REFERENCE DOCUMENT

RF 0015

INDEPENDENT ASSESSMENT AND CERTIFICATION OF THE SAFETY INTEGRITY LEVEL OF PRODUCTS OR SYSTEMS

ACCORDING TO STANDARDS

CENELEC EN 50126, EN 50129, EN 50128, EN 50657, EN 50716

ISO 26262

IEC EN 61508

LIST OF SUCCESSIVE VERSIONS

Version	Date	Change
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.
3	15/03/2019	Addition of reference documents: - ISO/IEC 17020 standard: 2012 - Standard EN 50126 (2017) - Standard EN 50129 (2018) - Standard IEC EN 61508 (2011) - Standard ISO 26262 (2011) - 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.
4	31/03/2022	General update
5	20/03/2025	Update with: - Adding the new EN 50716 standard - Assessment process SIL0/BI - RAM assessment - Non safety-related certification - Series production - Use of the Logo - Cross-acceptance - Adding new ISA certificates And General update.

The most recent version supersedes the previous versions.

MEMBERS OF THE WORKING GROUP ESTABLISHING THE REFERENCE DOCUMENT

- Olivier GROSSIN
- Patrick OZELLO
- Jérôme CARLIER
- Annette LAFORME
- Aurélien DUBOIS
- Wenjun TONG
- Diego ELIA

MEMBERS OF THE TECHNICAL COMMITTEE APPROVING THE REFERENCE DOCUMENT

- Pierre FLEURY, ALSTOM
- François BARANOWSKI, UNIVERSITE GUSTAVE EIFFEL
- Thierry FRENEAUX, CSEE
- Robert CAPEL, ALSTOM
- Emmanuel LAURANS, SNCF
- Philippe PLESSIS, RATP

APPROVAL OF THE REFERENCE DOCUMENT

Following a favourable opinion returned by the Approval Committee , this reference document was signed by :

	Signature
Name: Jérôme CARLIER **Position:** Technical Director	Jérôme CARLIER Signé numériquement par Jérôme CARLIER DN : cn=Jérôme CARLIER, c=FR, o=CERTIFER, ou=RT - CCS, email =jerome.carlier@certifer.eu Date : 2025.03.21 17:03:47 +01'00'
Name: Aurélien DUBOIS **Position:** Quality Director	

People who have written and checked this report (listed on the cover) approved it using secure electronic authorisation, with CERTIFER's EDM software keeping a trace of it.

TABLE OF CONTENTS

1. PURPOSE AND SCOPE

This reference document establishes the requirements and the procedure for the independent assessment and certification by CERTIFER of the Safety Integrity Level (SIL) 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 or any national equivalent consumer code.

2. REFERENCE DOCUMENTS

2.1 STANDARDS

Standards	
[Reg 1]	ISO/CEI 17065:2012 – Conformity assessment – Requirements for bodies certifying products, processes and services
[Reg 2]	ISO/IEC 17020:2012 – Conformity assessment – Requirements for the operation of various types of bodies performing inspection
[Reg 3]	EN 50126-1:2017+A1:2024 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process
[Reg 4]	EN 50126-2:2017 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety
[Reg 5]	*EN 50126-1:1999 – Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)*
[Reg 6]	EN 50129:2018 – Railway Applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling
[Reg 7]	*EN 50129:2003 – Railway Applications – Communication, Signalling and Processing Systems – Safety Related Electronic Systems for Signalling*
[Reg 8]	EN 50128:2011+A2:2020 – Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems
[Reg 9]	*EN 50128:2001 – Railway Applications – Communication, Signalling and Processing Systems – Software for Railway Control and Protection Systems*
[Reg 10]	EN 50657:2017 – Railway Applications – Rolling stock applications – Software on Board Rolling Stock
[Reg 11]	EN 50716:2023[2] – Railway applications – Requirements for software development
[Reg 12]	ISO 26262:2018 (series) – Road vehicles – Functional safety
[Reg 13]	IEC EN 61508:2011 – Functional safety of electrical/electronic/programmable electronic safety-related systems (various parts)
[Reg 14]	IEC 62279:2015 – Railway Applications – Communication, signalling and processing systems – Software for railway control and protection systems

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

[2] The EN 50128:2011 and EN 50657:2017 will be withdrawn by the EN 50716:2023 on 30/10/2026.

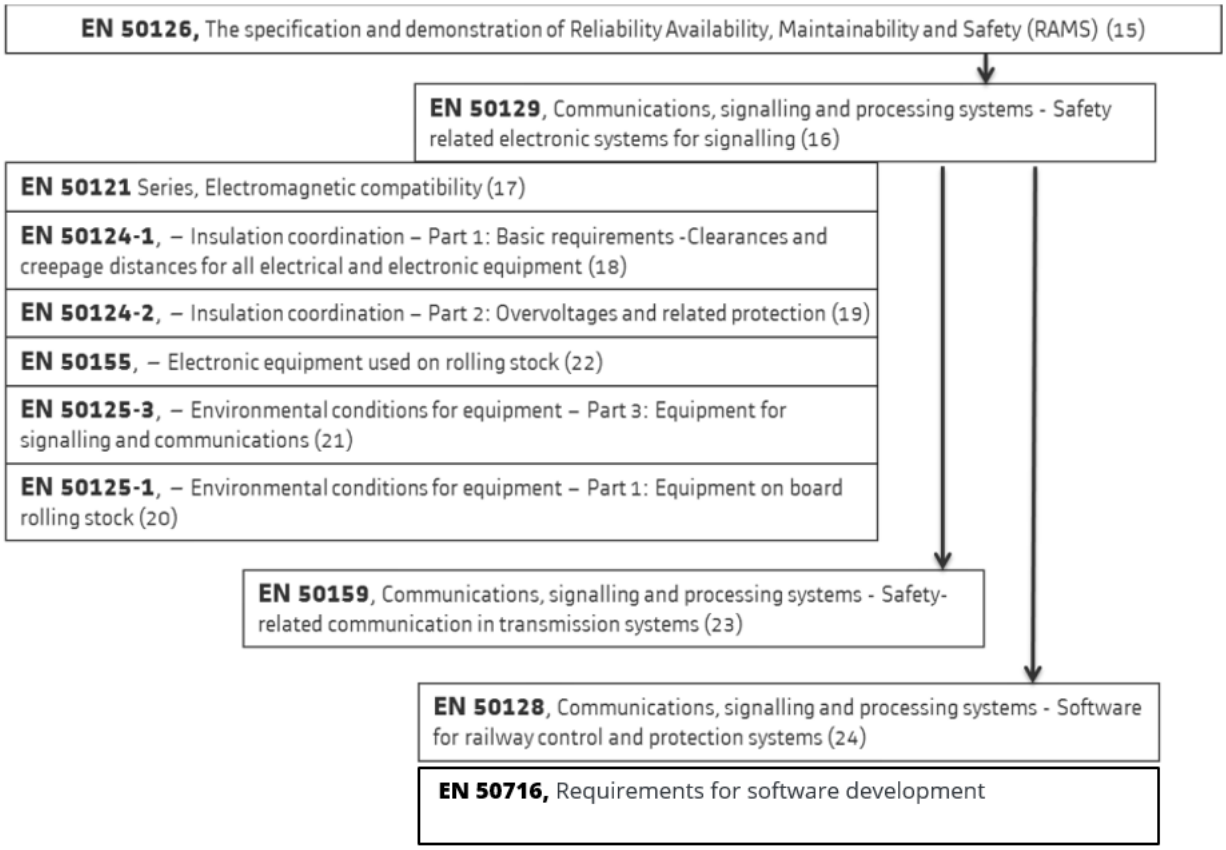
2.2 ADDITIONAL STANDARDS

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

Additional Standards
[Reg 15] EN ISO 9001 – Quality Management Systems – Requirements
[Reg 16] EN 50121 – Railway applications - Electromagnetic compatibility (various parts)
[Reg 17] EN 50124 – Railway applications - Insulation coordination (various parts)
[Reg 18] EN 50125 – Railway applications - Environmental conditions for equipment
[Reg 19] EN 50155 – Railway Applications Electronic Equipment Used on Rolling Stock
[Reg 20] EN 50159 – Railway applications - Communication, signalling and processing systems. Safety-related communication in transmission systems
[Reg 21] EN ISO/IEC 17025 – General requirements for the competence of testing and calibration laboratories

2.3 STRUCTURAL ORGANISATION OF CENELEC STANDARDS

The Figure 1 below provides the illustration of the structural organization of the CENELEC standards:



2.4 CYBERSECURITY

As far as cybersecurity standards are concerned, it is useful to consider the functional safety implications of electronic safety systems for railway signalling applications, which are simply additional effects of the threats generally taken into account by cybersecurity (refer to CERTIFER's recommended practice [Reg 29] for the assessment of cybersecurity to cover EN 50129:2018).

Security Standards	
[Reg 22]	EN ISO 27000 family — Information security management
[Reg 23]	ISO/IEC/TR 19791 – Information technology
[Reg 24]	IEC 62443 – Security for industrial automation and control systems
[Reg 25]	CLC/TS 50701 – Railway applications - Cybersecurity

2.5 CERTIFER's Recommended Practices (REP)

REP	
[Reg 26]	REP_CERTIFER_0001 – Application of EN 50126:1999 in case of adaptation of an existing product or system
[Reg 27]	REP_CERTIFER_0002 – Application of EN 50129:2018 §6.2 in case of use of pre-existing items
[Reg 28]	REP_CERTIFER_0003 – Assessment of application data process
[Reg 29]	REP_CERTIFER_0004 – Assessment of cybersecurity to cover EN 50129:2018
[Reg 30]	REP_CERTIFER_0005 – Impact of EN 50129:2018 §6.3 "safety-related tools for electronic systems" in assessment and certification activities
[Reg 31]	REP_CERTIFER_0007 – Impact of EN 50129:2018 in assessment activities and certification
[Reg 32]	REP_CERTIFER_0008 – AsBo safety Assessment Report when the CENELEC standards EN 50126-1-2, EN 50128 and EN 50129 are used for the demonstration of risk management process

3. DEFINITIONS AND ACRONYMS

3.1 DEFINITIONS

- **Applicant**[3]
  Entity responsible for demonstrating to CERTIFER that the product or system being assessed meets the required safety integrity level. This entity is responsible to organize the audits required by the Assessment Plan and to provide to CERTIFER all necessary documents relating to the design, manufacturing, installation, verification, testing, safety studies and use of the product or system.

- **Minor Non-Conformity (or Remark)**
  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.

3.2 ACRONYMS

ATO	Automatic Train Operation
BI	Basic Integrity
COFRAC	COmité FRançais d'ACréditation
EMC	Electro-magnetic Compatibility
GP	Generic Product
GA	Generic Application
ISA	Independent Safety Assessor or Independent Safety Assessment
OCC	Operation Control Centre
Q(S)MS	Quality (and Safety) Management System
RAM(S)	Reliability, Availability, Maintenability (and Safety)
REP	Recommended Practice (document written by CERTIFER)
RFU	Recommendation for Use (document written by NB-Rail Coordination Group)
REX	Return of Experience
SA	Specific Application
SIL	Safety Integrity Level
SRAC	Safety Related Application Condition
TFFR	Tolerable Functional (unsafe) Failure Rate
THR	Tolerable Hazard Rate: the maximum permissible hazard rate

[3] In some cases, the applicant should not be confused with the customer. Depending on the contractual arrangement, the customer may not be the applicant. The client has a contract with the assessment body and is the owner of the certificate, if any, issued by Certifer. The applicant is the entity responsible for demonstrating safety.

4. PROCEDURES AND REQUIREMENTS

The following paragraphs describe the chronological stages of the Independent Safety Assessment and the associated requirements.

As a reminder, the Independent Safety Assessment does not constitute an additional verification or validation activity compared to those carried out by the applicant. Moreover, the assessor may ask for additional verification and validation work to the applicant.

The detailed role for Independent Safety Assessor is specified for example in Table G.4 of Annex G of [Reg 3] and in Table B.8 of [Reg 8].

The Independent Safety Assessment can be defined as the process to determine whether the system/product meets the specified safety requirements and to form a judgement as to whether the system/product is fit, from the point of view of safety, for its intended purpose.

All operations associated with the assessment service, including those not mentioned in this reference document, but appearing in the procedures of CERTIFER's quality system, must be executed in accordance with the requirements of the ISO 17020 / ISO 17065 standards, the IAF (International Accreditation Forum) and EA (European Accreditation) guides and COFRAC documents applicable to the type certification and/or inspection.

In particular, CERTIFER owns and maintains a complete system of procedures, instructions and forms that comply with ISO 17020 / ISO 17065 standards.

For an ISA assignment carried out under accreditation:

- The assessment is carried out by applying an inspection process in accordance with ISO 17020:2012.
- If a certificate is issued in addition to the assessment report, and only for this certificate, a certification process is applied in accordance with ISO 17065:2012.

4.1 DEFINITION OF THE PRODUCT OR SYSTEM

CERTIFER accurately defines, in close collaboration with the applicant, the limits of the product or system to be assessed, explaining:

- The physical architecture, the components and the internal and external functional and technical interfaces ;
- The standards applicable to the project ;
- The functions of the product or system ;
- The configuration and version of the product or system ;
- The list of software and hardware, together with the safety integrity level (SIL) and the safety objectives (THR/TFFR, hazards) for of them.

The assessment of the product or system may also include processes to be assessed (e.g. processes such as parameterisation or downloading). These must be specified in the definition of the product or system to be assessed.

4.2 ASSESSMENT PLAN

CERTIFER draws up an **Assessment Plan** detailing at least the following aspects:

- A list of successive versions and changes made ;
- The name of the writer and reviewer(s) ;
- The identification of the applicant ;
- The context of the assignment (a brief description of the project which will use the product or system, the stages of the assessment where there are several, the history of assessments where previous versions have already been assessed including previously assessed system/product versions, assessment reports and certificates with their references and versions) ;
- The identification and limits of the product to be assessed (see §4.1), as well as the processes to be assessed, where applicable ;
- The identification of the standards which will be used in the assessment in accordance with the standards presented in section 0. When assessing existing products which have been modified, the applicable requirements of the standards must be specified ;
- The assessment stages (risk analysis, specifications, requirements allocation, design, manufacture, installation, unit tests, integration tests, laboratory tests, on-site tests, safety case, operation and maintenance) ;
- Whether the assessment concerns a generic product (GP), a generic application (GA) and/or a specific application (SA) such as those defined in standards EN 50126 and EN 50129 ;
- Identification of the people involved (name and role), if known ;
- The assessment methodology (number of audits, documentary reviews, visits, and if possible, the depth of the document reviews). Also indicate whether this is a gap assessment where a previous version of the product or system has already been assessed ;
- Cross-acceptance activities (list of assessment reports to be sent to CERTIFER) ;
- The list of assessment tasks ;
- Deliverables (audit reports, assessment reports, certificate) ;
- The list of documents to be assessed if available at this stage

And, if necessary :

- A list of attachments and appendixes ;
- Special provisions (language, sampling, confidentiality, staff safety, allocation of tasks to partners, sub-contractors or contractors, etc.) ;
- Assumptions ;
- An indicative schedule / planning

The Assessment Plan can be updated as often as necessary during the performance of the service.

Note: The Assessment Plan complies with the CERTIFER template in force.

4.3 APPLICANT'S AGREEMENT OF THE PROPOSED CERTIFICATION

The applicant must approve the Assessment Plan and undertake to comply with the applicant's obligations stipulated in ISO 17020 / ISO 17065 standards.

4.4 ALLOCATION OF TASKS TO THE PARTIES CONCERNED

The parties (individuals and/or organisations) responsible for assessing products conformity are chosen on the basis of their competence and their independence. They undertake to keep confidential all information gathered during their mission.

4.5 CONDUCTING THE ASSESSMENT

The parties appointed by CERTIFER perform the conformity examination against the standards specified in the Assessment Plan (§4.2). They then act as assessors against the following standards:

- EN 50128 or EN 50716 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
- EN 50125 and EN 50155 for requirements relating to physical environmental conditions
- EN 50159 for requirements relating to safety communications
- ISO 26262 for autonomous vehicles used for public transports
- IEC EN 61508 for safety-related electrical / electronic / programmable electronic systems not specific to railway applications

It is strongly recommended that the assessment is initiated and conducted in parallel with the product or system development cycle.

The Independent Safety Assessment includes :

- An audit of the QSMS of the entity responsible for the design, manufacture, installation, verification, testing, safety studies and use of the product or system ;
- A surveillance audit of the QSMS applied during the project ;
- A design examination of the product or system.

Where an assessment covers only changes to the product or system and, in order to carry out these changes, the applicant resubmits the organisation and processes audited and accepted by the ISA (may not be CERTIFER) during the previous stage, then CERTIFER may decide that a further audit of the quality and safety management system is not necessary.

4.5.1 AUDIT OF THE QUALITY AND SAFETY MANAGEMENT SYSTEM (QSMS)

CERTIFER ensures that the standards defined in the Assessment Plan (§4.2) are implemented as part of the policies applied by the company, on the basis of a Quality Management System (QMS) that complies with the provisions of the standard ISO 9001 [Reg 15] (or equivalent regulation).

Where the applicant uses 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, CERTIFER takes the existing QMS certification into account during its audit of the QSMS (see Appendix 3: QSMS audit applied to the product or system under assessment, in the case of a certified QMS).

CERTIFER draws up a **QSMS Audit Plan** before the audit, based on the ISO 9001 structure (see Appendix 3: QSMS audit applied to the product or system under assessment, in the case of a certified QMS).

The audit team has experience in Quality and Safety Management Systems (QSMS) and consists of at least:

- One quality auditor with deep knowledge of the standard ISO 9001 or equivalent ;
- One technical auditor experienced as an assessor in the product or system and the technology concerned, as well as knowledge of the standards defined in the Assessment

Plan (§4.2).

Note : The technical auditor may act as a quality auditor and carry out the QSMS audit, provided that he is recognised as competent for the standard ISO 9001 [Reg 15] or equivalent.

The audit includes a visit to the applicant's premises if possible, otherwise remotely[4]. The team of auditors (or the assessor competent for the ISO 9001 standard [Reg 15]) examines the documentation describing the processes, methods and tools, as well as all technical documents produced during the development of the product or system being assessed, in order to verify the applicant's ability to implement these processes, methods and tools and to ensure conformity with the requirements of the standards defined in the Assessment Plan (§4.2).

The audit team formalises its conclusions in a **QSMS Audit Report**.

Note: The QSMS Audit Report complies with the CERTIFER template in force.

In the case of a "simple" product or system (e.g. a single tool, a process, etc.), it is allowed to limit the audit to a documentary audit carried out by the assessor, the result of which can be provided directly in the Assessment Report (no QSMS Audit Report needed in this case).

Note 1: A tool composed of several tools if considered as a "complex" product (therefore subject to a QSMS audit report).

A **Technical Visit** is an audit focusing only on the technical parts of the product or system. It may include safety topics but not necessarily quality topics. Unlike a QSMS audit, a **technical visit** may be conducted by a safety/technical assessor (the presence of a quality auditor is not necessarily mandatory.).

The need to perform additional Technical visits may be identified in the Assessment Plan (e.g. as per the REP_CERTIFER_0003 [Reg 28] recommendations, CERTIFER performs a Technical Visit of the application data process, for any product or system which is configured by SIL4 application data).

[4] If it is not possible to carry out the audit on site, it can be carried out remotely if the applicant agrees.

4.5.2 SURVEILLANCE OF THE QUALITY AND SAFETY MANAGEMENT SYSTEM (QSMS)

The purpose of Surveillance Audit is to ensure that the applicant duly fulfils the obligations arising from the approved quality management system (QMS).

CERTIFER will then carry out periodic audits to ensure that the applicant maintains and applies the quality and safety management system (QSMS). These audits will take place at least every two years if the assessment assignment is still in progress. Generally, the Surveillance Audit focuses on the on-going phase of the project.

It is possible to limit the Surveillance Audit to a documentary audit.

The team of auditors formalises its conclusions in a **QSMS Audit Report** or directly in the **Assessment Report**.

4.5.3 DESIGN EXAMINATION

The applicant must deliver all the documentation concerning the product or system to enable CERTIFER to understand the design, manufacture, installation, checks, tests, as well as safety studies and user manuals, in order to assess their conformity with the requirements of the standards referenced in the Assessment Plan (§4.2).

CERTIFER assesses the relevant documentation of all system, subsystem, software, hardware (programmable electrical, electronic and electronic components), assemblies and parameterisation processes[5] which applies to the product or system under assessment. CERTIFER assessment also covers the software development cycle, the hardware development cycle and the integration of software and hardware. During the design examination, CERTIFER ensures 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.

CERTIFER may carry out sample[6]checks of the documentation, but may also carry out a more in-depth assessment depending on the criticality of the information contained in the documentation. The depth of the assessment should always be at least equivalent to that stipulated in Appendix 2: Depth of documentary reviews.

The documentary assessment must be carried out by assessors competent in the techniques and methods used by the applicant.

[5] See CERTIFER recommendation [Reg 28] for the assessment of the application data process

[6] From §7.1.2 of ISO 17020: “Where applicable, the inspection body shall have sufficient knowledge of statistical techniques to ensure statistically sound sampling procedures and the correct processing and interpretation of results.” As a result, the assessor shall be able to justify his sampling selection.

CERTIFER assesses the product or system **Safety Case**. It will ensure that all the risks identified in the **Hazard Log** are covered and that the safety constraints relating to use (integration, operation or maintenance) are clearly defined.

See also these CERTIFER's recommended practices:

- [Reg 26] for application of EN 50126:1999 in case of adaptation of an existing product or system
- [Reg 27] for application of EN 50129:2018 §6.2 in case of use of pre-existing items

4.5.4 CROSS-ACCEPTANCE

Where a part of the product or system has already been assessed by an independent body (may not be CERTIFER), CERTIFER takes this into account to avoid repeating the assessment. CERTIFER applies the cross-acceptance methodology.

CERTIFER then examines:

- The recognition of the organisation which carried out the assessment ;
- The assessment method applied ;
- The Assessment Report provided.

The cross-acceptance criteria used are those defined in Appendix 4: Cross-acceptance methodology.

CERTIFER may, if necessary, requests additional information required for a proper understanding of the results of the assessment report (safety case, conditions of use of the product, etc.).

4.5.5 UPDATING AN EXISTING ASSESSMENT

In case the product or system under assessment is modified (e.g. for an enhancement or error correction) CERTIFER may limit its assessment to the scope of the modifications. However, CERTIFER should also endorse the previous assessment results and conclude for the product or system as a whole. To do this, CERTIFER cross-accepts the results of the previous assessment. If another assessment body (ISA) carried out the previous assessment, the applicant must submit the previous Assessment Report and certificate (if any) to CERTIFER for cross-acceptance.

4.5.6 TEST ACTIVITIES

With regard to input data, CERTIFER may accept the test reports (EMC, environmental, etc. but also functional tests) produced by a laboratory, after ensuring that all the necessary tests have been carried out for the intended use of the product or system. CERTIFER will ensure that the tests are duly admissible (see Appendix 1: Acceptance of test results).

4.5.7 RELIABILITY, AVAILABILITY, MAINTAINABILITY (RAM)

CERTIFER assesses the safety integrity level (SIL) of the product or system under assessment, but certain aspects of the RAM can also be assessed. As explained in the CENELEC standards :

"The RAMS elements are interlinked in the sense that a weakness in any of them or mismanagement of conflicts between their requirements can prevent achievement of a dependable system.
For example, a safety target can be achieved by ensuring the system enters a safe state (e.g. all trains stopped) in the event of a particular failure. The defined safe state can depend on

operational/maintenance context (e.g. a train at standstill at platform rather than in tunnel). If there are circumstances where this safe state has a significant adverse impact on reliability/availability then a different and optimised solution might be needed in order to achieve the RAM targets without compromising safety."

The independent assessment of "RAM+S" requirements is entirely the responsibility of CERTIFER.

However, CERTIFER limits the assessment to the RAM aspect used in the safety demonstration only (example: periodical preventive maintenance because this periodicity has been used in the demonstration of a quantitative safety target).

Consequently the assessment of the aspect of RAM which is not used in the safety demonstration (example: product availability) remains outside the scope of CERTIFER.

4.5.8 NON SAFETY-RELATED PRODUCT OR SYSTEM

For a product or system that is not safety-related, i.e. that is not involved in any feared event (e.g. radio, ATO, OCC), the applicant may sometimes wish to apply a SIL process (e.g. SIL1 or SIL2). The reason is generally to transpose the SIL process for availability or quality purposes, although this is not the initial purpose (SIL process is for safety purpose only).

In this case, and if the applicant requests an ISA certificate, CERTIFER agrees to issue it provided that the information is clearly given. The ISA certificate (and its appendix) should clearly state that only the development process is assessed in accordance with the SIL1/SIL2, with no feared events for safety. The product or system then meets a very high level of availability (the value is specified) and quality.

4.6 ASSESSMENT REPORT

The Assessment Report covers at least the following aspects:

- A review of the context of the service ;
- Identification of the product undergoing conformity assessment ;
- Identification of the standards used ;
- Identification of the Assessment Plan ;
- Identification of the product designer or manufacturer, where it is not the applicant ;
- The name and role of the persons involved (including sub-contractors) in the conformity assessment ;
- The name of the report writer, reviewer and approver ;
- The scope of the assessment ;

  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 permitted).
  It must be stated whether the assessment concerns 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 valid only if it is assumed that the requirements are met (functional, environmental, operational, etc.), these requirements, postulates and expectations must be clearly defined. Assumptions concerning non-assessed parts must also be mentioned.

- Description of the conformity assessment work carried out ;

  And problems encountered, and the steps taken to resolve them.
  All discrepancies between the assessment plan and the work actually carried out must be indicated and justified.
  Visits and audits carried out during the project must be recorded.

- Conformity assessment method ;

  The depth of assessments should be indicated, e.g. by listing the documents assessed using a sampling[7] process.

- Identification of assessed documents ;
- Results ;

  Justifications for cross-acceptance activities

  Where the assessment makes use of results obtained in the course of other assessment assignments, the assessment report will include a summary of the assessment results for each of these reports

  The conclusions of the audits of safety and quality management systems, as well as any deviations found during the audits and their status (corrective actions in progress, closed reservations, etc.)

  The list of hardware and software components assessed, their versions, and the SIL (or ASIL) achieved (mention 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.

- Conclusion

  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 standards and regulations (and their references and versions) and with the SIL objective. When non-conformities are remaining, the report must specify the extent of additional assessments required.

Note: The Assessment Report complies with the CERTIFER template in force.

4.6.1 SPECIFIC CASE OF PRODUCTS WITHOUT SAFETY CASE:

For software, none of the standards EN 50128 and EN 50657 and EN 50716 and ISO 26262 part 6 and IEC EN 61508 part 3 requires the production of a safety case. Consequently, CERTIFER will not always have a safety case for assessing use and safety exported constraints. Furthermore, the behaviour of a software component depends largely on the hardware on which it is executed.

In its Assessment Report, CERTIFER specifies:

- All the phases of the software life-cycle covered by the assessment, including software/hardware integration and validation ;
- The safety constraints exported to the software user and defined by the applicant ;
- Any additional exported constraints if necessary ;

[7] Could be explained in the assessment form (QRF), or even in the assessment report.

- The hardware used to run the software.

4.7 CERTIFICATION

4.7.1 CERTIFICATE

Preamble: The ISA certificate can only be issued if no major non-conformity is identified in the Assessment Report.

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

Note: The ISA certificate complies with the CERTIFER template in force.

For clarity purpose, we distinguish the following hereafter:

- Design Examination Type certificate
- Series (production) certificate
- Inspection certificate
- Intermediate (Report and) Certificate

Design Examination Type certificate

This certificate relates to the design (including validation) of a generic product (GP) or generic application (GA) or even of the design phase of a specific application (SA).

The text of the certificate stipulates that it in no way presumes the series production of the “type” certified, and that it only applies to the design (including validation) of the product/system (referred to) and the resulting descriptive file.

CERTIFER also issues, in association with the certificate, an **appendix (to certificate)** containing all the essential information contained in the Assessment Report (see 4.6) without repeating the detailed results of the assessment, just its conclusion. Conditions of use and maintenance are specified, as is part of the product/system identification (product/system version and documentation).

The period of validity is unlimited as long as there are no changes.

Series (production) certificate

At the request of the applicant, CERTIFER may also issue a Series certificate. This certificate covers the series production phase of the product or system being assessed.

The prerequisite for issuing a series certificate is that CERTIFER has successfully assessed the applicant's production process for the product or system being assessed.

This assessment must be carried out by means of an audit of the QMS applied to the production phase of the product or system being assessed.

The text of the series certificate stipulates that the period of validity is limited to 2 years. Renewal for a further period of validity of 2 years is subject to a surveillance audit.

In this case, the certificate can refer directly to the QMS Audit Report (no appendix to certificate is produced).

Inspection certificate

This certificate relates to the design and deployment (i.e. physical implementation) of a Specific Application (SA). The installation and on-site testing phases are therefore assessed and included in the ISA certificate.

The prerequisite for issuing an inspection certificate is that CERTIFER has successfully assessed the applicant's installation process and on-site testing process for the product or system being assessed.

This assessment must be carried out by means of an audit of the quality management system applied to the installation and on-site testing phases of the product or system being assessed. Generally, CERTIFER performs an on-site audit with both physical inspection of the installation and witnessing of the dynamic tests.

The text of the inspection certificate stipulates that the period of validity is unlimited as long as there are no changes to the installation and on-site testing processes.

In this case, the certificate can refer directly to the Assessment Report, which should refer also to the Audit Report (no appendix to certificate is produced).

Intermediate Report and Certificate

When the safety assessment is limited to certain phases of the life cycle of the product or system, the results of the assessment shall be documented in an Intermediate Assessment Report and in an Intermediate ISA certificate which explains clearly which phases are assessed, and which are not.

The Intermediate ISA certificate shall indicate that **only the development process** is assessed in accordance with the SILx (in no case must the certificate state that the product or the system complies with SILx).

The period of validity is unlimited as long as there are no changes.

4.7.2 REVIEW AND CERTIFICATION DECISION

The decision whether or not to award certification or not is taken by a Certification Commission including (in application of the CERTIFER's procedures) members who did not participate in the safety assessment. The committee bases its decision on:

- The contents of the Assessment Report ;
- The conclusions of the QMS audit, if any ;
- The results of its "technical review" ;
- The presentation made by the assessment team ;
- The answers provided by the assessment team to its questions.

The Certification Commission is responsible for taking decision to issue a new certificate, to approve the extension or renewal of the ISA certificate, to suspend and withdraw the certificate.

Major and minor non-conformities can be identified during the assessment. A major non-conformity cannot lead to the edition of a certificate. Major non-conformities have to be corrected within a given period in order to obtain or maintain the certificate.

In order to mitigate a situation of major non-conformity, the applicant may, alternatively, do one or more of the following:

- Correct the product or system under assessment
- Establish conditions for use of the product or the system and other restrictions

On the contrary, minor non-conformities do not prevent the certificate from being issued. However, the accumulation of minor non-conformities leads to a lack of confidence in the system's efficiency. It is up to the Certification Commission to check whether an accumulation of minor non-conformities during the assessment is likely to compromise the issue of the ISA certificate.

In addition, when one or more quality audits have been carried out, there must be no major non-conformities, and any minor non-conformities identified during the audit must be associated with an action plan validated by the Lead Auditor.

Certification Commission vote

The certification decision is subject to a vote (in application of the CERTIFER's procedures).

- Only members of the Commission not implicated in the assessment can vote ;
- Each voting member has one vote ;
- Decisions are taken by simple majority without any negative vote ;
- Each abstention or negative vote shall be justified in writing.

In case a negative vote has been pronounced, then the application must be reconsidered.

In case of positive vote, without comments from the Certification Commission, the final version of the documents of the certification file can be submitted to the relevant persons to perform the final signatures.

4.7.3 COMPLAINTS AND APPEALS

CERTIFER makes 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.

4.7.4 USE OF THE CERTIFICATION BODY'S MARK

Type certification does not permit the marking of products, packaging, notices or guarantee certificates, nor the affixing of the CERTIFER's logo on any medium whatsoever.

However, the holder may refer to the certificate in declarations of conformity and suitability for use, as well as in correspondence, technical files, commercial offers, etc. In this case, he must provide :

- Either all the information on the certificate (including the list of its appendixes) ;
- Or all the information appearing on the certificate and its Appendixes,

in order to avoid any confusion about the scope of the certification.

In order to be able to refer to the certification on product-specific publicity documents (brochures, leaflets, advertising materials, audiovisual media, websites, etc.), the holder must have received prior authorisation to use a logo created by the certification body. The certification body will send the logo and its conditions of use to the applicant.

This authorisation is, of course, only valid for the actual period of validity of the certificate, i.e. it ceases in the event of suspension, withdrawal or cancellation. An ISA certificate and its use cannot be transferred, even to a third party licensee or successor.

4.7.5 SURVEILLANCE OF THE CERTIFICATE

CERTIFER applies the procedures for the surveillance, maintenance and renewal established in compliance with ISO 17065.

CERTIFER carries out surveillance during the period of validity of the certificate.

The holder may be contacted to examine any changes made to the certified system or the holder's quality system, as well as any complaints that may have been made. It is understood that information concerning:

- Changes made to the system ;
- Changes made to the quality system ;
- Complaints received,

likely to call into question the validity of the certificate, must in any event be notified to CERTIFER no later than one month after they occur.

5. APPENDIX 1: ACCEPTANCE OF TEST RESULTS

This note summarises the requirements, derived from standards (including ISO/CEI 17065 [Reg 1]), in order to ensure that the test results have been obtained under conditions that guarantee their validity.

The respect of the conditions below are verified by CERTIFER.

If compliance with the following 3 categories of requirements is, in CERTIFER 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 additional information.

Depending on the answers and new evidences provided by the customer, the assessor may either close the point or change 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.

A. CONTENT OF THE TEST REPORT (OR ANY OTHER COMPARABLE DOCUMENT)

To be admissible, the test report must include at least :

	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.
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.

B. EN ISO/IEC 17025 ACCREDITATION

<u>For all tests (EMC, Environment...) except functional tests</u>

- **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 an audit carried out by a third-party, covering the specific application, the specific techniques and conditions under the test was carried out.
- **Other cases**
  Acceptance of the report presenting the test results is subject to the results of a third-party audit of compliance with the requirements of standard EN ISO/IEC 17025.

For functional tests

Unlike EMC tests, environmental tests, etc. (see above), the EN ISO/IEC 17025 standard is not considered to be systematically applicable for QSMS of functional testing, for which the ISO 9001 standard (or equivalent standard) applies.

In addition to the QSMS audits to be carried out as part of the certification program (see §4.5), which already cover several phases including the testing phase, if CERTIFER deems it necessary (e.g depending of the specific features of the project), it may also carry out a specific audit for functional tests in the laboratory or on-site for a specific application, in order to:

- Gauge the relevance of the tools, procedures and methods used and ensure compliance with the requirements of the QSMS ;
- Witness the performance of certain tests (CERTIFER may ask for additional tests to be performed).

C. 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 the assessment must be provided to CERTIFER by correspondence or presented on site.

Note: An accreditation according to EN ISO/IEC 17025, whether fixed or flexible, for the testing activity in question dispenses with the latter requirement.

6. 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

* When Reading by sampling applies (see table below), it is the assessor's responsibility [8]to justify his choice of sampling in the documentation assessed.

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	
System or product safety case				X

[8] From §7.1.2 of ISO 17020: "Where applicable, the inspection body shall have sufficient knowledge of statistical techniques to ensure statistically sound sampling procedures and the correct processing and interpretation of results." As a result, the assessor shall be able to justify his sampling selection.

Documents to be reviewed	NE	FR	SR	CR
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 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 verification reports		X1,X2	X3,X4	
Software validation report		X1,X2	X3,X4	
Software application data validation report (for a specific application configured by application data)		X1,X2	X3,X4	

Note: For SIL0/BI software, product or system:

- Software: In accordance with EN50128 §6.4.2.1, the requirements of this standard shall be met, but where a certificate attesting to compliance with standard EN ISO 9001 is available, no assessment is be required.
- System, product: In accordance with EN50129 §5.3.15, the ISA shall only assess the conformity and correctness of the process up to the allocation of the SIL (phases 4 and 5 of the life cycle). No other activities are required.

7. APPENDIX 3: QSMS AUDIT APPLIED TO THE PRODUCT OR SYSTEM UNDER ASSESSMENT, IN THE CASE OF A CERTIFIED QMS

Preamble: According to standards EN 50126/50128/50716/50129, 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)

8. APPENDIX 4: CROSS-ACCEPTANCE METHODOLOGY

"Cross-acceptance" designates the simplified process for assessment in case of existing assessment.

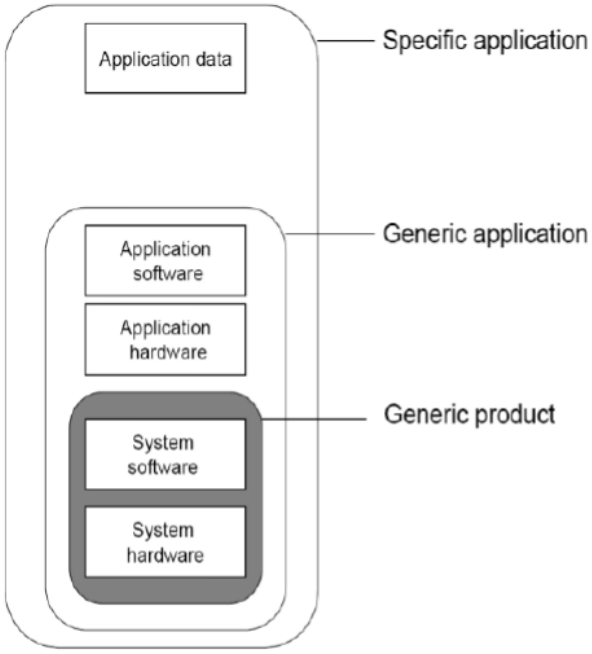
CENELEC provides several definitions:

- **Cross-acceptance:**
  Status achieved by a product that has been accepted by one authority to the relevant standards and is acceptable to other authorities without the necessity for further assessment [EN 50129 § 3.1.7]

- **Acceptance:**
  Status achieved by a product, system or process once it has been agreed that it is suitable for its intended purpose [EN 50126-1 § 3.1]

- **Authority:**
  Body responsible for delivering the authorization for the operation of the safety-related system [EN 50126-1 § 3.65]

An existing assessment can be encountered in the GP/GA/SA organisation defined by CENELEC to structure GPSC/GASC/SASC Safety Cases:



For example:

- A GA project relies on one or several GP projects.
- A SA project relies on one or several GA projects.

CENELEC provides also other definitions:

- In case of re-use or adaptation of a system with previous acceptance, a mutual recognition (sometimes referred to as cross acceptance) of previous acceptance may be applied limiting

the effort on the related lifecycle. This case is considered as a special case of tailoring. This case may also be applied to specific application of a defined generic product / application as defined in Clause 8 [EN 50126-1 § 6.5.4]

- Cross-acceptance is aimed at the acceptance of generic products or generic applications that can be used for a number of different specific applications, and not at the acceptance of any single specific application. [EN 50129 § Intro]
- When using a previously accepted Generic Product or a Generic Application in the context of a Specific Application, safety acceptance should be based on existing related independent safety assessment (i.e. cross-acceptance). No cross-acceptance shall be possible for Specific Applications [EN 50129 § 8.1]

To achieve this objective, CERTIFER has defined a procedure for cross-acceptance. The table below provides the checklist to be implemented by the ISA to perform a cross-acceptance.

See also Recommended Practices [Reg 26] for adaptation of an existing product or system and [Reg 27] for use of pre-existing items.

This table shall be included in the Assessment Report together with the evidence of the verification done by the assessor.

CHECKLIST	GUIDANCE FOR THE VERIFICATION
Cross-acceptance of the ISA (may not be CERTIFER) - Independence and competency	
The competence of the ISA is relative to the product or subsystem assessed	- Check if the ISA has an accreditation to ISO/IEC 17020 or 17065 covering the relevant technical scope (either RST, CCO, CCT) in respect to the product. - Otherwise, review the CV of the assessor.
The competence of the ISA is relative to the standards and methods used in the assessment	- Check if the ISA has an accreditation to ISO/IEC 17020 or 17065 for CENELEC standards EN 50126, EN 50128, EN50657, EN50716, EN 50129 or IEC 61508. - Otherwise, review the competences of the assessor.
The ISA shall have the level of independence as defined in EN 50128 (fig. 2) / EN 50129 (fig. 6) depending on the SIL of the item under assessment	- Check if the ISA has an accreditation to ISO/IEC 17020 or 17065. - Otherwise, review the competences of the assessor.
Cross-acceptance of the ISA (may not be CERTIFER) - Assessment Results	
The item under assessment is well defined (description, documents, software configuration, ...)	- Check if there is a sufficient description of the architecture, functions, etc. - Check if there is a delivery sheet or a release note.
The standards or other normative documents used are well defined and appropriate	- Check if the assessment referential is specified. - Check if it is compatible with the one applicable by the project that does the cross-acceptance.
The methodology used by safety assessors is well defined and appropriate	- Check if the methodology is specified. - Check if it is compatible with the one authorised by CENELEC (see EN 50129 § 5.3.15: appropriate assessment methods, such as interviews, analyses, audits, witnessing tests, physical inspections).

CHECKLIST	GUIDANCE FOR THE VERIFICATION
The environment of the product (physical, CEM, technical, functional, ...) is well defined and appropriate	- Check if the environment is specified. - Check if it is compatible with the one applicable by the project that does the cross-acceptance.
The scope and/or the limits of validity of the safety assessment result are well defined	Check if there is a sufficient description. e.g. in case of a GA project to be cross-accepted by the SA project: Has the generic application data process been assessed? See [Reg 28]
Establishment of SRACs (including exported constraints)	Check the applicant has established SRACs (including exported constraints) and that the ISA has accepted them. Note that the verification of the coverage of these SRACs (including exported constraints) is not part of the cross-acceptance activity but is part of the assessment activity (the evidence is generally provided either in the Safety Case or in the Hazard Log to be assessed).
Conclusion of the assessment report	- Check that the report concludes on the achievement of the safety objective from the referential and provides the SIL achieved. - Check if the SIL achievement is subject to the respect of clearly identified SRAC. - Check if there are other restrictions and limitations.