RF 0015

REFERENCE DOCUMENT

FOR THE CERTIFICATION

OF THE SAFETY INTEGRITY LEVEL

OF PRODUCTS OR SYSTEMS

ACCORDING TO EN 50126, EN 50128,

EN 50129, EN 50657, ISO 26262

and IEC EN 61508 STANDARDS

CERTIFER 18 rue Edmond Membrée CS 40141 F59308 Valenciennes Tél : +33 [0]3 27 28 35 00 - Fax: +33 [0]3 27 28 35 09 - www.certifer.eu

LIST OF SUCCESSIVE VERSIONS:

Version	Date	Changes
1	14/05/2013	Creation
2	09/12/2014	Addition of the registration document: - ISO/IEC Standard 17065:2012 Addition of the special case of software in Chapter 4.6. Addition of clarification on the certificate in Chapter 4.8.
3DA	04/07/2018	Addition of reference documents: - ISO/IEC 17020 standard: 2012 - Standard EN 50126 (2017) - Standard EN 50129 (2018) - IEC EN 61508 (2011) standard - ISO 26262 (2011) standard - Standard EN 50657 (2017) Addition of cybersecurity standards Deletion of the document: - Standard NF EN 45011 (1998) Reference replacement in Annex 1: - RFU-STR-016 replaces RFU-2-000-16 Extension of the special case of software to products without safety records in Chapter 4.6.
3DB	03/01/2019	Internal review
3DC	12/02/2019	Validation commission 1st submission
3	15/03/2019	Validation commission 2st submission

Version	Date	Changes
4DA	03/02/2022	General update
4DB	01/03/2022	Internal review (POZ, JCA, ALA, ARU)
4DC	18/03/2022	Validation commission 1st submission
4	31/03/2022	Prise en compte commentaire M. FRENEAUX et M. THUMELAIRE

CERTIFER 18 rue Edmond Membrée CS 40141 F59308 Valenciennes Tél : +33 [0]3 27 28 35 00 - Fax: +33 [0]3 27 28 35 09 - www.certifer.eu

MEMBERS OF THE WORKING GROUP ESTABLISHING THE REFERENCE DOCUMENT:

- Philippe BERNAGE, CERTIFER
- Sergio FURLAN, CERTIFER
- Olivier GROSSIN, CERTIFER (author of v4)
- Patrick OZELLO, CERTIFER (reviewer of v4)
- Aryldo RUSSO, CERTIFER
- Jérôme CARLIER (reviewer of v4)
- Annette LAFORME (reviewer of v4)
- Aurélien DUBOIS (reviewer of v4)

MEMBERS OF THE COMMITTEE APPROVING THE REFERENCE DOCUMENT:

- Nicolas CASTRE SAINT MARTIN, ALSTOM
- François BARANOWSKI, UNIVERSITE GUSTAVE EIFFEL
- Thierry FRENEAUX, HITACHI RAIL STS
- Emmanuel LAURANS, SNCF
- Philippe PLESSIS, RATP
- Bernard VINCENT, APAVE
- Ambroise THUMELAIRE

APPROVAL OF THE REFERENCE DOCUMENT:

Following a favourable opinion returned by the Approval Committee (in compliance with CERTIFER procedure 7407), this reference document was signed by:

The Chief Executive Officer of CERTIFER
Pierre KADZIOLA

CERTIFER 18 rue Edmond Membrée CS 40141 F59308 Valenciennes Tél : +33 [0]3 27 28 35 00 - Fax: +33 [0]3 27 28 35 09 - www.certifer.eu

TABLE OF CONTENTS

1. OBJECT AND AREA OF APPLICATION

This reference document establishes the requirements and the procedure for the certification of the safety integrity level of products[1] and systems likely to be used in guided transport systems.

Subsequently it does not fall under the scope of application of the French Consumer Code.

2. REFERENCE DOCUMENTS

a) <u>Standards</u>:

- ISO/CEI 17065 (2012): Conformity assessment – Requirements for bodies certifying products, processes and services
- ISO/CEI 17020 (2012): Requirements for the operation of various types of bodies performing inspection
- ISO/ IEC 17021 (2015): Conformity assessment — Requirements for bodies providing audit and certification of management systems
- EN 50126 (1999, 2017): Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- EN 50128 (2001, 2011, A1/2020, A2/2020): Railway applications – Communications, signalling and processing systems – Software for railway control and protections systems
- EN 50129 (2003, 2018): Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling
- EN 50657 (2017) Railways Applications – Rolling stock applications – Software on Board Rolling Stock
- ISO 26262 (2018 series): Road vehicles – Functional safety
- IEC EN 61508 (2011): Functional safety of electrical/electronic/programmable electronic safety-related systems (various parts)
- IEC 62279 (2015): Railway Applications – Communication, signaling and processing systems – Software for railway control and protection systems

These standards may be completed, when required, by other standards (the last published version applies):

[1] In this reference document, the term “product” refers to both hardware and software products.

- ISO 9001: Quality management systems - Requirements
- EN 50121: Railway applications - Electromagnetic compatibility (various parts)
- EN 50125: Railway applications - Environmental conditions for equipment
- EN 50155: Railways Applications Electronic Equipment Used on Rolling Stock
- EN 50159: Railway applications - Communication, signalling and processing systems. Safety-related communication in transmission systems
- IEC/ISO standards on cybersecurity: ISO 27000 series, ISO/IEC/TR 19791, IEC 62443 series and CLC/TS 50701 (*)
- ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories

* These cybersecurity standards are also useful to take into account the functional safety impacts of electronic safety systems for signalling railway applications, which are simply additional effects of threats generally considered by cybersecurity. See CERTIFER's recommended practice [REP_CERTIFER_0004] for the assessment of cybersecurity to cover EN 50129:2018.

b) <u>Recommended Practice written by CERTIFER</u>:

Reference	Title	Version
REP_CERTIFER_0001	Application of EN 50126:1999 in case of adaptation of an existing product or system	Applicable version
REP_CERTIFER_0002	Application of EN 50129:2018 §6.2 in case of use of pre-existing items	Applicable version
REP_CERTIFER_0003	Assessment of application data process	Applicable version
REP_CERTIFER_0004	Assessment of cybersecurity to cover EN 50129:2018	Applicable version

c) <u>Recommendation for use written by NB-Rail Coordination Group</u>:

Reference	Title	Version
RFU-STR-016	Acceptance of assessment reports on safety prepared by other parties	02

3. DEFINITIONS AND ABREVIATIONS

The definitions of the following reference documents are applicable:

COFRAC: COmité FRançais d'ACréditation

EMC: Electro-magnetic Compatibility

The safety integrity level of products and software is designated by the English acronym **SIL**, (except under the EN50128:2001 Standard for software "Software safety integrity level": English acronym **SSIL**).

ISA: Independent Safety Assessor.

Applicant: entity responsible for demonstrating to the ISA that product or system being assessed meets the required safety integrity level. They are responsible for organising the audits required by the ISA and providing them with all necessary documents relating to the design, manufacturing, installation, verification, testing, safety studies and use of the product or system.

Minor Non Conformity: Any individual non-conformity which does not impair the operability of the Management System, the product or the system. Minor Non-Conformities are mentioned in the assessment report.

Major Non Conformity: Major Non-conformities are mentioned in the assessment report and have to be corrected within a given period in order to obtain or maintain the certificate

TFFR: Tolerable Functional (unsafe) Failure Rate

THR: Tolerable Hazard Rate: the maximum permissible hazard rate

QMS: Quality Management System

QSMS: Quality and Safety Management System

REP: Recommended Practice (document written by CERTIFER)

RFU: Recommendation for Use (document written by NB-Rail Coordination Group)

REX: Return of Experience

SIL: Safety Integrity Level

SSIL: Software Safety Integrity Level

4. PROCEDURES AND REQUIREMENTS

The following paragraphs describe the chronological stages and associated requirements.
All operations associated with the certification service, including those not mentioned in this reference document, but appearing in the procedures of the ISA's quality system, must be executed in compliance with all requirements of the ISO 17020 / ISO 17065 standard, the IAF (International Accreditation Forum) and EA (European Accreditation) guides and COFRAC documents applicable to the type certification.
In particular, the certification body must possess and maintain a complete system of procedures, instructions and forms compliant to SO 17020 / ISO 17065.

4.1. Detailed definition of the product or system to be certified

The certification body must accurately define, in conjunction with the applicant, the limits of the product or system to be certified, explaining:

- The physical architecture, the components and the internal and external functional and technical interfaces
- The standards which are applicable for the project
- The functions of the product or system
- The list of software and hardware, as well as the safety integrity level (SIL and SSIL) and the safety targets (THR/TFFR, hazards) for each one

It is possible that the certification of the product or system also includes processes to be assessed (e.g. processes such as parameterisation or downloading). These must be stipulated.

4.2. Creation of the assessment plan

The certification body will establish an assessment plan detailing at least the following aspects:

- The list of successive versions and modifications made
- The names of the writers (and verifiers, if any)
- The Identity of the applicant
- The context of the mission (a short description of the project which will use the product or system, the assessment stages when there are more than one, the history of assessments when previous versions have already been subject to an assessment)
- The identity and limits of the product to be assessed (see §4.1 of this document), as well as the processes to be assessed, if any
- Identification of the standards which will be used in the assessment according to the standard presented in Chapter 2, (see also § 4.5 below...)..When assessing existing products which have been modified, the applicable requirements of the standards must be specified

- The stages included in the assessment (Risk analysis, Specifications, Allocation of requirements, Design, manufacturing, Installation, unit testing, integration testing, laboratory tests, on-site tests, safety case, operation and maintenance)
- If the assessment concerns a generic product, a generic application or a specific application (such as those defined in the EN 50126 and EN 50129 standard)
- The identification of the persons involved, if known
- The assessment method (number of audits, documentary reviews, visits, and if possible, the depth of documentary reviews). Also state whether the assessment is a gap assessment when a previous version of the product or system has already been subject to an assessment
- The cross-acceptance activities (list of assessment reports to be sent to the ISA)
- The list of assessment tasks
- The deliverables (audit reports, assessment reports, certificate)

And, if required:

- A list of attachments and appendixes
- The special provisions (language, sampling, confidentiality, staff safety, allocation of tasks to partners, sub-contractors or contractors, …)
- Assumptions
- A schedule

The assessment plan may be updated as many times as necessary during performance of the service.

4.3. Agreement of the requesting party on the proposed certification

The applicant must approve the assessment plan and undertake to comply with the obligations of the applicant stipulated in the ISO 17020 / ISO 17065 Standard.

4.4. Tasking of parties involved

The parties (individuals and/or organisations) responsible for assessing the conformity of the products will be selected based on their competence and their independence. They undertake to maintain all information gathered during their mission confidential.

4.5. Performance of the assessment

The parties tasked by the certification body perform the conformity examination in regards to the standards specified in the assessment plan. They are then acting in the capacity of the "assessment officer" in regards to the following standards.

The standards used are :

- EN 50128 for railway control and protection system software
- EN 50657 for embedded software for railway rolling stock
- EN 50129 for signalling, telecommunications and processing products and systems. Electronic safety systems for railway signalling.
- EN 50126 for railway systems and assemblies
- EN 50121 for EMC requirements
- EN50125 and EN50155 for requirements relating to physical environmental conditions
- EN50159 for requirements relating to safety communications
- ISO 26262 for autonomous vehicles used for public transports
- CEI EN 61508 for safety-related electrical / electronic / programmable electronic systems not specific to railway applications

It is strongly recommended to start and conduct the assessment in parallel with the development cycle of the product or system.

The Independent safety assessment must include:

- An assessment of the QSMS of the entity (applicant) in charge of the design, manufacturing, installation, verification, testing, safety study and use of the product or system
- An assessment of the QSMS applied during the project
- A design examination of the product or system

When an assessment only covers modifications to the product or system and, in order to make the modifications, the applicant resubmits the organisation and processes audited and accepted by the ISA during the previous stage, the ISA may decide that a new audit of the quality and safety management system is not required.

a) The Quality and Safety Management System (QSMS)

The ISA must ensure that the standards defined in the documents created in §4.1 and §4.2 are implemented within the framework of the policies applied by the company, based on a Quality Management System (QMS) which conforms to the provisions of [ISO 9001] standard (or equivalent rules).

When the applicant operates a Quality Management System (QMS) certified by an accredited body, for the phases to be covered by the assessment of the product or system in question, the ISA shall take this into account during his QSMS audit (see Appendix 3) .

The team of auditors must have experience in Quality and Safety Management Systems (QSMS) and have at least one member experienced as an assessor in the product or system and the technology concerned, as well as knowledge of the standards defined in the documents created in §4.1 and §4.2.

The audit will include an assessment visit to the applicant's premises*. The team of auditors will examine documentation describing the processes, methods and tools, as well as all technical documents produced during the development of the product or system under assessment, in order to verify the ability of the applicant to implement these processes, methods and tools and to ensure conformity with the requirements of the standards defined in the documents created in §4.1 and §4.2.

The auditing team formalises their conclusions in a QSMS audit report.

* In the case of a "simple" product or system (example: a tool), it is allowed to limit the audit to a documentary audit carried out by the assessor, whose result can be provided directly in the assessment report (no QSMS audit report needed in this case).

b) Surveillance of the Quality and Safety Management System (QSMS)

The purpose of surveillance is to make sure that the applicant duly fulfils the obligations arising out of the approved Quality Management System (QMS).

The assessment will affect all phases, including design, manufacturing, installation, verification, testing and safety studies.

The ISA will periodically perform audits to ensure that the applicant maintains and applies the Quality and Safety Management System (QSMS). These audits will take place every two years at least if the certification contract is still in progress.

It is possible to limit the surveillance audit to a documentary audit.

The auditing team will formalise its conclusion in a QSMS audit report or directly in the assessment

report.

c) Design examination

The applicant must provide the ISA with all documentation regarding the product or system to enable them to understand the design, manufacturing, installation, verifications, testing, as well as safety studies and user manuals, in order to evaluate their compliance with the requirements of the standards defined in the documents created in §4.1 and §4.2.

The ISA must assess the documentation for all software, hardware (programmable electrical, electronic and electronic components), assemblies and parameterisation processes. See CERTIFER's recommended practice [REP_CERTIFER_0003] for the assessment of application data process. The ISA's assessment will also affect the software development cycle, the hardware development cycle and the software and hardware integration. During the documentary assessment, the ISA will make sure that:

- The safety requirements are traceable over the entire life cycle
- The techniques and methods specified in the quality and safety management system are implemented
- The safety verification and validation processes have been implemented
- The functional and technical safety requirements (correct operation under failure-free conditions, the impacts of failures and external influences) are verified

in compliance with the requirements of the standards defined in the documents created in §4.1 and §4.2.

The ISA may perform sample verifications of the documentation, but may also perform a more in-depth assessment depending on the criticality of the information contained in the documentation. The depth of the assessment must always be at least equivalent to the one stipulated in Appendix 2.

The documentary assessment must be conducted by assessors who are competent in the techniques and methods implemented by the applicant.

When a part of the product or system has already been assessed by an independent organisation, the ISA may take this into account to avoid repeating the assessment.

ISA then examine:

- The recognition of the organisation performing the assessment
- The assessment method applied
- The assessment report provided

The assessment criteria used will be those defined in document [RFU-STR-016].

The ISA may, if required, request additional information necessary to the proper understanding of

the results of the assessment report (safety case, description of the conditions of use of the product…etc).

In terms of input data, the ISA will accept test reports (EMC, Environment… and also functional tests) produced by laboratories, after making sure that all necessary tests have been performed based on the intended use of the product or system. The ISA will make sure that the tests are properly admissible (see Appendix 1).

The ISA will assess the safety case of the product or system. He will make sure that all risks identified in the Hazard Log are covered, and that safety constraints relating to usage (integration, operation or maintenance) are clearly defined.

See also these 2 other CERTIFER's recommended practices:

- [REP_CERTIFER_0001] for application of EN 50126:1999 in case of adaptation of an existing product or system
- [REP_CERTIFER_0002] for application of EN 50129:2018 §6.2 in case of use of pre-existing items

4.6. Assessment reports

The assessment report(s) will cover at least the following aspects:

- A review of the context of the service
- The identity of the product undergoing conformity assessment
- The Identification of the standards used
- The identification of the Assessment Plan
- The Identification of the designer or manufacturer of the product, when it is not the applicant
- The names and roles of the persons involved (including sub-contractors) in the conformity assessment
- The names of the writers, checkers and approvers of the report
- The scope of the assessment described in the report
  The report must clearly detail the phases and/or parts of the product and/or the sites subject to the conformity assessment referred to in the report (an extract of the assessment plan is permissible).
  It must be stated whether the assessment affects a generic product, a generic application or a specific application (such as those defined in the standards EN 50126 and EN 50129)
  It must also be stated whether the processes were subject to assessment (e.g. parameterisation processes).
- The constraints and assumptions used in the conformity assessment, if any
  When the results of the conformity assessment are only valid when requirements are assumed to be complied with (functional, environmental, operational…) these requirements, postulates and expectations must be clearly defined. Assumptions made about non-assessed parties must also be mentioned.
- Description of the conformity assessment work completed
  And problems encountered, as well as provisions made to resolve them.
  All discrepancies between the assessment plan and the actual work done must be indicated and justified.
  The visits and audits conducted during the project must be listed
- Conformity assessment methods
  The depth of assessments must be indicated, e.g. listing the documents assessed using a sampling process.
- Identification of assessed documents
- Results
  The assessment report must contain the following elements:

- *Justifications regarding cross-acceptance activities*

- *When the assessment uses results obtained from other assessment missions, the assessment report will include a summary of the assessment results for each of these reports*
- *The conclusions of audits of safety and quality management systems, as well as any discrepancies found during the audits and their statuses (corrective actions in progress, closed reservations…)*
- *The list of hardware and software components assessed, their versions, and the SIL (or ASIL) achieved (specification of the "THR" is also recommended), as well as the conclusions of the assessment for each of the components;*
- *The conclusions of the assessment of the product or system, its version, the SIL achieved (specification of the "THR" is also recommended)*
- *The list of exported safety constraints, or a reference to the safety case when listed therein. Note: The assessment report must mention all discrepancies detected and other open points, or refer to observation and question sheets and non-conformity sheets, if any.*

- Conclusions
  - On the progress of the service (tasks performed, in progress, pending).
  - On the conformity (or lack of conformity) of the product or system with the SIL objective. When non-conformities are remaining, the report must specify the extent of additional assessments required.

<u>Special case of products without safety case</u>:

Example for software: Standards EN 50128 and EN 50657 and ISO 26262 part 6 and IEC EN 61508 part 3 do not require that a software safety case be produced. Subsequently, the ISA will not always have a safety case for the assessment of the exported use and safety constraints. Furthermore, the behavior of a piece of software will largely depend on the hardware on which it is executed.

The ISA shall specify in its report:
- all phases of the life-cycle of the software covered by the assessment, including software/hardware integration and validation
- the safety constraints exported to the user of the software are defined by the applicant
- the hardware used to run the software

4.7. Certification decision

The decision to award certification or not is taken by a committee comprising (in application of the certification body's procedures) members who have not participated in the conformity assessment. The committee will base its decision on:
- the contents of the assessment report
- the results of the "technical review"
- the presentation made by the lead assessor
- the answers provided by the lead assessor to the committee questions.

The Committee is responsible for making decision to issuing new certificates, approving extension or renewals of certificates, making decision on the suspension and withdrawing the certificates.

4.8. Certificates

Preamble: The certificate could be delivered only when no major non-conformity is identified in the assessment report.

The text of the certificate stipulates that it in no way presumes the mass production of the "type" certified, and that it only applies to the design of the product (referred to) and the resulting descriptive dossier.

Intermediate Report and Certificate:
When the safety assessment is limited to certain stages of the life cycle of the product or system, the results of the assessment may be documented in an Intermediate Independent Safety Assessment Report and in an Intermediate ISA Certificate which explain clearly which stages are assessed, and which are not.

The term of validity of the certificate and the certificate surveillance procedure are specified in the procedures used by the certification body.

4.9. Complaints and appeals

The certification body will make its complaints and appeals procedures available to the applicant. In particular, the notification of refusal of a certificate must describe the appeal procedures against this decision.

4.10. Use of the certification body's mark

Type certification does not allow for the marking of products, packaging, notices or guarantee certificates, or the inclusion of the certifier's logo on any medium.

However, the holder may refer to the certificate in conformity and suitability for use declarations, as well as in letters, technical files, commercial tenders etc. They must then communicate:

- Either the entirety of the information appearing on the certificate (including the list of its appendixes)
- Either the entirety of the information appearing on the certificate and its Appendixes

so as to avoid any confusion about the scope of certification.

In order to refer to certification on advertising literature specific to the product (brochures, leaflets, advertising materials, audiovisual media, websites… etc.), the holder must have been previously authorised to use a logo created by the certification body. The latter will send the logo and its conditions of use to the applicant.

4.11. Operations after certification

The certification body will apply the procedures for the surveillance, maintenance and renewal established in compliance with ISO 17065.

Appendix 1: Validity of test results

This note summarizes the requirements, derived from standards (including ISO/CEI 17065), in order to ensure that the results have been obtained under conditions that guarantee their validity.

The respect of the conditions below must be verified by certification body.

If compliance with the following 3 categories of requirements is, in our opinion, insufficiently demonstrated in the documents provided by the customer, "open points" will be created in the remarks and questions sheets: in the form of questions and/or requests for additions.

Depending on the answers and new evidence from the customer, the assessor may either close the item or transform it into an "observation" or "attention point" or even a "remark" or "non-conformity" in the final report, depending on the extent of the concerns raised regarding the credibility of the test results.

1) Content of the test report (or other comparable document)

To be admissible, it must at least include:

	Requirement	Objective
1	A unique identification and, on each page, an indication to ensure that the page is recognized as part of the document, as well as a clear indication of the end of the document	Ensure that nothing has been removed or added
2	The name and address of the entity that carried out the tests	Ensure that the person responsible for the test results is identified
3	Description of (or reference to) the method	Ensure that the method is relevant
4	The precise identification of the equipment used	Ensure that the calibration evidence corresponds to the equipment used (or can be found)
5	The unambiguous description and identification of the test object	Ensure that the sample tested is representative of the product being evaluated
6	The results of the test with, if applicable, the units of measurement	Ensure that the results demonstrate the product's compliance with the requirements
7	Information on specific test conditions, such as ambient conditions, where they are likely to affect the result	Ensure that no test conditions are likely to invalidate the results

	Requirement	Objective
8	A statement of the measurement uncertainty (if it is important for the validity of the results or when it affects compliance with the limits of a specification)	Ensure that the measurement error interval does not exceed the permissible tolerances on the value of the product

2) Quality and Safety Management System (QSMS)

a) For all tests (EMC, Environment…) except functional tests

- Laboratory accredited to EN ISO/IEC 17025 for the test under consideration:

  If the fixed scope of accreditation of the test organization includes the test under consideration, the report presenting the test results is considered acceptable.

- Laboratory accredited EN ISO/IEC 17025, whose flexible scope includes the test under consideration:

  If the flexible scope of accreditation of the test organization includes the test under consideration, the report presenting the test results is considered acceptable.

- Laboratory accredited EN ISO/IEC 17025, whose scope does not include the test under consideration:

  Acceptance of the report presenting the test results is subject to the results of a third-party audit, covering the specific application, specific techniques and conditions for carrying out the test.

- Other laboratories:

  Acceptance of the report presenting the test results is subject to the results of a third-party audit on compliance with the requirements of EN ISO/IEC 17025.

b) For functional tests

Contrarily to EMC, Environment,… tests (see 2.1 above), the EN ISO/IEC 17025 standard is not considered to be systematically applicable for QSMS of functional tests, for which the ISO 9001 standard (or equivalent rules) applies.

Additionally to the QSMS audits to be done in the certification program (see chap. 4.5 above) which already cover several phases including test phase, if the ISA deems it necessary (example: depending of the project specificities), he can also conduct a specific audit for functional tests in laboratory or on-site for a specific application, in order to:

- Gauge the relevance of the tools, procedures and methods used and to ensure compliance with the QSMS requirements,
- Witness some tests performed (the ISA may require additional tests to be performed).

3) Calibration

Certificates demonstrating the validity of the calibration of all equipment used for measurements and tests that have a **significant influence on the results of our evaluation** must be provided to the certification body by correspondence or presented on site.

Note: An accreditation according to EN ISO/IEC 17025 fixed or flexible of the test activity concerned exempts the latter requirement.

Appendix 2: Depth of documentary reviews

Abbreviations used, from the most demanding level to the least demanding:

CR: Critical reading
SR: Reading by sampling
FR: Fast reading
NE: Not examined

And:

X: The method is used regardless of the level of safety integrity of the product
X1: The method is used when the product integrity level is SIL1
X2: The method is used when the product integrity level is SIL2
X3: The method is used when the product integrity level is SIL3
X4: The method is used when the product integrity level is SIL4

Documents to be reviewed	NE	FR	SR	CR
a) QSMS documents				
Quality manual		X (if ISO9001)		X (if not ISO9001)
Procedures and instruction sheets	X (if ISO9001)		X (if not ISO9001)	
Management plan				X
Quality plan				X
Safety plan				X
Quality registration documents (Report, review, anomaly sheets, change sheets, etc.)		X		
b) System or product documents				
System or product risk analysis			X	
System or product functional specifications				X
System or product architecture specifications		X1,X2		X3, X4
System or product safety principles		X1,X2		X3, X4
System or product integration test specifications and installation		X1,X2	X3,X4	
System or product integration test results and installation		X1,X2	X3, X4	
System or product validation tests specifications		X1,X2	X3, X4	
System or product validation test results		X1,X2	X3, X4	
System or product Hazard Log			X	

Documents to be reviewed	NE	FR	SR	CR
System or product safety case				X
c) Hardware documents				
Hardware risk analysis		X1,X2	X3,X4	
Hardware functional specifications		X1,X2		X3,X4
Hardware architecture and safety principles		X1,X2		X3,X4
Hardware integration test specifications		X1,X2	X3,X4	
Hardware integration tests results		X1,X2	X3,X4	
Hardware validation tests specifications		X1,X2	X3,X4	
Hardware validation tests results		X1,X2	X3,X4	
Hardware environmental tests results (EMC, vibration, temperature, ...)		X		
d) Software documents				
Software risk analysis		X1,X2	X3,X4	
Software functional specifications			X1,X2	X3,X4
Software architecture specifications		X1,X2		X3,X4
Software detailed design specifications		X1,X2	X3,X4	
Software source code	X			
Software test tools documentation		X		
Software integration test specifications		X1,X2	X3,X4	
Software integration test results		X1,X2	X3,X4	
Software validation tests specifications		X1,X2	X3,X4	
Software application data validation report (for a specific application configured by application data)		X1,X2	X3,X4	

CERTIFER 18 rue Edmond Membrée CS 40141 F59308 Valenciennes Tél : +33 [0]3 27 28 35 00 - Fax: +33 [0]3 27 28 35 09 - www.certifer.eu

Appendix 3: QSMS audit applied to the product or system under assessment, in the case of a certified QMS

Preamble: According to standards EN 50126/50128/50129, the quality management system should be compliant to EN ISO 9001 (or equivalent rules).

If the applicant operates a Quality Management System (QMS) certified by a certification body, the audit topic shall include only the reference highlighted in **bold and underlined**. The remaining references, not bold and not highlighted, are meant to be already covered during the evaluation for [ISO 9001] for certification by the certification body.

1. General Aspects of QMS, QMS Documentation, Document Management
All the elements, requirements and provisions adopted by the applicant shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. The quality management system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.
(ISO 9001:2015 4.1 to 4.4; 7.4; 7.5)

2. Management Responsibility
The quality objectives and the organisational structure, responsibilities and powers of the management with regard to design and product quality,
(ISO 9001:2015 **5.1.2a,b**; 5.1 to 5.3, 6.1; 6.2; 6.3)

3. Human Resources
The quality records, such as qualification reports on the personnel concerned, etc.,
(ISO 9001:2015 **7.1.1; 7.1.1; 7.1.4; 7.1.6; 7.2; 7.3**)

4. Infrastructural Resources
The corresponding manufacturing, quality control and quality management system techniques, processes and systematic actions that will be used,
(ISO 9001:2015 **7.1.1; 7.1.3; 7.1.4**)

5. Design - Planning, Inputs, Outputs
The technical design specifications, including standards, that will be applied,
(ISO 9001:2015 **8.1; 8.2; 8.3.1 to 8.3.3; 8.3.5**)

6. Design - Evaluation, Verification& Validation
The design control and design verification techniques, processes and systematic actions that will be used when designing the product pertaining to the product category covered,
(ISO 9001:2015 **8.3.4**)

7. Control of Design Changes

The design control and design verification techniques, processes and systematic actions that will be used when designing the product pertaining to the product category covered,
(ISO 9001:2015 **8.2.4; 8.3.6; 8.5.6**)

8. Production/ Service provision - Performance, Evaluation, Verification& Validation, Release of Products, Control of non-conforming products

The corresponding manufacturing, quality control and quality management system techniques, processes and systematic actions that will be used, the examinations and tests that will be carried out before, during and after manufacture, and the frequency with which they will be carried out, the means of monitoring the achievement of the required design and product quality and the effective operation of the quality management system
(ISO 9001:2015 **8.5.1; 8.5.2**; 8.5.3; **8.5.4**; 8.5.5; **8.6; 8.7; 9.1; 10.2**)

9. Control of Monitoring and Measurement Equipment

The corresponding quality control and quality management system techniques, processes and systematic actions that will be used,
(ISO 9001:2015 **7.1.5; 8.5.1b**)

10. Procurement and Control of purchased goods/ services

The corresponding quality control and quality management system techniques, processes and systematic actions that will be used,
(ISO 9001:2015 **8.4**)

11. Continuous Monitoring, Measurement, Analysis

The corresponding manufacturing, quality control and quality management system techniques, processes and systematic actions that will be used, the quality records, such as inspection reports and test data, calibration data, qualification reports on the personnel concerned, etc., and the means of monitoring the achievement of the required design and product quality and the effective operation of the quality management system.
(ISO 9001:20155 **9.1**; 9.2; 9.3)

12. Continuous Improvement – Corrective Actions, Preventive Actions (incl. project SMS)

The corresponding manufacturing, quality control and quality management system techniques, processes and systematic actions that will be used
(ISO 9001:2015 **10.1; 10.2**; 10.3)