonstrate that when subjected to the external influences defined in the System Requirements Specification, the system/sub-system/equipment*

- *continues to fulfil its specified operational requirements,*
- *continues to fulfil its specified safety requirements (including fault conditions).*"

Operation with external influences is covered by the environmental testing ("*STM-DK_Cubicle_TYP_TEST_REPORT_ENVIRONM*" = EMC_Test, ref. [15]).

SINTEF considers operation with external influences to be acceptably handled.

3.4.5 Safety-related application conditions

EN 50129, clause 5.4 states:

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

Safety-related application conditions from the DK-STM subrack that are applicable to the cubicle have been transferred to the application rules for the cubicle (AppRule_cubicle, ref. [8]). Their handling is described in the attachment to the safety case (ref. [2]) although this is neither mentioned in the safety case (ref. [1]) nor the TSR (ref. [37]).

SINTEF considers this to be tolerable.

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 section 6 demands safety qualification tests as described in Annex B.6 (normative). Section B.6.1 describes the requirements:

"*The extent and duration of the Safety Qualification Tests shall be agreed between the railway authority and the safety authority, and shall be justified having regard to the degree of novelty and complexity associated with the system/sub-system/equipment.*

Because completion of the Safety Qualification Tests is contained within the Safety Case, the safety of the system is not fully assured during the test period. Therefore appropriate precautions, procedures and monitoring shall be provided, to ensure safety of the railway during the test period..."

Safety qualification tests "*will be part of supervised test operation of specific applications*".

SINTEF considers this to be acceptable.

3.5 Related safety cases

EN 50129, clause 5.1 states:

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

Reference is made to the DK-STM GASC (GASC_Cert ref. [16]). The SRACs coming from that safety case are all covered by application rules. See also section 3.4.5.

SINTEF considers the handling of safety related application conditions 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 DK-STM project states:

"This GASC demonstrates that the DK-STM when mounted in the cubicle is sufficiently safe provided that the accompanying safety related conditions are fulfilled, [AppRule_cubicle]" (ref. [8]) and recapitulates the application conditions that are mentioned in the safety case.

SINTEF considers the conclusion to be acceptable

3.7 DK-STM Cubicle update from version VE5 to version VE6

This section covers the safety assessment related to the DK-STM Cubicle update from version VE5 to version VE6, including updated standards as specified in the Safety Note (ref. [48]).

A separate Safety Note VE6, ref. [48], has been performed. This Safety Note addresses if relevant standards/regulation have changed and if the STM-DK Cubicle is fulfilling the requirements. The original STM-DK Cubicle SRS (ref. [34]) has not changed, therefore there are no new customer requirements. It is therefore stated in the safety note that it will focus only on the impact of changed legislation/standards and the impact of using the CPU board VE6 instead of VE5. The following are discussed:

- Environmental (mechanical, climatical and EMC/Radio)
- Misc standards (EN 50155 and EN 45545-2)
- GASC (ref. [1]) and application rules (ref. [50])

The Safety Note describes the possible changes in the environmental conditions, either due to the requirements from legislation/standards have been updated since the STM-DK Cubicle was developed or to using VE6 instead of VE5. Mechanical, Climatical and EMC/Radio requirements are discussed. The Safety Note further argues for the fulfilment of updated standards, and refer to Type Test Certificate for components of the basis system Train Control Computer (TCC) (ref. [53]) and Internal typetest Temperature test with VE6 (ref. [51]). SINTEF considers this to be acceptable.

The rolling stock standard for electronic equipment, EN 50155, has changed from EN 50155:2007 to EN 50155:2017. There is also an EN 50155:2021 edition, but as the STM-DK Subrack adheres to EN 50155:2017, this version is therefore also chosen by Siemens for the STM-DK Cubicle. Moreover, it is stated that as the design was done in 2015, the design (process) cannot retrospectively be changed. Installation requirements

are only considered by Siemens where relevant. The Safety Note compares the EN 50155:2007 to EN 50155:2017 and argues for compliance of EN 50155:2017. The conclusion reads: *The STM-DK Cubicle complies therefore to the (changed) EN50155 requirements*.

SINTEF considers this to be acceptable.

The Safety Note addresses the GASC, consisting of the main GASC (ref. [1]) and an attachment to the GASC (ref. [2]), and the conditions from the GASC:

> *#COND-Cubicle STM-DK GASC-001#: In case a new version of the DK-STM generic application is created the accompanying application rules for installation must be analysed in order to reveal differences. If differences are found it must be proven that the safe use of the cubicle is unaffected.*
>
> *New application rules have been created by the DK-STM generic application. These are analyzed in this safety note, see section 4.2.*

This is considered acceptable by SINTEF, see also below.

> *#COND-Cubicle STM-DK GASC-002#: Changes to the cubicle affecting specifications, performance or application rules must trigger a new version of this GASC*
>
> *As the VE6 update is only a minor change, this safety note is written instead.*

This is considered acceptable by SINTEF.

> *#COND-Cubicle STM-DK GASC-003#: Rules and directions for installation and maintenance prescribed in document [AppRule_cubicle] must be observed.*
>
> *The installation and maintenance documentation will be updated.*

Updated installation and maintenance manuals (ref. [54] and [55]) have been delivered and are referred in the updated Safety Note version B (ref. [48]). SINTEF considers this to be acceptable.

> *#COND-Cubicle STM-DK GASC-004#: SRACs exported to testing, to Banedanmark, to the EVC provider (via Banedanmark) and to the specific application via the document [AppRule_cubicle] must be observed*
>
> *Application rules are analyzed in this safety note, see section 4.2.*

This is considered acceptable by SINTEF, see also below.

For the TSR (ref. [37]) it is in the Safety Note stated that:

1) *VE5 is mentioned instead of VE5/VE6, but this has no impact on the content.*
2) *A hazard workshop (ref [52]) for the use of VE6 instead of VE5 has been held.*
   The increased internal temperature due to VE6 was discussed, and it was agreed that the proposed mitigation to sharpen the installation requirements as stated in section 2.2 and 4.2, was a good solution.
   No new hazards were found.
3) *Change in environmental conditions, e.g. in EMC and temperature is handled in section 2.*
4) *The THR has not changed, as the THR for the LRU STM-DK Subrack is the same with VE5 and VE6. The other components in the STM-DK Cubicle have not changed*.

Annex 7.1 in the Safety Note, new or changed rules originating from STM-DK Subrack Application Rules version 10 [STMDKR_APPR10] have been analysed. The analysis shows if the new or changed rules should be used (forwarded or reworded) in the STM-DK Cubicle application rule document or not. A table is also provided in section 4.2 of the Safety Note, shows the changed and new rules originating from STM-DK Subrack Application Rules version 10 (ref. [49]), and how they shall be used, if relevant in the STM-DK Cubicle Application Rule document, version C (ref. [50]).

Concerning the updated Application rules, SINTEF has reviewed the updated STM-DK Cubicle Application rules, ref. [50]. Based on the analysis in annex 7.1 in the Safety Note, SINTEF has not identified any inconsistencies between the updated Application rules for DK-STM GASC Software in relation to the corresponding updates made for the STM-DK Cubicle.

The safety analysis Safety Note VE6, ref. [48], concludes that the STM-DK Subrack with VE6 can be used in the STM-DK Cubicle, when using the sharpened installation requirements as stated in application rule APPRU_228.

SINTEF endorses the referenced documentation of the DK-STM Cubicle VE6 with respect to the assessment of the safety, having no additional comments related to the completeness and correctness of the referenced documentation.

4 Assessment

The changes concerning the upgrade for DK-STM Cubicle from VE5 to VE6, including updated standards, have been described in a separate Safety Note for STM-DK Cubicle VE6, ref. [48]. This Safety Note, including referenced documentation, has been assessed. It relies also on the existing GASC for the DK-STM cubicle, which has been assessed in ref. [42] and ref. [40].

SINTEF is confident that the submitted safety documentation provides the correct status of the safety condition of the STM-DK Cubicle VE6.

SINTEF has not found any evidence to the contrary that the system can be used as a SIL 4 system in accordance with CENELEC EN 50126-1:1999 and EN 50129:2003, and finds that the safety and quality management and technical safety are taken care of in the project.

In the opinion of SINTEF, the submitted safety documentation provides a basis for recommending that the STM-DK Cubicle VE6 can be used for future specific applications.

4.1 Application conditions, Reservations and Recommendations

There are no application conditions, reservations or recommendations in this report.

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 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; the list is sorted in alphabetical order of the acronyms.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	date	Comment
[1]	-, GASC for the STM Cubicle	G81002-E3134-U002-B	B	2015-10-06	Assessed in this report.
[2]	-, Handling of SRACs in the cubicle project	G81002-E3134-U002B Attachment	-	2015-10-06	This is an attachment to the safety case that is not referenced in the safety case; see also section 3.4.5. It describes how SRACs are handled and which ones are passed to Banedanmark , the EVC provider (via Banedanmark), testing or the specific application. The remaining application conditions are closed by design or modified and redirected to new application conditions.
[3]	EN 50126, Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	EN50126-1		Sep 1999	These are the standards against which the assessment has been performed. They require a structured safety case as a basis for assessment. Since the cubicle doesn't involve software, EN 50128 is not applicable.
[4]	EN 50129, Railway Applications – Safety Related Electronics Systems for Signalling	EN50129		Feb 2003	
[5]	-, Prosjekttilbud Assessment for dansk STM	90513001-STMDK	1.0	2007-12-07	This contains a description of the assessment activities to be performed during the project. It is included as an integral part of the contract between Banedanmark and SINTEF and has been accepted by Trafikstyrelsen as an adequate assessment plan.
[6]	- Safety Assessment Report STM-DK Generic Application (Baseline 3.0) version 03.00.07	SINTEF F27264	1.0	2015-10-30	This is the assessment report of ref. [16]. It concludes "*SINTEF sees nothing that speaks against approving that the STM-DK generic application version 03.00.07 for use in specific applications provided the application conditions in the safety case are fulfilled by the specific application.*"
Safety Case References					
[7]	AppRule, Application Rules	G81001-X3107-L005-07	07	2015-03-11	The reference given in the safety case is evidently a file path; the file that has been submitted contains the document that is commented here. The document states the rules that must be followed to use the DK-STM 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.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	date	Comment
[8]	AppRule_cubicle Application rules	G81002-E3134-L001-A	A	2015-06-22	The document states the rules that must be followed to use the DK-STM cubicle in safety related train installations. The rules are classified according to categories that indicate where they shall be applied: • EVC requirements • Installation manual • Maintenance manual • Qualification test • Specific application.
[9]	BOM_CUB110V STM Cubicle 24 VDC, Stykliste	G81002-E3134-L111-A	A	2015-06-12	This is a Bill of Material for the 110 Volt cubicle.
[10]	BOM_CUB24V STM Cubicle 24 VDC, Stykliste	G81002-E3134-L025-A	A	2015-06-11	This is a Bill of Material for the 24 Volt cubicle.
[11]	BOM_CUB72V STM Cubicle 24 VDC, Stykliste	G81002-E3134-L073-A	A	2015-06-11	This is a Bill of Material for the 72 Volt cubicle.
[12]	DesSpec_cubicle Hardware Architecture and design specification	G81002-E3134-R002-A	A	2015-09-04	This document describes how the requirements in the hardware design specification (ref. [34]) will be fulfilled. It addresses • Architecture overview • General design considerations • Design considerations for sub-circuits • Fulfilment or requirements • Application rules • Preliminary Bill of materials
[13]	DocList, Document List and Document Control	G81001-X3107-L001-05	05	2015-03-16	This is a complete list of documents produced in the project, including their actual version and release status.
[14]	DocList_cubicle, Tegningsnr-oversigt	G81002-X3134	-	2015-10-06	This is an Excel file containing a list of drawings produced for the cubicle.
[15]	EMC_Test EMC immunity test of DK-STM Cubicle	T211144-1	-	2015-07-01	This is the finalised EMC test report. It confirms that all tests have been passed and concludes "*The test object ... meets the requirements of the standard ... EN 50121-3-2:2006 ...*".
[16]	GASC_Cert GASC	G81001-X3107-U405-05	05	2015-08-28	This is the generic application safety case for the baseline 3.0 version of the STM with software version 03.00.07. It has been assessed by SINTEF; see ref. [6].
[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 2015-06-15 from ClearQuest DK-STM project	-	-	2015-06-15	This is a report of hazards in the ClearQuest database; see also section 3.3.4 in this report. All hazards are "*Resolved*" or "*Closed*"

Ref.	Safety case ref. Document Name	Document Id.	Ver.	date	Comment
[19]	HazWorkshpCubicle STM-DK Cubicle Hazard workshop report after design	G81002-E3134-U004-A	A	2015-06-24	This is a report from a hazard workshop based on a manufactured prototype of the cubicle. No new hazards were identified, but a number of enhancements were identified that would further reduce the likelihood of cables breaking, falling out or connecting with a wrong position.
[20]	InstMan, DK-STM Installation Manual	IN 655.00 Q2962	1.07	2015-02-22	This is the installation manual for installing the DK_STM as an add-on to an ETCS system. It addresses • General rules and procedures • Electric interfaces and diagrams • Configuration of DK-STM • Functional test • Diagnosis
[21]	InstMan_cubicle, DK-STM Installation Manual	IN 655.00 Q4432	2.00	2015-04-23	This is the installation manual for installing the DK_STM cubicle. It addresses • Mechanical installation • Electric interfaces • Accessories • Coding of multi connectors at DK-STM cubicle • Installation of DTM-DK in vehicles without DK-ATC
[22]	ISO9001cert Siemens A/S ISO 9001 approval Certificate	CPN0002463	-	2014-07-10	This is a certificate of approval of the management system of Siemens A/S, Ballerup, according to ISO 9001:2008, ISO 14001:2004 and OHSAS 18001:2007. It is valid until 2016-08-27.
[23]	KS_Checkliste Quality Chekliste	G81001-X3107-L007-01	01.06	2012-03-29	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.
[24]	MaintMan DK-STM Vedligeholdsmanual	VN 655.00 Q2961	1.03	2015-02-22	This is the maintenance manual for DK-STM. 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
[25]	MaintMan_cubicle Vedligeholdsmanual cubicle	VN 655.00 Q4433	2.00	2015-04-21	This is the maintenance manual for DK-STM cubicle. It addresses • Maintenance o including competency of personnel, tools, repair etc. • Diagnosis via PC • Appendices o Maintenance form sheet o Error reporting form sheet o Error detection, power supply o Error detection, Profibus connection o Cubicle error detection guide

Ref.	Safety case ref. Document Name	Document Id.	Ver.	date	Comment
[26]	OrgComp, Organisation and Documentation of Personnel Competence	G81001-X3107-U404-04	04	2014-04-14	The Organisation and Documentation of Personnel Competence for the DK-STM project. This document documents the competence of everyone participating in the DK-STM certification project, including the mapping of roles in the project with standard roles according to what is required, and shows the project organisation.
[27]	QaPl, Quality assurance plan	G81001-X3107-U400-02	02	2015-04-15	*This quality assurance plan ...:* - *Applies to all activities within the framework of the project's quality assurance that are to be carried out at the system | hardware level and at the software level during the certification.* - *Is valid for all staff members and organisational units participating in the project.* - *Is valid for the whole duration of the project* *This document is intended to ensure the definite scheduling of those measures, methods, tools, responsibilities, supplier QA measures, verifications and resources required for the compliance with the normative requirements for quality assurance in the project.*"
[28]	RMPlan RM-Plan Guide	A6Z00002541903	D	2013-12-27	This is a DOORS report that contains the requirement management guideline. It addresses • Work Products of Requirements Management • Traceability • Test and Validation of Requirements • Structures in DOORS • Corresponding Topics
[29]	RamProofCubicle RAM demonstration	G81002-E3134-U0008-A	A	2015-09-17	This is a document that demonstrates fulfilment of the specified RAM requirements. The RAM requirements are recapitulated in the document and detailed RAM calculations are included. All RAM requirements are fulfilled.
[30]	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.
[31]	RiskAn_cubicle Hazard workshop report after design	G81002-E3134-U004-A	A	2015-06-24	This is the report from a walk-through of the physical construction of the cubicle in order to detect eventual causes of new hazards that might require a change in design. No new hazards were detected, but some enhancements were identified.
[32]	SafePln_cubicle, Safety Plan for DK-STM Cubicle project	G81002-E3134-U001-A	A	2015-09-24	This is the safety plan for the cubicle project. It defines the process for specification, design and production of the DK-STM cubicle. The plan fulfils the applicable requirements for a safety plan as stated in EN 50126 and EN 50129. SINTEF considers the safety plan to be acceptable.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	date	Comment
[33]	SRS BDK_SRS30 SRS ZUB123-STM issue 14 based on UNISIG SRS Baseline 3	G81001-X3107-R243-15 Released	15	2015-03-31	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. SINTEF notes that the document's title page still identifies it as "*Issue 14*" and "*Version 12.0*". This is due to a typing error in the Doors module, but the page footer correctly identifies the issue as 15 and the change log identifies the date and changes for issue 15. SINTEF considers this to be tolerable.
[34]	SRS_cubicle Hardware Requirement Specification	G81002-E3134-R001-B	B	2015-04-03	This document specifies the requirements for the 3 cubicle variants (24VDC, 72VDC and 110VDC). Each requirement is contained in a dedicated textbox "*with a notation as #REQ-RS_STM-DK-Cubicle/Subitem/Category-"running number"#*". The requirements are grouped by "*Subitem*".
[35]	SyRamPl, 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 cis is a DOORS report that 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 Requirement Specification (SRSClar).
[36]	SysDes_cubicle, STM-DK_ cubicle System description	KN 655.00 Q4434	2.00	2015-04-23	The System Description for the DK-STM cubicle. The document is written in English language and specifically covers the aspects: • General design o Mechanical o Electrical • Description of interfaces o Antenna A o Antenna B o Power supply o Emergency brake o Isolation switch function o Profibus (EVC) o Service brake and traction cut-off • Dimensions • Connection plate
[37]	TSR_cubicle, Technical Safety Report, STM-DK cubicle	G81002-E3134-U006-B	B	2015-09-29	Assessed in this report (see section 3.4).
[38]	Type_test_cubicle_int STM-DK Cubicle, Type test, internal	G81002-E3134-U010-A	A	2015-03-10	This document contains the results of internal type tests that have been performed. The tests distinguish the three different types of cubicle (24V, 72V and 110V) except where they are identical (e.g. internal wiring).

Ref.	Safety case ref. Document Name	Document Id.	Ver.	date	Comment
[39]	ValRep_cubicle Validation Report DK-STM Cubicle	G81002-E3134-U020-B	B	2015-10-08	This is the validation report for the DK-STM cubicle. It lists the status of the requirements as specified in ref. [34]. A few requirements could not be validated; they result in a total of 3 validation conditions which must be addressed in the safety case (ref. [1]).
[40]	Assessment of updated STM-DK Cubicle documentation	102004427-KOR-2018-05	1.0	2018-08-31	SINTEF assessment of two documents STM-DK Cubicle Application rules, ref. [44], and the DK-STM Cubicle Installation Manual, ref. [45]. Based on the review of the above referenced documentation, SINTEF's conclusion is that the existing Safety Cases for the STM DK Cubicle, ref. [1], and Application Design for installation in trains, ref. [41], and their corresponding safety assessments, refs. [42] and [43], are considered still to be valid with the updated DK-STM GASC Software version 03.00.09, ref. [46]. There are no additional conditions with this assessment.
[41]	ADSC LITRA MF	G81002-F3123-U004	C	2016-06-06	-
[42]	Safety Assessment Report – DK-STM Cubicle	SINTEF F27049	1.0	2015-10-30	-
[43]	Safety Assessment Report – ADSC LITRA MF	SINTEF F27638	2.0	2016-07-07	-
[44]	STM-DK Cubicle – Application rules	G81002-E3134-L001	B	2017-12-15	-
[45]	DK-STM Cubicle – Installation Manual	IN 655.00Q4432	3.0.2	2017-11-20	-
[46]	DK-STM GASC Software	G81001-X3107-U405	07	2017-12-01	-
[47]	SafetyNote_16	54CO 00735	01	2017-12-21	-
Added new references related to the DK-STM Cubicle VE6					
[48]	STM-DK Cubicle Safety Note, VE6	G81002-E3134-U015	B	2022-06-22	This Safety Note addresses if relevant standards/regulation have changed and if the VE6 is fulfilling the requirements. The original STM-DK Cubicle SRS (ref. [34]) has not changed, therefore there are no new customer requirements. It is therefore stated in the safety note that it will focus only on the impact of changed legislation/standards and the impact of using the CPU board VE6 instead of VE5. The Safety Note is assessed in the report at hand.
[49]	DK-STM Application Rules	G81001-X3107-L005-10	5.0	2022-01-27	The document states the rules that must be followed to use the DK-STM cubicle in safety related train installations.
[50]	STM-DK Cubicle – Application rules	G81002-E3134-L001	C	2022-03-30	The document states the rules that must be followed to use the DK-STM cubicle in safety related train installations. The rules are classified according to categories that indicate where they shall be applied: • EVC requirements • Installation manual • Maintenance manual • Qualification test Specific application.
[51]	STM-DK Cubicle Internal type test Temperature test with VE6	G81002-E3134-U012	A	2022-05-09	Temperature test on the STM-DK Cubicle using a VE6 instead of VE5.

Ref.	Safety case ref. Document Name	Document Id.	Ver.	date	Comment
[52]	STM-DK Cubicle Hazard Workshop VE6/2022-1	G81002-E3134-U016	A	2022-04-08	This note describes the outcome of a hazard identification workshop for upgrading the STM-DK Cubicle with a STM-DK Subrack using VE6 instead of VE5 carried out 2022.03.16 at Siemens, Ballerup. The result of the workshop was one finding: *Increased internal temperature in the STM-DK Cubicle, due to increased power consumption of VE6.* *Safety measure* *1. New application rule for sharpening of the installation requirements.* *2. Update installation manual* *3. Update maintenance manual* *=> the STM-DK Cubicle(VE6) is compliant to be installed in an environment with a max ambient temperature of max 40° C.*
[53]	Type Test Certificate	A6Z00001275102/PM2/000/Q	-	2021-07-01	Type Test Certificate for components of the basis system Train Control Computer (TCC).
[54]	DK-STM Cubicle Installation Manual	IN 655.00 Q4432	3.03	2022-06-07	This document is the Installation Manual for the DK-STM Cubicle. DK-STM Cubicle is the equipment that enables ETCS-equipped trains to use the ATC infrastructure. Together with ETCS Onboard DK-STM makes up the ETCS system.
[55]	DK-STM Maintenance Manual Cubicle	VN 655.00 Q4433	3.03	2022-06-20	This document is the maintenance manual for the DK-STM Cubicle edition, which is a sub component in an ETCS system.
[56]	EN50126, Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)	EN 50126-1	-	2017	-
[57]	EN50129, Railway Applications – Safety Related Electronics Systems for Signalling	EN 50129	-	2018	-