FUNCTIONAL SAFETY CERTIFICATION
PROGRAM & MARK GUIDANCE

Guidance Document for Intertek's Functional Safety Propriety Standard (INT/FS/2019) and Certification Program for Industrial Automation, Process Machinery, and Associated Equipment

intertek.se/provning/functional-safety

CONTENTS

INTRODUCTION

Machine safety is one of the most rapidly growing areas of importance in industrial digitisation and automation – an important aspect of Industry 4.0, robotics, smart buildings, and smart cities. New safety strategies offer manufacturers a way of improving productivity and competitiveness in the market. Safety becomes an integrated part of machine functionality and operability, rather than as an after-thought added on to meet regulation.

In developed economies, national laws require that machines meet essential health and safety requirements, meaning new machinery must meet basic requirements when imported and supplied to the manufacturing base. Manufacturers comply by designing machines to meet international standards specifically for machine safety. These standards are recognized globally and equivalency charts between requirements facilitate machinery trade and shipments between countries.

Functional Safety (FS) is an engineering process that emphasizes safe design, operation, and control of protection systems as individual components, sub-assemblies, and complete machines to mitigate unreasonable risk caused by the application of the system. Best practice in functional safety is not to simply conform to industry standards and protect against accidents, but to drive a more effective and productive operation, reducing downtime and costly repairs to equipment. Manufacturers that adopt FS into their processes and equipment will have the advantage of an internationally recognized safety rating that enables their solutions to be sold on a global stage.

Machine systems designed for functional safety risk mitigation and hazard reduction provide:

- Increased machine safety
- Availability (reduced downtime)
- Reliability (on demand durability)
- Maintainability (lifecycle capability)
- Increased productivity (performance)
- Cost efficiencies

There are various FS standards for different disciplines that address necessary safety measures, potential failures, development requirements, and recommendations for a specific safety critical system. One such standard that addresses the general functional safety requirements for machine systems design is the ISO 12100 standard.

Intertek's Functional Safety Propriety Standard (INT/FS/2019) has been developed with the objective to satisfy each stakeholder of the industrial value chain. Our modular solutions provide flexible options for manufacturers, while our comprehensive services and certifications provide industrial stakeholders the option to review safety measures in more detail, a common request from buyers and regulators.

This guidance document defines the evaluation and validation process for the determination of machine design using international standards, national standards, and the Intertek Functional Safety Propriety Standard (INT/FS/2019) as reference material for a risk-based reverse design evaluation approach in order to validate and certify the functional and general safety of machines.

SECTION 1

CONFORMITY FRAMEWORK

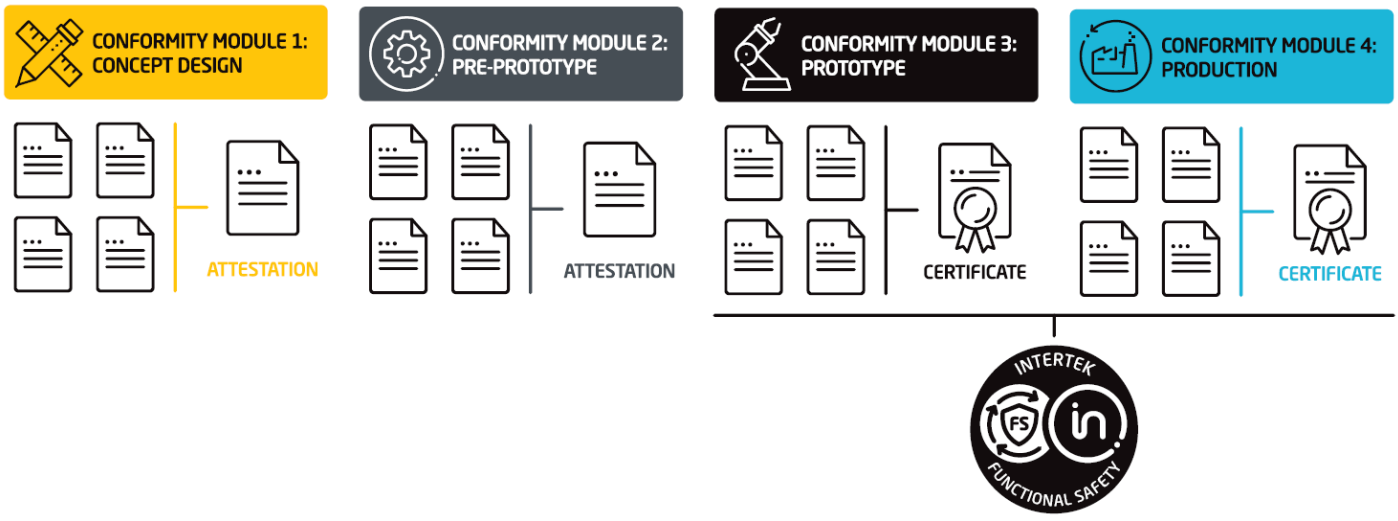
The primary purpose of this guide is to provide an overview of the conformity framework for the Intertek methods to be used to validate the design integrity and to determine claimed machine safety, performance levels (PL), and safety integrity levels (SIL) of machinery leading to the awarding the Intertek Functional Safety (FS) Mark.

The approach taken is risk based and validation of design basis by calculation, using IS0 12100 as the basic horizontal standard, Intertek Functional Safety Propriety Standard (INT/FS/2019), and specific equipment or product standard/s as the vertical platform for the consideration of machine design basis, machine design evaluation, risk assessment, validation, verification, and inspection methodologies.

INT/FS/2019 Proprietary Standard:

- Modular Levels of Conformity Approach
- Engineering Block Structures
- Risk-Based Approach / Design Evaluation Method
- PL and SIL Calculations
- Hardware and Software Integration

Whether you are at the stage of concept design, pre-prototype, prototype, or incorporating all safety elements within production, our modular functional safety solutions provide industrial stakeholders the option to review the safety requirements in more detail.



The outcome of this conformity assessment approach is the validation of performance levels (PL) and safety integrity levels (SIL) claimed, and general safety for the purpose of granting certification and marking (FS Mark) of machine systems or processes in accordance to the critical decision path of ISO/IEC 17065 process for product certification methods. Those methods being application, evaluation, certification review, and certification final decision for the conformity of complete systems, sub systems, or component/individual standalone equipment level.

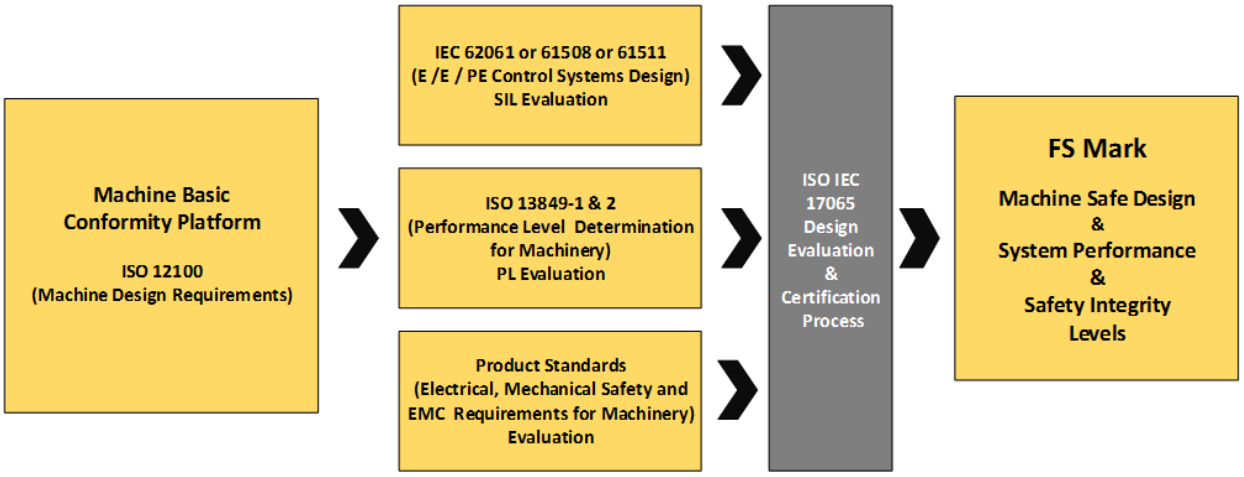


Fig 1.0 (Example - General Conformity Approach)

SAFETY INTEGRITY LEVELS

SIL stands for safety integrity level and is a means to express the required risk reduction needed to reduce the risk to an acceptable level. According to IEC 61508, the safety levels are 1, 2, 3 and 4 with an order of magnitude increase in safety requirements as you go from one level to the next. SIL 4 is not seen in machinery and factory automation where generally no more than one person is typically exposed to a hazard. It is rather reserved for applications like nuclear and rail where hundreds or even thousands of people are involved.

PERFORMANCE LEVELS

ISO 13849. Its performance levels A, B, C, D, and E can be mapped to the SIL 1 to SIL 3 scale.

Common cycle data (MTTFd) is used for the calculation of both PL and SIL ratings.

Calculation of SIL alone to IEC 6l508 cannot map to PL category A, B, C, D, or E.

The meaning and purpose of functional safety is to protect from harm, foreseen and unforeseen hazards, in the event of real time failure impacting:

- People
- The environment
- The asset (machine)

Functional safety achieves this by design intent on implementation of control and protection concepts that lower the probability of undesired events, thereby minimizing failure across the full life cycle of the machine.

Safety standards define safety as freedom from unacceptable risk. The most effective way to eliminate risks is to design them away. But as risk reduction by design is not always possible or practical, safeguarding with static guards are often the next best option for several reasons. Stopping a machine quickly and safely not only reduces risk but also increases machine uptime and productivity compared with abrupt safety stops. At the same time, the legal obligations are met, and the safety of people, the environment, and the asset are assured.

Functional safety in machinery usually means systems that safely monitor and, when necessary, override the machine applications to ensure safe operation. A safety-related system thus implements the required safety functions by detecting hazardous conditions and bringing operation to a safe state by ensuring that a desired action, e.g. safe stopping, takes place.

BENEFITS

Incorporating Functional Safety design principles provides:

- Reduction of risk levels
- Safe machine design
- Protections and safeguards for: operator, environment, machine life cycle

1.1 System Conformity Framework: General

For the purposes of conformity assessment, Intertek will use ISO 12100 and Intertek Propriety Standard INT/FS/2019 as the risk-based approach, and normative references contained within shall provide the basic safety framework for covering the machine lifecycle by determining safe design, claimed functional safety (PL and SIL), and general safety of machines.

ISO 12100 specifies basic terminology, principles, and a methodology for achieving safety in the design of machinery. It specifies principles of risk assessment and risk reduction for design requirements. These principles are based on knowledge and experience of the design, use, incidents, accidents, and risks associated with machinery.

ISO 12100 defines three types (or 'classifications') of standards representing different levels of granularity:

- Type A standards establish general, overarching guiding principles – all machines (horizontal)
- Type B standards have specific design principles for a specific technology (horizontal)
- Type C standards are application-specific or product standards (vertical)

1.2 Functional Safety (FS) Mark – Conformity Framework (All System Levels)

Overall, ISO 12100 applies to the system level (entire machine), but specific elements trace down to the product or component level. ISO 12100 is a Type A standard that applies to everything that is defined as a machine. Type B standards relate the sub systems or sub-assemblies of the machine, while Type C standards are dedicated to the specific product or machine, or to a component of the machine.

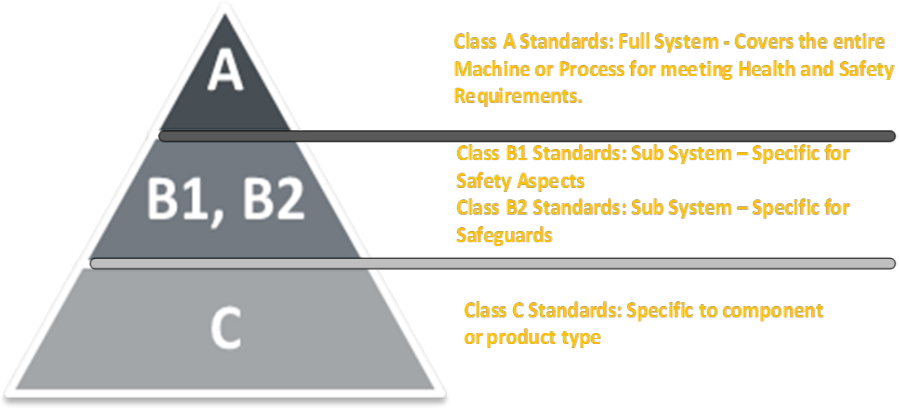


Fig 1.1 (Standards Classification Structure)

1.3 Type A Classification: Systems Conformity Assessment

Table 1.1 illustrates an example of typical Class A standards used for the risk assessment framework of a full systems (the complete machine).

Type A Classification (Full Systems)	ISO Standard
Safety of machinery, general principles for design — risk assessment and risk reduction (full system)	ISO 12100
Robots and robotic devices — Safety requirements for industrial robots	ISO 10218

Table 1.1

1.4 Type B1 Classification: Sub-Systems Conformity Assessment

Table 1.2 provides an example of typical Class B1 standards applied for a sub-systems conformity assessment framework.

Type B1 Classification (Sub-Systems) Specific Aspects	ISO Standard
Fixed and movable guards (safety fences, barriers, covers)	ISO 14120
Interlocking devices associated with guards (interlocking of safety gates, etc.)	ISO 14119
Prevention of unexpected start-up	ISO 14118
Protective devices (light grids, light beam devices, scanners, pressure-sensitive mats, etc.)	ISO 13856
Two-hand control devices	ISO 13851
Adjustable safeguards that restrict access fixed and movable guards	ISO 14120
Emergency stop	ISO 13850

Table 1.2

1.5 Type B2 Classification: Sub-Systems Conformity Assessment

The example given in Table 1.3 is for a typical Class B2 standard applied for sub-systems conformity assessment framework.

Type B2 Classification (Sub-Systems) Functional Safety and Safety-Related Controls	Standards
Safety-related parts of control systems	ISO 13489 IEC 62061
Safety-related requirement of pneumatics	ISO 4414
Safety-related requirement of hydraulics	ISO 4413
General Safety Electrical equipment	IEC 60204 ISO 62061
Electrical Systems and Controls	IEC 61508
Electrical Instrumentation	IEC 61551

Table 1.3

1.6 Type C Classification: Standalone or Component Level

Example of typical Class C standards in Table 1.4 for product conformity assessment framework.

Type C Classification Specific Equipment	Standard
Hydraulic presses	ISO 16092
Robots, robotic systems	ISO 10218 – 1&2
Collaborative robots	ISO TS 15066
Woodworking machines	ISO 19085
Automated guided vehicles (AGV)	ISO 3691
Semi-Conductor Devices	IEC 60747

Table 1.4

SECTION 2

TERMS & DEFINITIONS

Terms and definitions applied under this document reference shall be made in all cases to the specific standards and clauses listed in Table 1.5 below. The year of issue has intentionally been removed on the basis that the current issue of the standard is referred.

Standards & Clauses
ISO 12100: Safety of machinery — General principles for design — Risk assessment and risk reduction, Clause 3.
ISO 10218-1: Robots and robotic devices — Part 1 Robots. Safety requirements for industrial robots, Clause 3.
ISO 10218-2: Robots and robotic devices — Safety requirements for industrial robots. Part 2: Robot systems and integration. Clause 3.
IEC 61508-1: Functional Safety of Electrical / Electronic / Programable Electronic Safety Related Systems, part 1 General Requirements. Clause 3.
IEC 61508-2: Functional Safety of Electrical / Electronic / Programable Electronic Safety Related Systems, part 2 Requirements for electrical/electronic/programmable electronic safety-related systems Clause 3.
IEC 61508-3: Functional Safety of Electrical / Electronic / Programable Electronic Safety Related Systems, part 3 Software requirements. Clause 3.
IEC 61508-4: Functional Safety of Electrical / Electronic / Programable Electronic Safety Related Systems, part 4 Definitions and abbreviations. Clause 3.
IEC 61508-5: Functional Safety of Electrical / Electronic / Programable Electronic Safety Related Systems, part 5 Examples of methods for the determination. Clause 3.
IEC 61508-6: Functional Safety of Electrical / Electronic / Programable Electronic Safety Related Systems, Part 6: Application of IEC 61508-2 and IEC 61508-3. Clause 3.
IEC 61508-7: Functional Safety of Electrical / Electronic / Programable Electronic Safety Related Systems, part 7 Overview of techniques and measures. Clause 3.
IEC 61511 -1: Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware, and application programming requirements. Clause 3.
IEC 61511-2 Functional safety — Safety instrumented systems for the process industry sector —Part 2: Guidelines for the application. Clause 3.
IEC 61511-3: Functional safety — Safety instrumented systems for the process industry sector Part 3: Guidance for the determination of the required safety integrity levels. Clause 3.
ISO 13489-1: Safety of machinery — Safety related parts of control systems. Part 1: General principles for design. Clause 3.
ISO 13489-2: Safety of machinery — Safety related parts of control systems. Part 2: Validation. Clause 3

Table 1.5

SECTION 3
SCOPE

The determination of Performance Level, Safety Integrity Level of Safety Related Parts of a Control System (SRP/CS), and the downstream impacts of machine construction design is subjected to a design evaluation, inspection, and certification process which includes affixing the Intertek Functional Safety Mark. This process applies to the following industry sectors:

- Stand-alone industrial and commercial machinery and equipment
- Stand-alone industrial and service robotics
- Bespoke integrated/automated industrial machinery (incorporating industrial robotics and indexing systems)
- Energy storage and charging systems and automated guided vehicles (AVGs)
- Machine tools
- Automation systems
- Industrial furnaces
- Refrigeration systems
- Packaging machinery
- Agricultural machines
- Food Processing equipment
- Construction equipment
- Equipment for explosive atmospheres
- Mining
- Oil/Gas/Chemical equipment
- Processing
- Earth-moving & tunnelling
- Cranes/Lifts/MHE
- Forestry/Plant machinery
- And many others

SECTION 4

ENGINEERING BLOCK STRUCTURES

To evaluate and determine machine performance and safety integrity levels, including upstream and downstream impacts on the overall machine design, engineering block structure architecture is used by selection of Classification Levels A, B1, B2, and C, which form the overall conformity approach upon selection.

The example below in Figure 1.2 represents a fully integrated automated machinery system, incorporating standalone machines integrated together to form one complete end-to-end machine system.

Class A (+Class C) Engineering Block Structure:

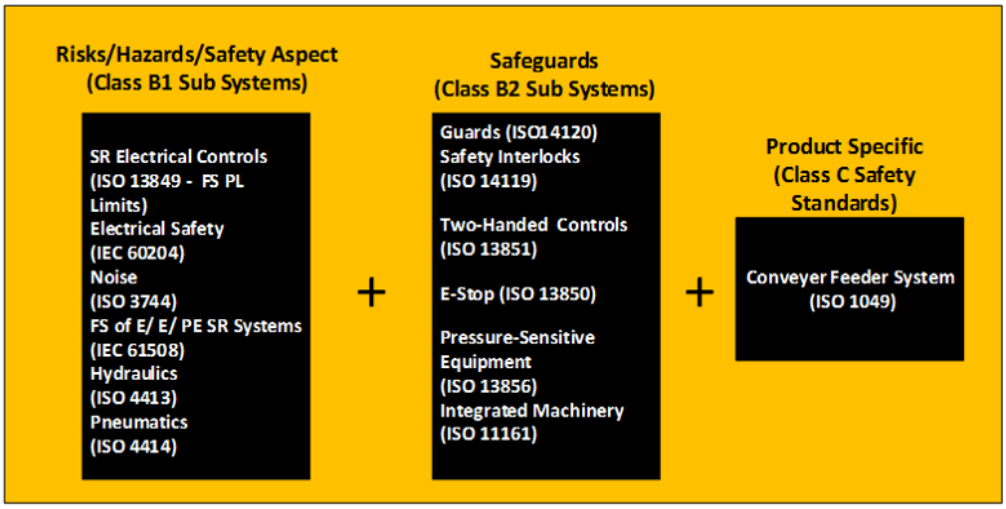


Fig 1.2 (Class A + Class C)

SECTION 5

CONFORMITY MODULES

5.1 All machinery on application for functional safety shall be subject to a design evaluation, validation, verification, and certification process using ISO 12100 as the basis of conformity.

5.2 Pending the machine status within the design stage gate, conformity is determined based on subjecting the machine design to a defined evaluation module, each module uses selected clauses from ISO 12100 to determine machine conformity by reverse design calculation as a means of validating and verifying the design intent or protection concept incorporated into the intended design or build construction of the machine (Intertek Propriety Standard (INT/FS/2019)).

5.3 The four conformity modules are and illustrated in Figure 1.3 below:

- Conformity Module 1 - Concept (Design Phase)
- Conformity Module 2- Pre-prototype (1st Build)
- Conformity Module 3 - Prototype (Pre-Production Build Phase)
- Conformity Module 4 - Production (In service build)

General outline of design stage gate and conformity module deliverables:

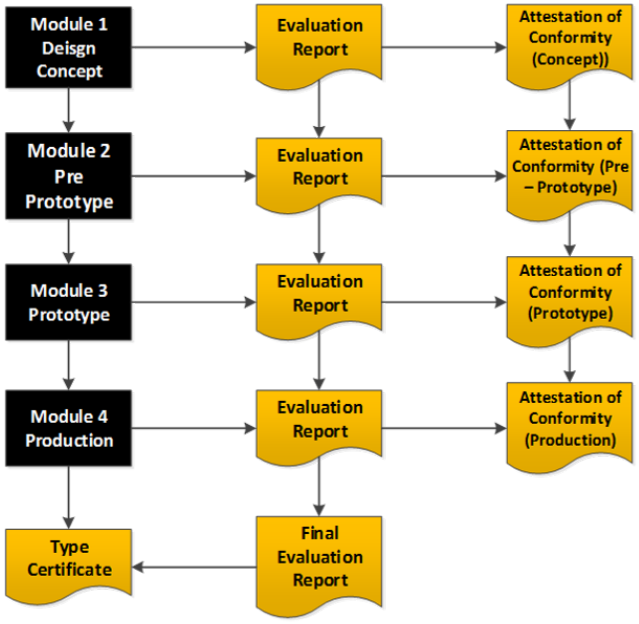


Fig 1.3 (Basic Modules of Conformity)

5.4 This figure illustrates the variation of selected clauses of Class A & B standards applied per specific conformity module when applicable for the determination of conformity.

5.5 Each FS conformity module (ISO 12100 basic level) shall follow the same process of evaluation by breaking down the risk assessment into four sub modules. This sub module approach is designed to identify, quantify, validate, and evaluate the risk as illustrated by Figure 1.4 below.

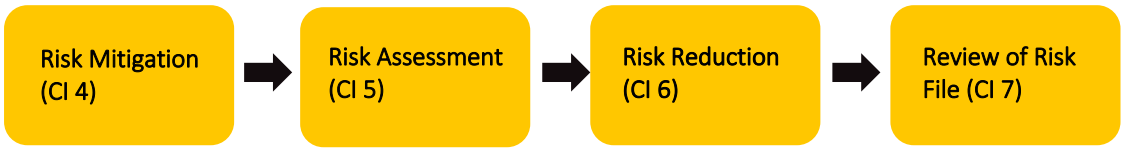


Fig. 1.4 (Basic Conformity Approach Topics)

5.6 The engineering block structure as defined within the previous section, Class A standard (ISO 12100), is the horizontal basis for the machine end-to-end design evaluation incorporating Class B1 and B2 standards to evaluate by calculation for claimed PL (ISO 13489) and SIL (IEC 62061, 61508, and 61151 Standards series).

Note: Electrical safety of machines is not covered by any of the Functional Safety Standards ISO 13489, IEC 61508, or IEC 61511 series. For Electrical Safety refer to IEC 60204 series standards.

5.7 The described same modular approach and sub-module structure, in addition to using the engineering block structure shall be applied to:

- The complete machine, known as the full system
- A sub system or sub assembly of the complete machine
- A component part of the complete machine or standalone machine

SECTION 6

CERTIFICATION: GENERAL REQUIREMENTS

Overview

6.1 The general certification process to be followed for the evaluation of a complete machine, sub system, assembly, component, or standalone product leading onto the award of an attestation of conformity or type certificate and affixing of the Intertek Functional Safety (FS) Mark shall be that outlined in ISO/IEC 17065 and 17067.

6.2 In all cases, the conformity assessment system to be adopted for issuing an attestation of conformity or type certificate shall undergo a Type 1, 1a, or 3 conformity approach in accordance with ISO IEC 17067.

6.3 In accordance with ISO 17065, the process for the evaluation of functional safety and the safe design of a full system (complete machine assembly or standalone machine), sub-system or part assembly of a full system shall undergo and be subject to:

- An application by the applicant for certification (Intertek FS Mark)
- Signing of a certification agreement specific to the FS Mark and certification program.
- Draw up of the certification plan (defining the standards classification, engineering block structure and conformity module applied).
- Evaluation and validation by design evaluation of the manufacturers risk assessment/FMEDA for the full system, sub-system or assembly, or standalone product/component level, PL and SIL claims and applied factor of safety (FoS) applicable to the safety levels applied to the build construction by assessment to a defined module of conformity and applicable C classification standards.
- Verification of critical build/assembly aspects related to the construction build by onsite inspection of key elements identified from the design evaluation/testing and validation phase.
- Technical review for certification by validation that the full system (complete machine), subsystem or assembly or standalone product/component meets the conformity module applied and confirms the PL and SIL claim before recommending an attestation or type certificate of E.
- Final certification decision is made by ensuring all the steps proceeding the final decision have been carried out in full before issuing any certification and awarding the affixing of the Intertek FS Mark.

APPLICATION REVIEW
↓
PLANNING PHASE
↓
DESIGN EVALUATION
↓
MANAGEMENT OF FUNCTIONAL SAFTEY (FS MARK ONLY)
↓
VALIDATION
↓
REVIEW PHASE
↓
CERTIFICATION PHASE

Certification Process

6.4 All calculations and value tables (example MTTFd values) used for the means of design evaluation and validation confirmation related to functional safety or safe machine design shall be derived from normative functional safety standards, product, engineering application standards, and known art from engineering science reference material.

6.5 The design evaluation, validation, and verification (inspection) shall be conducted to confirm overall safe build of the full system, subsystem or assembly, or standalone product/component by reverse design engineering techniques (calculation check) or application of engineering knowledge of sound engineering practices (SEP) and documented by engineering statement confirmation of design intent as to the safety integrity of the design build.

6.6 Attestations of conformity shall be issued on successful evaluation, validation, verification, certification review, and final decision by undergoing and meeting the applicable requirements of conformity modules 1 and 2 in full, issued for full systems (complete machines), subsystems or assemblies, or product/component level at the following design stage gate levels:

- Conformity Module 1 - Concept (Design Phase)
- Conformity Module 2 - Pre-Prototype (1st Build)

Not under any circumstances can a type certificate bearing the Intertek FS Mark be issued for only completing conformity modules 1 and 2.

6.7 A full type certificate bearing the FS Mark shall be issued on successful evaluation, validation, verification, certification review, and final decision by undergoing and meeting the applicable requirements of conformity modules 3 and 4 in full, issued for full systems (complete machines), subsystems or assemblies, or product/component level at the following design stage gate levels:

- Conformity Module 3 - Prototype (Pre-production Build Phase)
- Conformity Module 4 - Production (In-service build)

6.8 Certificate ongoing validity for an attestation of conformity or type certificate depends on the type approved remaining to type during its life cycle. Authorised design changes impacting the PL, SIL, FoS, and general safety integrity can only be approved by the issuing body.

Functional Safety Mark Usage

6.9 Unauthorised design changes impacting the PL, SIL, FoS integrity, and general safety shall result in the issued certificate and FS Mark being withdrawn and the application for license (FS Mark) terminated.

6.10 Abuse or unauthorised use of the Intertek FS Mark by false claim or by advertising through inappropriate use in all cases shall result in the FS Mark being withdrawn and the application for licence use (FS Mark) terminated.

6.11 The Intertek Functional Safety (FS) Mark, as illustrated below, shall be awarded on successfully completing the conformity assessment approach as detailed the section "Evaluation, Validation and Verification" and demonstrated by Figure 1.5.

Fig. 1.5

Note: "Claims" in the sample Mark above will be annotated with the claim of capability to respective functional and general international and national standards.

Functional Safety Type Examination Certificate: Example

6.12 Example of the functional safety type examination certificate issued for successfully meeting conformity modules 3 and 4:

intertek
Total Quality. Assured.

Type Examination Certificate

Certificate Number: BBB-SSS-NNNNNNNRn
Page 1 of 3

<Intertek Office> hereby confirms the below listed <equipment / component> on satisfactory evaluation is authorised to affix the Intertek Functional Safety Mark:

Model: <Model Name & Description & Rating / Characteristics>

Manufacturer: <Legal Entity & Full Address>

Has been evaluated in accordance to below listed Standards and deemed to provide a Performance Level (PL) CAT X and Safety Integrity Level (SIL) Y

Standard:	Title:

The decision to recommend affixing the Functional Safety Mark is based on satisfactory Certification Review of the following reports:

Report Number:	Issuing Body:

Safety Function:

Limitations:

Validity Date: <dd mm yyyy>

✓ Claim 1
✓ Claim 2
✓ Claim 3
✓ Claim 4

Signature
<Name>
Certification Officer
Issue Date: <dd mm yyyy>

SAMPLE

This Certificate is for the exclusive use of Intertek's client and is provided pursuant to the agreement between Intertek and its Client. Intertek's responsibility and liability are limited to the terms and conditions of the agreement. Intertek assumes no liability to any party, other than to the Client in accordance with the agreement, for any loss, expense or damage occasioned by the use of this Certificate. Only the Client is authorized to permit copying or distribution of this Certificate and then only in its entirety. Any use of the Intertek name or one of its marks for the sale or advertisement of the tested material, product or service must first be approved in writing by Intertek.

<Intertek Legal Entity Address>

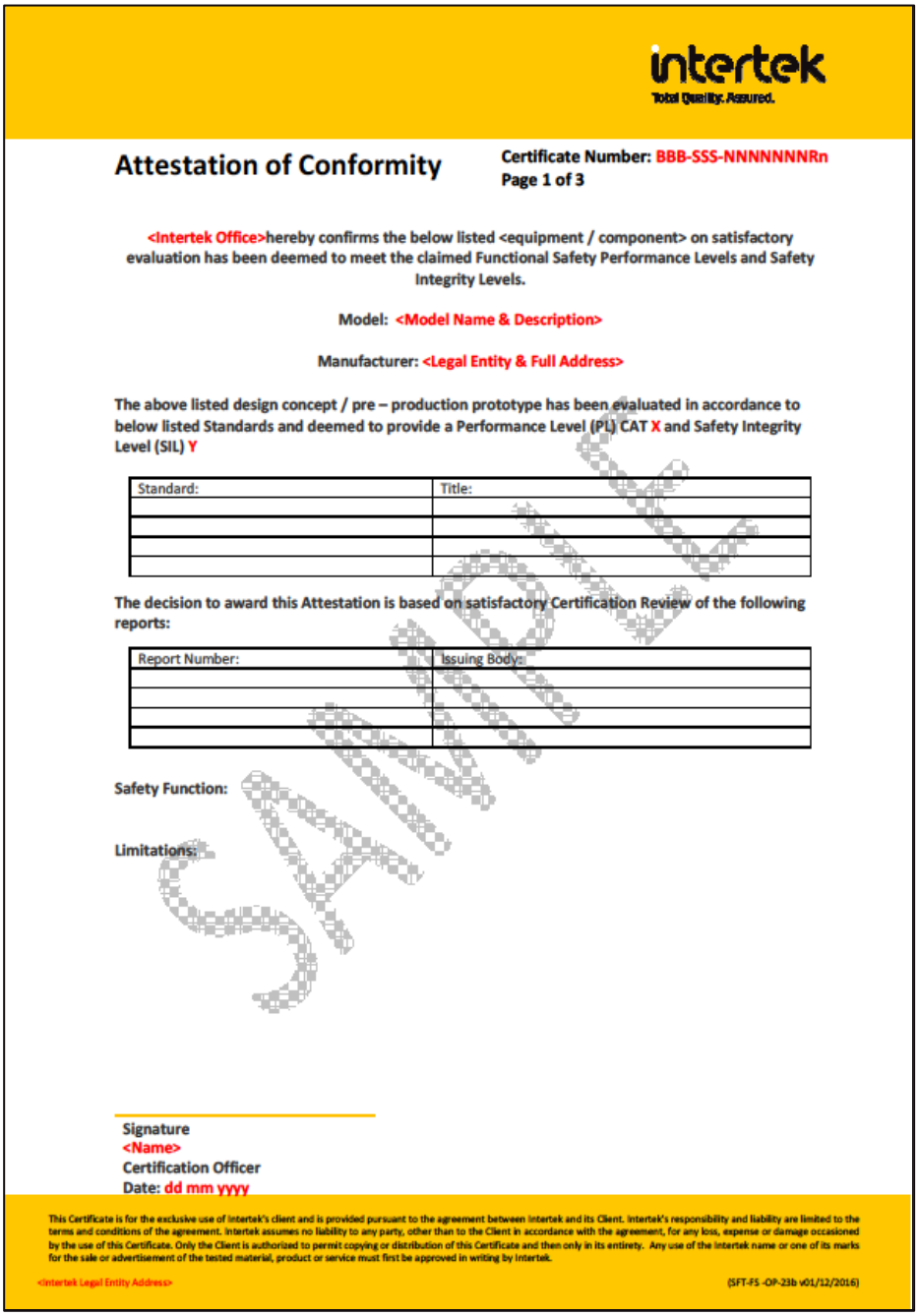
(TF-FS -OP-23a V1 14 May 2020)

TYPE EXAMINATION CERTIFICATE

- Type Approval Certificate
- Issued for complete Machine Systems conforming to Modules 1–4
- Issued for E/E/PE Control Systems
- Issued for Component Level/ Standalone Machines
- Covers Management of Functional Safety (IEC 61508-1 Cl 6)
- Intertek Functional Safety Mark
- 5 Year Certificate Validity Period
- Product Conformity to Class A, B1, or Class C standards and supporting evaluation reports
- PL & SIL calculated results
- PL and SIL validated Levels
- Reference to Evaluated Technical Construction File and Contents
- Accredited to ISO IEC 17065

Functional Safety Attestation of Conformation Certificate: Example

6.13 Example of the functional safety attestation of conformity certificate issued for successfully meeting conformity modules 1 and 2.



intertek
Total Quality. Assured.

Attestation of Conformity

Certificate Number: BBB-SSS-NNNNNNNRn
Page 1 of 3

<Intertek Office>hereby confirms the below listed <equipment / component> on satisfactory evaluation has been deemed to meet the claimed Functional Safety Performance Levels and Safety Integrity Levels.

Model: <Model Name & Description>

Manufacturer: <Legal Entity & Full Address>

The above listed design concept / pre – production prototype has been evaluated in accordance to below listed Standards and deemed to provide a Performance Level (PL) CAT X and Safety Integrity Level (SIL) Y

Standard:	Title:

The decision to award this Attestation is based on satisfactory Certification Review of the following reports:

Report Number:	Issuing Body:

Safety Function:

Limitations:

SAMPLE

Signature
<Name>
Certification Officer
Date: dd mm yyyy

This Certificate is for the exclusive use of Intertek's client and is provided pursuant to the agreement between Intertek and its Client. Intertek's responsibility and liability are limited to the terms and conditions of the agreement. Intertek assumes no liability to any party, other than to the Client in accordance with the agreement, for any loss, expense or damage occasioned by the use of this Certificate. Only the Client is authorized to permit copying or distribution of this Certificate and then only in its entirety. Any use of the Intertek name or one of its marks for the sale or advertisement of the tested material, product or service must first be approved in writing by Intertek.

<Intertek Legal Entity Address>

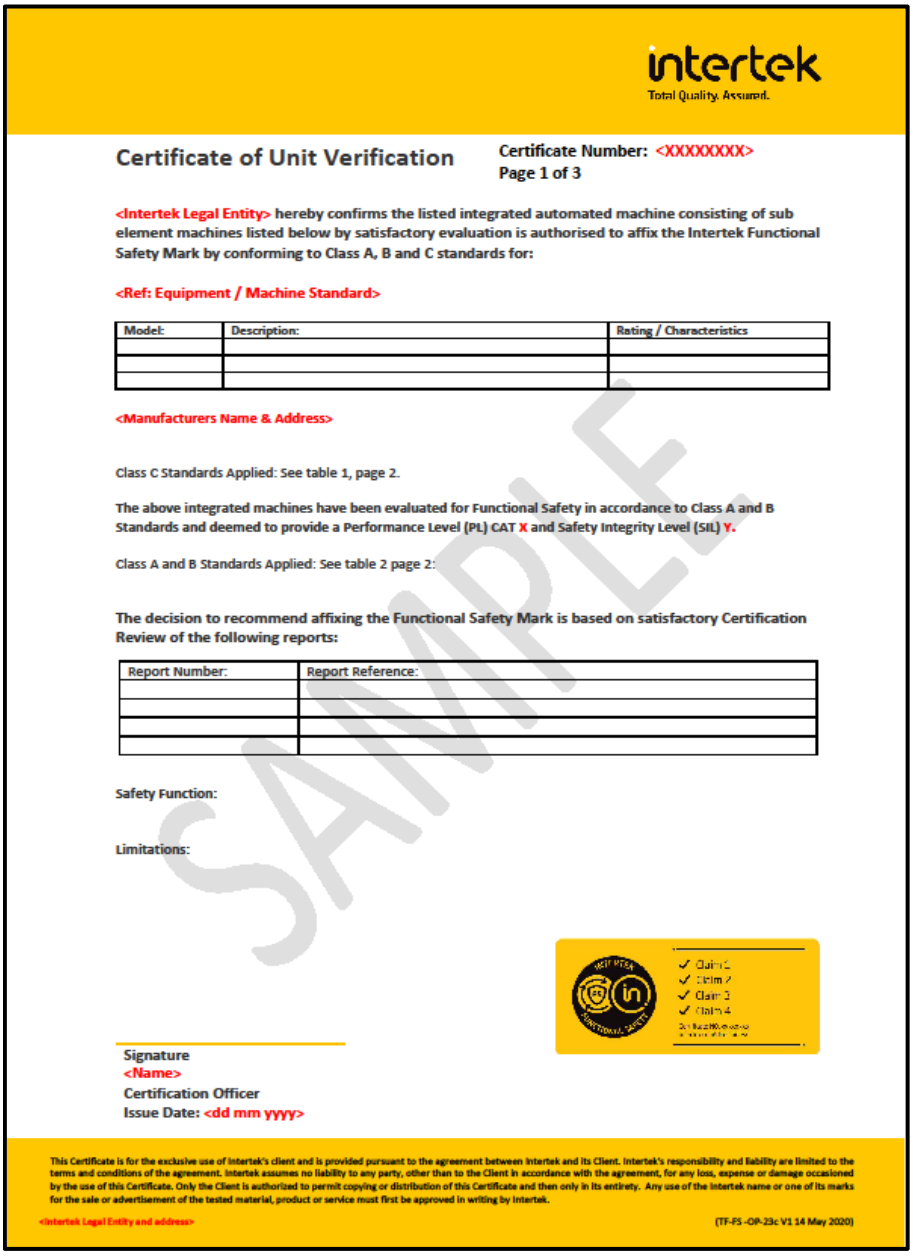
(SFT-FS -OP-23b v01/12/2016)

ATTESTATION OF CONFORMITY

- Issued as Type Approval on completing only Modules 1–4
- No Validity Period
- Issued for either PL rating or SIL rating, or both
- Validation using A, B, and C classifications
- Issued for concept or pre prototype design stage
- Issued for production or prototype stage of build
- Intertek Functional Safety Mark not awarded
- Reference to Evaluated Technical Construction File and Contents
- Accredited to ISO/IEC 17065

Functional Safety Certificate of Unit Verification: Example

6.14 Example of the functional safety Certificate of Unit Verification issued for bespoke machines.



intertek
Total Quality. Assured.

Certificate of Unit Verification

Certificate Number: <XXXXXXXX>
Page 1 of 3

<Intertek Legal Entity> hereby confirms the listed integrated automated machine consisting of sub element machines listed below by satisfactory evaluation is authorised to affix the Intertek Functional Safety Mark by conforming to Class A, B and C standards for:

<Ref: Equipment / Machine Standard>

Model:	Description:	Rating / Characteristics

<Manufacturers Name & Address>

Class C Standards Applied: See table 1, page 2.

The above integrated machines have been evaluated for Functional Safety in accordance to Class A and B Standards and deemed to provide a Performance Level (PL) CAT X and Safety Integrity Level (SIL) Y.

Class A and B Standards Applied: See table 2 page 2:

The decision to recommend affixing the Functional Safety Mark is based on satisfactory Certification Review of the following reports:

Report Number:	Report Reference:

Safety Function:

Limitations:

SAMPLE

✓ Claim 1
✓ Claim 2
✓ Claim 3
✓ Claim 4

Signature
<Name>
Certification Officer
Issue Date: <dd mm yyyy>

This Certificate is for the exclusive use of Intertek's client and is provided pursuant to the agreement between Intertek and its Client. Intertek's responsibility and liability are limited to the terms and conditions of the agreement. Intertek assumes no liability to any party, other than to the Client in accordance with the agreement, for any loss, expense or damage occasioned by the use of this Certificate. Only the Client is authorized to permit copying or distribution of this Certificate and then only in its entirety. Any use of the Intertek name or one of its marks for the sale or advertisement of the tested material, product or service must first be approved in writing by Intertek.

<Intertek Legal Entity and address>

(TF-FS -OP-23c V1 14 May 2020)

CERTIFICATE OF UNIT VERIFICATION

- Type Approval Certificate
- Issued for bespoke Integrated Complex Machines & Systems
- Issued for bespoke Standalone Complex Machines & Systems
- No Assigned Period of Validity
- Type Approval Based on Single one-off Design
- Product Certification Conformity (Class A, B1, or Class C)
- PL & SIL Determined
- PL / SIL calculated results
- FSM Required - IEC 61508-1 Cl 6 as a single one-off event
- Intertek Functional Safety Mark awarded
- Reference to Evaluated Technical Construction File and Contents
- Accredited to ISO IEC 17065

SECTION 7

CONFORMITY MODULES/VALIDATION: GENERAL DESCRIPTION

7.1 Reference to Class A, B, and C standards shall be used for the evaluation and validation of functional safety claims for PL, SIL, and machine safe design. To be achieved by validating (by calculation) and determination of design FMEDA risk assessment outputs (ISO 12100) and overall general machine design (determination of FoS and SEP applied). Thereby demonstrating the machine's intended safety function(s) during its life cycle and risk has been adequately reduced.

7.2 Demonstration of PL, SIL, and machine safe design, engineering block structure architecture, and conformity modules are combined and, when applied, form the FS conformity evaluation method for:

- Full systems (complete machine or integration of multiple machines) – Class A
- Sub-systems (example SR control systems of a full system) – Class B
- Standalone machines or component(s) – Class C

7.3 Selecting the appropriate modules of conformity to determine the evaluation and validation method for FS, PL, SIL, and integrity of machine safety to be applied depends on the stage gate design build status of the machine.

7.4 The conformity modules (1, 2, 3, and 4), when applied as the evaluation and validation methods, cover the general design intent and safety considerations associated with industrial machinery and that of the automotive industry for related hazards using ISO 12100 (Class A) as the vertical standard for respective engineering applications within the build construction:

- Mechanical
- Environment
- Chemical
- Electrical
- E/E/P control systems
- Software
- Cybersecurity (Optional)
- Ergonomics
- Commissioning
- Operability
- Maintenance
- Transportation

Engineering Block Structures

7.5 The Functional Safety conformity approach to determine PL, SIL, and overall machine safety is by selection of Class A + B1 + B2 + C standards, a process demonstrated by forming an engineering block structure. For example, a pre-production industrial integrated material processing unit incorporating an input feeder and output conveyer system is illustrated by Figure 1.6 and Table 1.6.

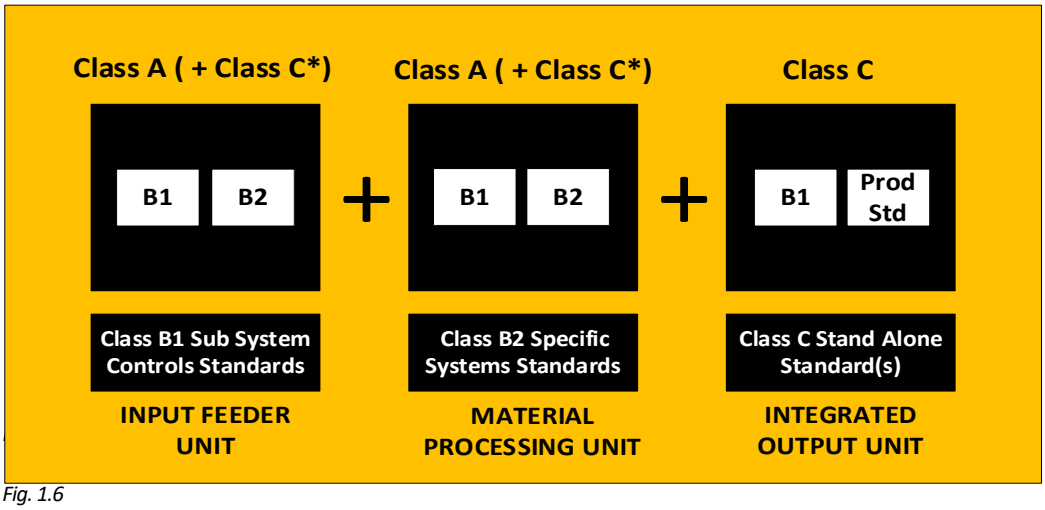


Fig. 1.6

Machine	FS Conformity Module	Classification	FS Conformity System (Process)	Machine Controls Evaluation	Applied Reference Standards	FS & M/C Design Evaluation
Material Processing Unit	4	A	A	A	ISO 12100 & 14121	M/C Design Risk Assessment Evaluation
			B	B2	IEC 61508-1	General - SIL Requirements
			B	B2	IEC 61508-2	Hardware - SIL Calculation
			B	B2	IEC 61508-3	Software - Evaluation
			B	B2	ISO 13489 -1 & 2	Safety of Electrical Control Systems - PLr Calculation
				B2	IEC 60204	Machine Electrical Safety
				B2	ISO 4413	Hydraulics
				B2	ISO 4414	Pneumatics
				B1	ISO 13850	Emergancy Stops
				B1	ISO 14118	Unexpected Start Up
				B1	ISO 14119	Interlocks
				B1	ISO 14120	Fixed Moveable Guards
				B2	ISO 11161	Machine Integration
Conveyer			C	C	ISO 1049	Conveyer Feeder System

Table 1.6 (Module 4: Standards Classification A, B and C to be applied)

SECTION 8

EVALUATION, VALIDATION, & VERFICATION

8.1 The general approach for the evaluation, validation, and verification leading to certification of the full system machine, sub-system, or component/standalone machine for general safety, PL, and SIL is illustrated by the process flow diagram Figure 1.7 below:

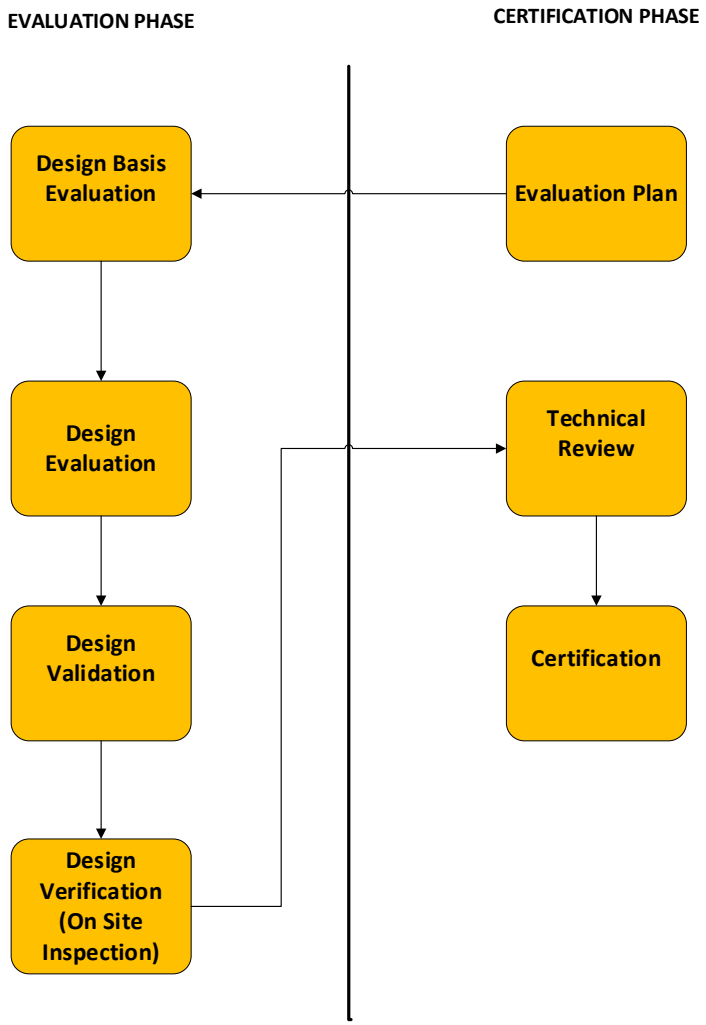


Fig. 1.7 (Conformity Approach Evaluation, Inspection and Certification)

8.2 Design Basis Evaluation

8.2.1 Depending on the stage gate cycle of the construction build the conformity module to be applied shall be selected the from Table 1.8 below:

Conformity Module	Life Cycle Stage Gate
1	Design Concept (Design Phase)
2	Pre-Prototype (First Build)
3	Prototype (Production Phase)
4	Production (In-Service Build)

Table 1.8 (Conformity Module Types)

8.2.2 The assessment criteria related to the risk method outlined in the process flow below (Fig 1.8) identifies the main clauses from ISO 12100 which form the basis of the conformity modules when applied:

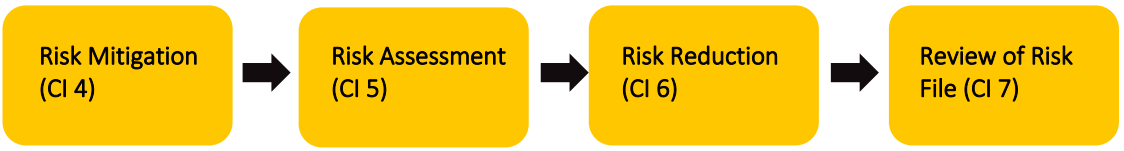


Fig. 1.8 (Evaluation of Risk Conformity Approach)

8.2.3 The design basis evaluation shall determine that the risk assessment/design FMEDA outputs of the respective full system (complete machine), sub-system assembly, or component are representative to the construction build using ISO 12100 as the general guide as confirmation that the design outputs specify:

- All risks and hazards are identified and are relative to the design intent of the construction build
- Declared design outputs Identify the hazard mitigation concepts and reference material (standards) met
- The construction design intent of operating and maximum limits
- A document register is generated listing all supplied design documents

8.2.4 Sub-modules: Determination of classification standards and block structure architecture applicable (sub-modules within each conformity module and engineering block structure and Class A + B sub modules) shall determine the horizontal standards (Class B1 and B2) to be applied, and if applicable outline the C classification standards, (example - module 4: conformity system process A, B, and C) to be applied.

8.3 Design Evaluation

8.3.1 In general, the reference horizontal and vertical standards applied to evaluate and verify conformity for functional safety (PL & SIL) and overall machine safety of the design FMEDA/risk assessment will be dependent on the engineering block structure applied in relation to the overall construction build, the tables below demonstrate the main normative standards to be used for the conformity approach and evaluation and validation methods.

Table 1.9 is an example of design evaluation conformity and validation method reference material.

Full System (Integrated Automated Machine) Intended Use – Industrial Sector	Evaluation Conformity Standard
Safety of machinery, general principles for design, risk assessment and risk reduction	ISO 12100 (Applicable Parts)
Safety of Machinery - Principles for the design and integration of safety-related parts of control systems	ISO 13489-1
Safety of Machinery - Safety-related parts of control systems, Validation. (PLr)	ISO 13489 -2
Safety of machinery - Electrical equipment of machines	IEC 60204-1
Safety of machinery - Functional safety of safety-related electrical, electronic, and programmable electronic control systems (SIL)	IEC 62061 or IEC 61508-1 / -2
Other Class B1 and B2 standards as applicable pending on construction build	Class B1 and B2 as Applicable
Other Class C Standards if integrated machine specific product standards (if applicable)	Class C as Applicable

Table 1.9 (Full System Machine conformity reference standards)

8.3.2 The conformity assessment process shall be based on the evaluation of the risk outputs of the FMEDA (ISO 12100), the method of evaluation to determine conformity shall be by design evaluation, to assure all design outputs meet the risk hazards identified, that applicable horizontal and vertical classification of standards have been applied and are met in full for:

- Full systems (complete end-to-end build)
- Sub-system assemblies
- Component level or standalone machine

8.3.3 The conformity approach, pending on machine and level of build will use ISO 12100 to identify engineering design applications incorporated in all types of machine, sub-system and component/standalone machine level.

8.4 Design Validation

8.4.1 The output results from the design evaluation (determination that all risks have been identified and mitigated by design intent), the risk assessment design FMEDA outputs/claimed integrity performance limits (PL), and safety integrity level (SIL) of the construction build shall be validated.

8.4.2 The validation of the design FMEDA/risk assessment outputs shall be conducted as an example to the specific standards listed in Table 1.10 below.

Validation Method	Standard
Design intent validation by calculation of SEP applied by FoS & MoS (Margin of Safety) validation	ISO 12100
Validation of PLr claims from Design FMEDA, by re-calculation of declared PLr, calculation to validate PLa actual as confirmation of claimed result	ISO 13489-1 and Part 2
Validation of SIL claims from Design FMEDA, by re- calculation of declared SIL, calculation to validate SIL actual as confirmation of claimed result	IEC 62061 or IEC 60158 -1/-2 / -3
Hydraulic Fluid Power – Safety of Systems and Components	ISO 4413
Pneumatic Fluid Power -- Safety of Systems and Components	ISO 4414
Software requirements for E/E/PE	IEC 60158-3

Table 1.10 (Listing – Evaluation & Validation)

8.5 Design Verification

8.5.1 Deemed critical elements of the construction build design appertaining to the overall safety and integrity related to the functional safety of the build and operation of the "product" shall be verified by physical inspection on site, either on initial build/manufacture or on commissioning run up/sign over.

8.5.2 The design evaluation and validation phase of the conformity assessment shall identify any deemed component, subassembly, or sub-system to be verified against the design intent/design evaluation to verify safety and operational performance integrity.

8.5.3 The verification shall be a physical inspection with defined parameters through measurement, site testing, or a combination of both to determine and confirm calculations or design limit parameters appertaining to the overall safety and integrity of the claimed design.

8.5.4 The design verification inspection results shall be used as the final validation of the overall calculated and documented results to ascertain final safety and functional safety levels claimed.

8.5.5 Functional safety management at this point shall be reviewed.

SOURCES OF FAILURE

Functional safety standards generally recognize two types of failures and then propose the means to address them.

Random hardware failures are the easiest to understand in that they are caused by, as the name suggests, random unexpected failures in equipment. The probability of failure due to random failures is expressed as the PFH (average frequency of dangerous failure) for the system. The allowed PFH depends on the required SIL and ranges from 10–5/h for SIL 1 to a minimum of 10–7/h for SIL 3.

Systematic failures are those inherent in a design, in the sense that they can only be fixed by a design change. Insufficient EMC robustness can be considered a systematic error, as can deficiencies in requirements, insufficient verification and validation, and all software errors. Systematic errors are effectively weaknesses that exist in every item produced rather than being present in individual units. If the right set of circumstances arise, the failure will occur with 100% probability.

To be suitable for use in a situation requiring a SIL X safety function, both the random and systematic requirements given in the standard for that SIL level must be met. Compliance to the hardware requirements alone is not sufficient.

8.6 Evaluation Plan

8.6.1 An evaluation plan (certification or test plan) shall be drawn up to identify all areas of the full system (complete machine), sub-system, or component/standalone machine to be evaluated.

8.6.2 The evaluation plan shall identify assigned reference standards/methods of validation which will ensure all areas of the intended design is adequately addressed in terms of evaluating general and functional safety.

8.7 Technical Review for Certification

8.7.1 The technical review for certification shall consist of a review of the conformity assessment process outputs and results and determination that the evaluated and validated results meet the required limits specified within Annex A to F, the results and limit values declared within the:

- Evaluation plan
- Review of the design basis for evaluation
- Design evaluation
- Design validation
- Design verification

8.8 Certification

8.8.1 The process for certification and award of the Intertek FS Mark shall be conducted in accordance with Intertek's internal procedures SMS-FS-OP-19 and Intertek Propriety Standard INT/FS/2019. On final certification review, confirming that all parts of the technical review have been satisfactorily completed and all criteria met, Intertek will award the Functional Safety Mark.

SECTION 9

FUNCTIONAL SAFETY MANAGEMENT

9.1 Functional safety management is required under IEC 61508 and IEC 61151 series standards, the functional safety management infrastructure shall be audited as part of the site visit inspection phase.

9.2 The objective is the assessment of the lifecycle model implemented, i.e. which parts within the overall lifecycle are relevant, define responsibilities, and specify management and technical activities that establish the documentation framework.

9.3 The documented functional safety management plan shall facilitate and demonstrate compliance to the standards, plan the verification, validation, and assessment activities, and provide a "live" planning document that can be maintained throughout the lifecycle.

9.4 A typical outline for a functional safety management plan should include:

- Responsibilities of the personnel involved
- The documented lifecycle
- Verification plan
- Validation plan
- Quality planning

9.5 The plan must always fit within the context of a company's wider framework of risk management. It cannot be seen in isolation. Functional safety systems implement risk reduction factors that contribute to an overall risk management strategy.

9.6 The structure of the plan may require many levels of functional safety management planning:

- An overall company-wide plan
- A plan for an individual operating facility
- A project plan for a specific project

9.7 The system vendors may have plans covering only their scope, similar to a quality process. A company that has a quality plan will usually prepare separate project execution plans for individual projects.

9.8 The document/lifecycle plan identifies which stages of the lifecycle apply for the scope of work planned, being:

- Conceptual design and requirements development
- System design and engineering
- Testing (FAT, SIT, SAT)
- Installation and commissioning
- Operations, maintenance, and ongoing modifications

9.9 Key documents to be identified as outputs from the Functional Safety management plan and structure include:

- Risk analysis (Design FMEDA)
- Safety requirements specification (SRS)
- Detailed design specifications
- Test specifications

9.10 The Safety Requirements Specification (SRS) is a collation of many elements, including:

- Control and safeguarding philosophy
- SIS architecture specification
- HAZOP reports
- SIL determination report
- Cause and effect charts
- Functional specifications
- SIF narratives
- Ranges, alarm and trip settings schedule
- Overrides

9.11 Detailed design specifications are required; the common elements in detailed design are:

- Hardware fabrication specifications and drawings
- Software architecture
- Software standards
- Detailed functional requirements
- Detailed non-functional requirements

9.12 Considerations for the quality plan include:

- Competency of management
- Procedures – internal operating procedures
- Techniques and measures
- Supplier quality
- Sub-contractors and third-party contractors
- Change management – design change
- Tracking and traceability
- Configuration management
- Issues management (complaints)
- Incidents and performance analysis
- FS audits and assessments

9.13 Key elements of a functional safety management plan are detailed in Figure 1.12:

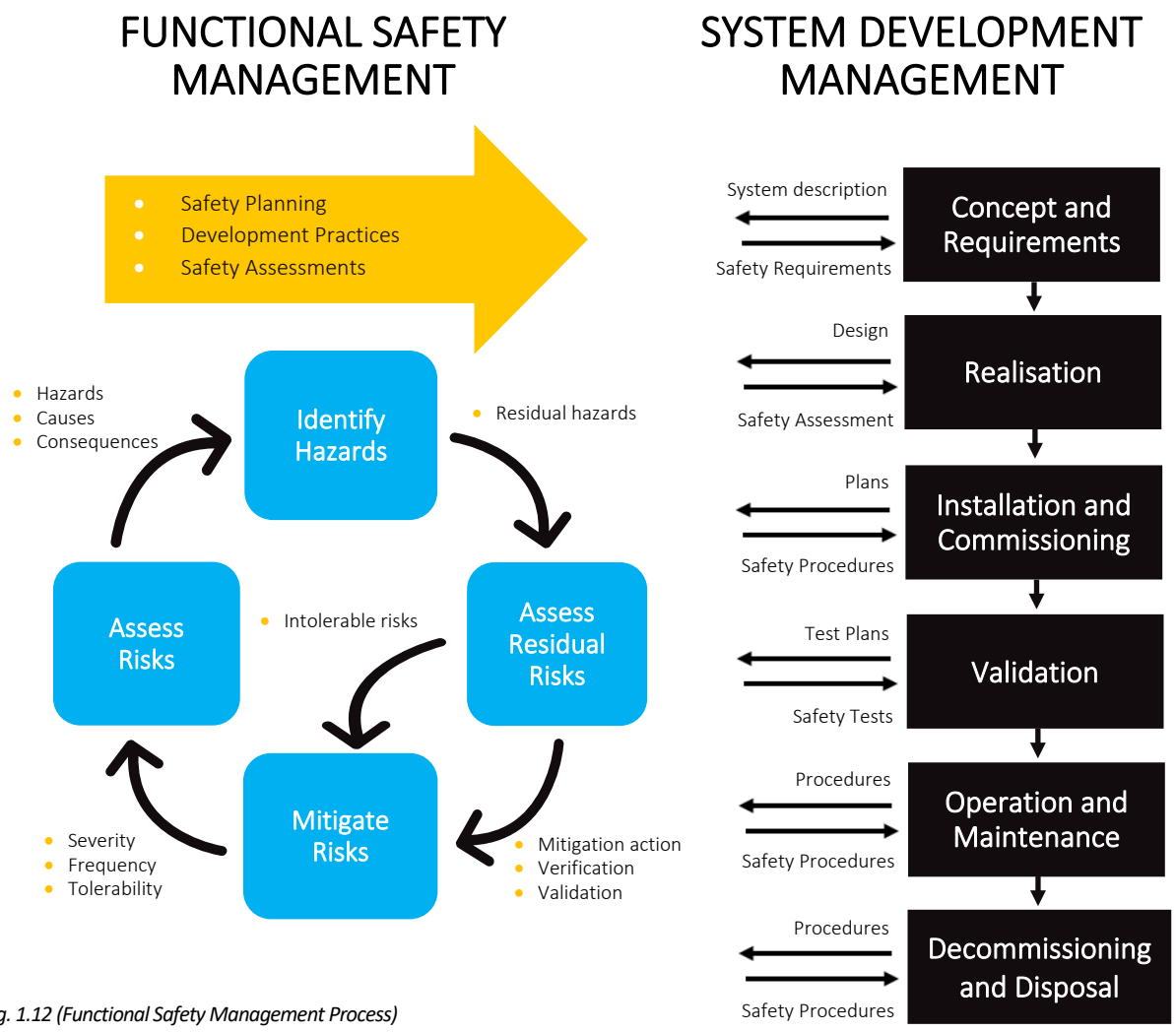


Fig. 1.12 (Functional Safety Management Process)

SECTION 10

COMMON ABBREVIATIONS

Abbreviation	Meaning/Description
SIL	**Safety Integrity Level** One of four levels to specify the item's or element's necessary requirements.
CCF	**Common Cause Failures** Failure of two or more elements of an item resulting from a single specific event or root cause. Common cause failures are dependent failures (DF) that are not cascading failures (CF).
CF	**Cascading Failure** Failure of an element of an item causing another element or elements of the same item to fail. Cascading failures are dependent failures (DF) that are not common cause failures (CCF).
CMF	**Common Mode Failure** A type of common cause failure (CCF) where multiple items fail in the same mode. Analyse using fault tree analysis (FTA).
DC	**Diagnostic Coverage** Proportion of the hardware element failure rate that is detected or controlled by the implemented safety mechanisms.
DCLS	**Dual Core Lockstep** Processing system that runs the same set of operations at the same time in parallel.
DF	**Dependent Failure** Failures whose probability of simultaneous or successive occurrence cannot be expressed as the simple product of the unconditional probabilities of each of them. Dependent failures include common cause failures and cascading failures.
DFA	**Dependent Failure Analysis** Aims to identify the single events or single causes that could bypass or invalidate a required independence or freedom from interference between given elements and violate a safety requirement or a safety goal.
DIA	**Development Interface Agreement** Agreement between customer and supplier in which the responsibilities for activities, evidence, or work products to be exchanged by each party are specified.
DTI	**Diagnostic Test Interval** Amount of time between the executions of online diagnostic tests by a safety mechanism.
E/E/PE	**Electrical, Electronics, and Programmable Electronic** IEC 61508-4 defines this as based on electrical and/or electronic and/or programmable electronic technology.
EMI	**Electromagnetic Interference: Disturbance** Effect on an electrical circuit due to either electromagnetic induction or electromagnetic radiation emitted from an external source.
EOS	**Electrical Overstress**

	Electrical overstress failures can be classified as thermally-induced, electromigration-related, and electric field-related failures. Can result in a latch-up short circuit.
ESD	**Electrostatic Discharge** A subclass of Electrical Overstress (EOS). The sudden flow of electricity between two electrically charged objects caused by contact, an electrical short, or dielectric breakdown.
FIT	**Failure in Time** The number of failures that can be expected in one billion (1x10^9) device-hours of operation. *Mean time between failures (MTBF) = 1,000,000,000 x 1/FIT*
FMEA	**Failure Mode and Effects Analysis** As opposed to fault tree analysis (FTA), failure mode and effects analysis (FMEA) is an inductive approach focusing on the individual parts of the system, how they can fail, and the impact of these failures on the system. Analysis starts at faults, which can lead to errors and then failures.
FMEDA	**Failure Mode Effects and Diagnostic Analysis** A procedure for the detailed determination of error causes and their impact on the system and can be very efficiently used in the early stages of systems development for the purpose of early identification of weaknesses.
FTA	**Fault Tree Analysis** As opposed to failure mode and effects analysis (FMEA), fault tree analysis (FTA) is a deductive (top down) approach starting with the undesired system behaviour and determining the possible causes of this behaviour.
FTTI	**Fault Tolerant Time Interval** The time between when a fault occurs and the system can transition to a safe state and be ready to experience another possible hazard. *Maximum FTTI = DTI + Fault Reaction Time + Safe State*
HSI	**Hardware-Software Interface** Hardware / Software compatibility of diagnostic analysis of input output signal.
LFM	**Latent Fault Metric** Latent faults are multiple-point faults (whose presence are not detected by a safety mechanism nor perceived by the driver within the multiple-point fault detection interval (MPFDI). The latent fault metric (LFM) is a hardware architectural metric that reveals whether or not the coverage by the safety mechanisms, to prevent risk from latent faults in the hardware architecture, is sufficient.
MBU	**Multiple Bit Upset** When two or more error bits occur in the same word. Cannot be corrected by simple single-bit.
MPFDI	**Multiple Point Fault Detection Interval** The time span to detect a multiple-point fault before it can contribute to a multiple-point failure.
PMHF	**Probabilistic Metric for (Random) Hardware Failures** The sum of the single point, residual, and multipoint fault metrics. Is expressed in FITs.
SEL	**Single Event Latch-up** A type of single event effect (SEE) caused by a single event upset (SEU) that causes a transient fault. This transient fault is "hard" and can only be corrected by cycling the power.
TD	**Tool Error Detection** The confidence in measures that prevent the software tool from malfunctioning and producing corresponding erroneous output, or in measures that detect that the software tool has malfunctioned and has produced corresponding erroneous output.

SECTION 11

CUSTOMER SUPPLIED TECHNICAL DOCUMENTS & SPECIFICATIONS

The tables in Section 11 demonstrate the design and technical documents to be supplied in support of Equipment Under Consideration (EUC) risk assessment mitigation outputs when meeting ISO 12100 outputs and Design FMEDA for complete machines, (Full Systems) sub-systems and components/standalone machines.

Note: Not all document references outlined in the tables below may apply, but shall be supplied if applicable to the EUC.

EUC Technical Documents and Specifications (if applicable) for ISO 12100 risk evaluation
Mechanical design calculations and specifications for the EUC in relation to static / dynamic loads (Stress / Strain load tables) materials, vibration, emissions, hazardous substances, radiation and impact to the environment.
Design specifications and schematic diagrams for Hydraulic and Pneumatic systems, integrated or standalone industrial Robotics, indexing systems, welded / fabricated assemblies, cutting systems (abrasive, thermal, acoustic or hydraulic).
Design specification related to Structure stability, foundation type and load stressing, environmental external forces.
Design specifications and calculations for structural – EUC Design specifications for CoG, loads, SWL / MWL / YWL calculations, lifting points.
Specifications related to any chemical hazards used by or omitted from EUC.
Controls (ISO 13489-1 and 13489-2) Design specifications and calculations for EUC active or passive SRCS with related MTTFd values.
Electrical Safety: EUC Design specifications for meeting IEC 60204, composing of electrical systems layout, schematics electrical wiring stress loading calculations / tables, identified critical components and safety approvals (if any). Component PLa and SIL coding (if any), Electrical Insulation classifications.
EUC Technical specifications (if applicable) for Grid Code connection, accessibility / creepage and clearance considerations.
Design and calculation (SIL) related to the EUC, Controls IEC 61508 -1 and -2 (E/E/PE) systems, design specifications for component MTTDd, SIL (If any) SILr calculations.
EUC Electronics: Design specifications and schematics for Analogue / digital electronic systems and components covering static / pulse loads, deviation, clock sequencing and PCB population levels. Active controls safety chain / loop.
EUC Software – IEC 61508 -3, design specifications and linear or flow layout for safety related functions, such as safe state, fault indication, error handling, sensor fault detection, fault analysis monitoring, online self - diagnosis, software revisions / uploads, function interfacing, software communications revisions – safe status, (IEC 60158-2).

EUC Technical Documents and Specifications (if applicable) for ISO 12100 risk evaluation - CONTINUED
EUC Software systems speciation capability, covering Independence Levels, 165 Safety Data Compatibility, Data interface (External Systems) Inconsistent Data, Corrupt data, Unauthorised Access – Data, and Unauthorised Access -Personnel. Include hardware (IEC 61508-3) All modes of operation & functions including set up / calibration. Architecture of the system. Logic Platform (if PLC?), Logic flow? Confidence Scale Level (SF) 1-4 Determination to meet IEC 61508 – 4, Hardware integration and systematic capability, Capacity / Response time, Equipment / Operator Interface and Self Diagnostic capability.
Ergonomics, Specifications related to Local Environment (Light, Access, Visual Displays), Control Access / Display.
Design specifications / instructions for Machine Set Up, 202 Pre - Machine Set Up, Calibration, Safety Measures – Check, Operation, Operating Modes, Raw Material Handling, Operating Controls, Operating Parameters, Operating Manual, Management Controls and Final Product Verification.
Technical Documents related to Commissioning, Machine Assembly, Adjustments, Connection Systems, Power Supply Connections, Demonstration (Trial Run Up), Preparation - Pre -Maintenance, Fixings (Anchors), Foundation Preparation, Run up - No Load. Run Up - Max Load.
Maintenance Manuals covering general Housekeeping - Cleaning / Lubrication / Fluid Levels) Disassembly / Re-assembly, Tool Replacement, Re-setting / Adjustments, Repairs / Modifications, Fault Finding and Fault Modes Process.
Instructions covering Transportation Loading, Packaging, Transportation, Unloading, Unpacking, Dismantling / Disabling and Disposal Plan.

Clause	EUC Technical Documents and Specifications for ISO 13489 -1
4.4	Design layout and structure of SRP/CS (component level (All Related Mechanical / Electrical / Electronic parts)
4.5.1	Technical specifications related to all SRP/CS referencing claims for PL, MTTFd, DC, CCF, Structure Claim
	FMEA
	Software ID code, systematic failure, environmental conditions claim, PL qualifying method, Architecture constraints.
4.5.2	PL Calculation Methods – From either Manufacturers Data, Tables from Annex C & D, Lifecycle Capability (# years)
4.5.5	Category calculation / PL claim less MTTFd calculation
4.7	Calculation method for Verification for PL achieved PLr and PL(sub SRP/CS) >= PLr
6.2.2	SRP/CS Architecture Block Structure documents
6.3	Method and demonstration of combined PL CAT for SRP/CS

Clause	EUC Technical Documents and Specifications for ISO 13489 - 2
4.2	EUC overall validation plan
4.3	EUC generic System fault list and defined limits
4.4	EUC specific fault list, with mitigation of each fault
4.5	EUC system validation (Software, PL calculation for the entire system)
5	EUC system validation method – comprising of technique for validation adopted
6	Plan for EUC end - product testing / validation
7 & 8	Technical document related to the EUC safety functions – specification for safety function requirements. Validation plan for testing and analysis of safety functions.
9	EUC adopted validation method of category specifications, validation of MTTFd, Dcavg and CCF, validation of measures against systematic failures related to performance level and category of SRP/CS. Validation of safety-related software, validation and verification of performance level. Validation of combined safety-related parts.
10, 11, 12	EUC validation plan for environmental analysis, maintenance, end user operator instructions

Documents to be submitted for IEC 62061

Information required	Subclause
Functional safety plan	4.2.1
Specification of requirements for SRCFs	5.2
Functional safety requirements specification for SRCFs	5.2.3
Safety integrity requirements specification for SRCFs	5.2.4
SRECS design	6.2.5
Structured design process	6.6.1.2
SRECS design documentation	6.6.1.8
Structure of function blocks	6.6.2.1.1
SRECS architecture	6.6.2.1.5
Subsystem safety requirements specification	6.6.2.1.7
Subsystem realisation	6.7.2.2
Subsystem architecture (elements & their interrelationships)	6.7.4.3.1.2
Fault exclusions claimed when estimating fault tolerance/SFF	6.7.6.1c)/6.7.7.3
Subsystem assembly	6.7.10
Software safety requirements specification	6.10.1
Software based parameterization	6.11.2.4
Software configuration management items	6.11.3.2.2
Suitability of software development tools	6.11.3.4.1
Documentation of the application program	6.11.3.4.5
Results of application software module testing	6.11.3.7.4
Results of application software integration testing	6.11.3.8.2
Documentation of SRECS integration testing	6.12.1.3
Documentation of SRECS installation	6.13.2.2
Documentation for installation, use and maintenance	7.2
Documentation of SRECS validation testing	8.2.4
Documentation for SRECS configuration management	9.3.1

Clause	EUC Technical Documents and Specifications for IEC 61508-1
7.3.2	Information concerning the EUC, intended operational environment and identified hazards.
7.4.2 7.5.2	Information defining scope of the hazard and risk analysis representative of the EUC.
7.6.2 7.7.2	Specification of the overall safety requirements in terms of the safety functions requirements and safety integrity requirements. Information on the allocation of the overall safety functions, Detailing target failure measures, and associated safety integrity levels Assumptions made concerning other risk reduction measures that need to be managed throughout the life of the EUC.
7.8.2 to 7.15.2	Information and results of the overall safety requirements allocation. A plan for the installation of the E/E/PE safety-related systems; Specification of the E/E/PE system safety requirements. A plan for the installation of the E/E/PE safety-related systems; Plan for the commissioning of the E/E/PE safety-related systems. Fully installed E/E/PE safety elated systems; Overall safety validation plan for the E/E/PE safety-related systems; Information and results of the overall safety requirements allocation including installation and maintenance.

Clause	EUC Technical Documents and Specifications for IEC 61508-2
7.2.2	E/E/PE system design requirements and specification, describing the equipment and architectures for the E/E/PE system
7.3.2	Plan for the safety validation of the E/E/PE safety related systems
7.4.2 to 7.4.11	Design of the E/E/PE safety related systems in conformance with the E/E/PE system design requirements specification Plan for the E/E/PE system integration test PE system architectural information as an input to the software requirements specification
7.5.2	Fully functioning E/E/PE safety-related systems in conformance with the E/E/PE system design Results of E/E/PE system integration tests
7.6.2	E/E/PE system installation, commissioning, operation and maintenance procedures for each individual E/E/PE system
7.7.2	Fully safety validated E/E/PE safety-related systems Results of E/E/PE system safety validation
7.8.2	Results of E/E/PE system modification
7.9.2	As above – depends on the phase Results of the verification of the E/E/PE safety-related systems for each phase
8	Results of E/E/PE system functional safety assessment
7.2.2	E/E/PE safety requirements specification as developed during allocation (see IEC 61508-1) E/E/PE system safety requirements specification (from IEC 61508-2)

Clause	EUC Technical Documents and Specifications for IEC 61508-2 - CONTINUED
7.3.2	EUC software safety requirements specification
7.4.3	EUC software safety requirements specification; E/E/PE system hardware architecture design (from IEC 61508-2)
7.4.4	EUC software safety requirements specification; software architecture design
7.4.5	EUC software architecture design; support tools and coding standards
7.4.5	EUC software system design specification; support tools and coding standards
7.4.6	EUC software module design specification; support tools and coding standards
7.4.7	EUC software module test specification; source code listing; code review report
7.4.8	EUC software system integration test specification software
7.5.2	EUC software architecture integration test specification; software/PE integration test specification (also required by IEC 61508- 2). Integrated programmable electronics.
7.6.2	EUC Design and Verification plan and specification for the above
7.7.2	EUC validation plan for software aspects of system safety
7.8.2	EUC software modification procedures; software modification updates on request
7.9.2	EUC appropriate verification plan (dependent on phase)
8	EUC software functional safety assessment plan

Intertek is a leading Total Quality Assurance provider to industries worldwide. Our network of more than 1,000 laboratories and offices and over 46,000 people in more than 100 countries, delivers innovative and bespoke Assurance, Testing, Inspection and Certification solutions for our customers' operations and supply chains. Intertek Total Quality Assurance expertise, delivered consistently with precision, pace and passion, enabling our customers to power ahead safely.

FOR MORE INFORMATION

Americas
+1 800 WORLDLAB (967 5352)
+1 251 459 6173

Europe
+46 8 750 0000

Asia
+852 2173 8888

Info-sweden@intertek.com

intertek.se/provning/functional-safety/

intertek
Total Quality. Assured.