Gladstone Ports Corporation

Growth, prosperity, community.

Engineering Site Standard

GPC-ESS-510

Functional Safety Standard - Functional Safety Management Plan

Brief description

This Engineering Site Standard outlines the requirements for functional safety systems at Gladstone Ports Corporation sites.

Document information	
Current version	2
First released	15/01/21
Last updated	15/01/21
Review frequency	Every 2 years or as required
Review before	15/01/23
Audience	All GPC personnel and contractors

Document accountability	
Role	**Position**
Owner	Technical Services Manager
Custodian	Specialist Electrical & Instrumentation Engineer

Endorsed by	Electrical Engineering Superintendent on 15/01/21

If you require any further information, please contact the Custodian.

Contents

Document Version Control

Version	Date	Author	Change Description
1	17/04/2018	D Smith	Original
2	15/01/2021	J Pajonk	Issued for use

1. Introduction

1.1. Background

Circa 2015 the Gladstone Port Corporations RG Tanna Coal Terminal upgraded their Shiploader 2 & 3 functional safety systems. As a part of those projects a Functional Safety Management Plan document was developed for the shiploaders. There is now a requirement for a Functional Safety Standard document to be created for the RGTCT site as a whole. As such, the Shiploaders Functional Safety Management Plan version 1 document has been renamed and updated to become the site standard document "ESS-510 – Functional Safety Standard – Functional Safety Management Plan".

At the time of the upgrade of the shiploaders there were a number of standards providing alternative techniques to address safety of machinery. The standards widely recognised in Australia include AS4024, AS61508 (AS62061) and ISO13849. These standards provide three different methods / techniques to measure the safety and integrity of controls and protection systems for machinery. The techniques include; Category using AS4024, Safety Integrity Level using AS62061 and Performance Level using ISO13849. These techniques offer certain benefits over each other whilst also having their own design limitations and associated cost implications throughout the various engineering and maintenance life cycle phases of the equipment / system.

Aurecon was engaged by GPC to develop an overarching functional safety management plan for the Shiploader 2 upgrade projects. That document was then expanded to cover Process Control Upgrade (PCU) projects on all the shiploaders.

Aurecon developed the document based on the current Australian legislative requirements and GPC's preference to apply ISO13849 to meet the machine safety requirements. Refer to section 1.5 for details.

1.2. Definitions and Terminologies

This document refers to more than one standard for achieving safety in machinery where these standards use different terminologies.

To avoid confusion and for standardisation purposes, this document will use a generalised terminology of "safety function" to refer an individual safety related control function and "safety system" to refer safety related control system. Refer to Appendix A for a list of definitions and terminologies used for safety related control systems.

1.3. Glossary of Terms

Term	Description
AS	Australian standard
CFSE	Certified functional safety expert (per www.cfse.org)
CFSP	Certified functional safety professional
DI	Delivery independence
FAT	Factory acceptance testing
FSM	Functional safety manager
FSMP	Functional safety management plan
GI	Geographical independence

Term	Description
GPC	Gladstone Ports Corporation
HAZOP	Hazard and operability study
IPL	Independent protection layer
ISO	International standards organisation
OI	Organisational independence
P&ID	Process and instrumentation diagram
PCU	Process control upgrade
PFD	Probability of failure on demand
PFH	Probability of failure per hour
PI	Probable injury
PL	Performance level
PLC	Programmable logic controller
PLL	Probable loss of life
QLD	Queensland
RGTCT	RG Tanna Coal Terminal
RPEQ	Registered Professional Engineer QLD
RRF	Risk reduction factor
SE	Safety engineer
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SL	Shiploader
SLC	Safety life cycle
SRCFs	Safety related control functions
SRECS	Safety related electrical control system
SRS	Safety requirement specification
TUV FSE	TUV certified functional safety engineer (per www.tuvasi.com)
WHS	Workplace health and safety

1.4. Purpose and Scope

This document has been developed for the definition, realisation, operation and maintenance phases of safety functions / systems and;

- Provides a structured criteria and ongoing methodology for projects with Functional Safety Systems, which include the;
- Identification of hazards and associated risks, where safety functions are implemented.

- Assessment for the associated level of risk for safety functions and subsequently to classify them either under the PL requirements of ISO13849 standard or under the SIL level requirements of AS62061.
- Definition of general guidelines for the management of machine safety in accordance with either ISO13849 or AS62061.

It is to be noted that this is a live document and must be updated as required throughout the entire lifecycle of GPC projects and the ongoing operation of the equipment. It should be noted that there are many limitations and practicalities that must be considered when implementing the new safety systems in accordance with the new standards. The standards are to be met as much as practicable and deviations from the standards are to be justified, documented and approved by the designated GPC site RPEQ and TUV FSE certified Functional Safety Systems engineer.

1.5. Applicable Codes and Standards for Machine Safety

The application of machine safety for GPC projects can be achieved by use of the following codes and standards.

Legislation

- QLD Workplace Health and Safety act 2011
- QLD Plant Code of Practice 2005

Overarching safety standards

- ISO12100–2010 Safety of machinery – General principles for design – Risk assessment and risk reduction
- AS61508–2011 Functional safety – Electrical / electronic / programmable electronic safety related systems

Machine safety application standards

- ISO13849–1– 2006 Safety of machinery – Safety related parts of control systems Part1: General principles for design
- ISO13849–2–2012 Safety of machinery – Safety related parts of control systems Part 2: Validation
- AS62061–2006 Safety of machinery – Functional safety of safety – related electrical, electronic and programmable electronic control systems
- AS4024–2014 Safety of machinery

Note: This FSMP has been developed based on the current available version of the above mentioned standards. All the required works as mentioned in this FSMP will be carried out in accordance with the latest available version of these standards at the time of their application.

1.6. Legislative Requirements

The requirements for machine safety are governed by the applicable acts and regulations, in particular Queensland Workplace Health and Safety. This legislation provides information regarding the requirements for safety. Codes of practice are provided for specific hazards which would achieve compliance with the WHS requirements in legislation. Codes of practice refer to the Australian standards which provide guidance that may assist in achieving compliance with the relevant legislation. The current relationship between the applicable QLD WHS Act, Plant Code of Practice and applicable standards can be seen in the legislative flowchart provided in Appendix B.

The flowchart shows that the plant code of practice identifies AS4024 and AS61508 for machine safety (refer to “QLD plant code of practice 2005, Appendix 4, Categories of reliability and safety integrity levels” for details). AS62061 is an application standard of AS61508 for machine safety applications.

ISO13849 is recognised within ISO12100 which is referred to as an appropriate standard for risk management for plant within the QLD Plant Code of Practice 2005.

1.7. Competency and Independence Requirements

Functional safety life cycle process requires competency and level of independence to be maintained within the team engaged in engineering design, approval, testing and operation of safety systems. The AS61508 which is a parent standard of AS62061 outlines the competency and level of independence requirements for the team. These requirements have been aligned with the current GPC organisation chart and are provided in Table 1 on the following page. Table 2 provides definition of the level of independence to be maintained within the team during different phases of safety life cycle (eg. design, verification and approval etc.).

1.7.1. Definition of Roles and Competencies

The Table 1 below provide definitions of roles and required competencies. Individual roles for each of the activities described in the following sections has not been detailed here and will be assessed and assigned by the project manager based on the guidelines provided in the following table and in the associated notes.

Position title	Responsibilities	Competencies
Cargo Handling General Manager	Overall accountable for the safety of the machinery.	Appreciation of safety life cycle processes of the mentioned standards.
Project Manager	Responsible for achieving the requirements of functional safety by managing the required activities in accordance with this plan on behalf of the Asset Owner.	Detailed understanding of the safety life cycle processes of the standards mentioned in section 1.5**Error! Reference source not found.**. Project management
Electrical/Control Systems Engineer	Responsible for functional safety system design, verification, validation, implementation and documentation.	Certified Functional Safety Professional (ie. TUV Functional Safety Engineer). RPEQ
External Consultant	Technical assistance in all aspects of the risk assessment, design, verification and validation phases as required.	Certified Functional Safety Professional (ie. TUV Functional Safety Engineer). RPEQ
Maintenance Superintendent	Implementation of testing and maintenance requirements throughout the lifetime of the shiploader.	Appreciation of safety life cycle processes of the mentioned standards and minimum of 3 years relevant experience with maintenance of the facilities.

Table 1 Definition of roles and competencies

Notes:

As a minimum, the following items should be addressed when considering the competence of persons, departments, organizations or other units involved in safety life-cycle activities:

a) Engineering knowledge, training and experience appropriate to the process application

b) Engineering knowledge, training and experience appropriate to the applicable technology used (for example, electrical, electronic or programmable electronic)

c) Engineering knowledge, training and experience appropriate to the sensors and final elements
d) Safety engineering knowledge (for example, process safety analysis)
e) Knowledge of the legal and safety regulatory requirements
f) Adequate management and leadership skills appropriate to their role in safety life-cycle activities
g) Understanding of the potential consequence of an event
h) The safety integrity level of the safety instrumented functions
i) The novelty and complexity of the application and the technology

1.7.2. Definition of Level of Independence

Level of independence	Definition
Delivery Independence	A person who does not have involvement in the production of the design / deliverable under review, however may be a member of the same organisation, department or team. Team supervisor may be considered as having Delivery Independence.
Geographic Independence	A person who is independent of the design / deliverable and is not located within the team who produced the design / deliverable under review, however may be a member of the same organisation or department. A person located in the same office as the design team, but as a member of a separate workgroup may be considered as having Geographic Independence.
Organisational Independence	A person who is independent of location to the team that produced the design / deliverable under review and who is employed by a separate organisation.

Table 2 Definition of independence

1.8. Reference documents

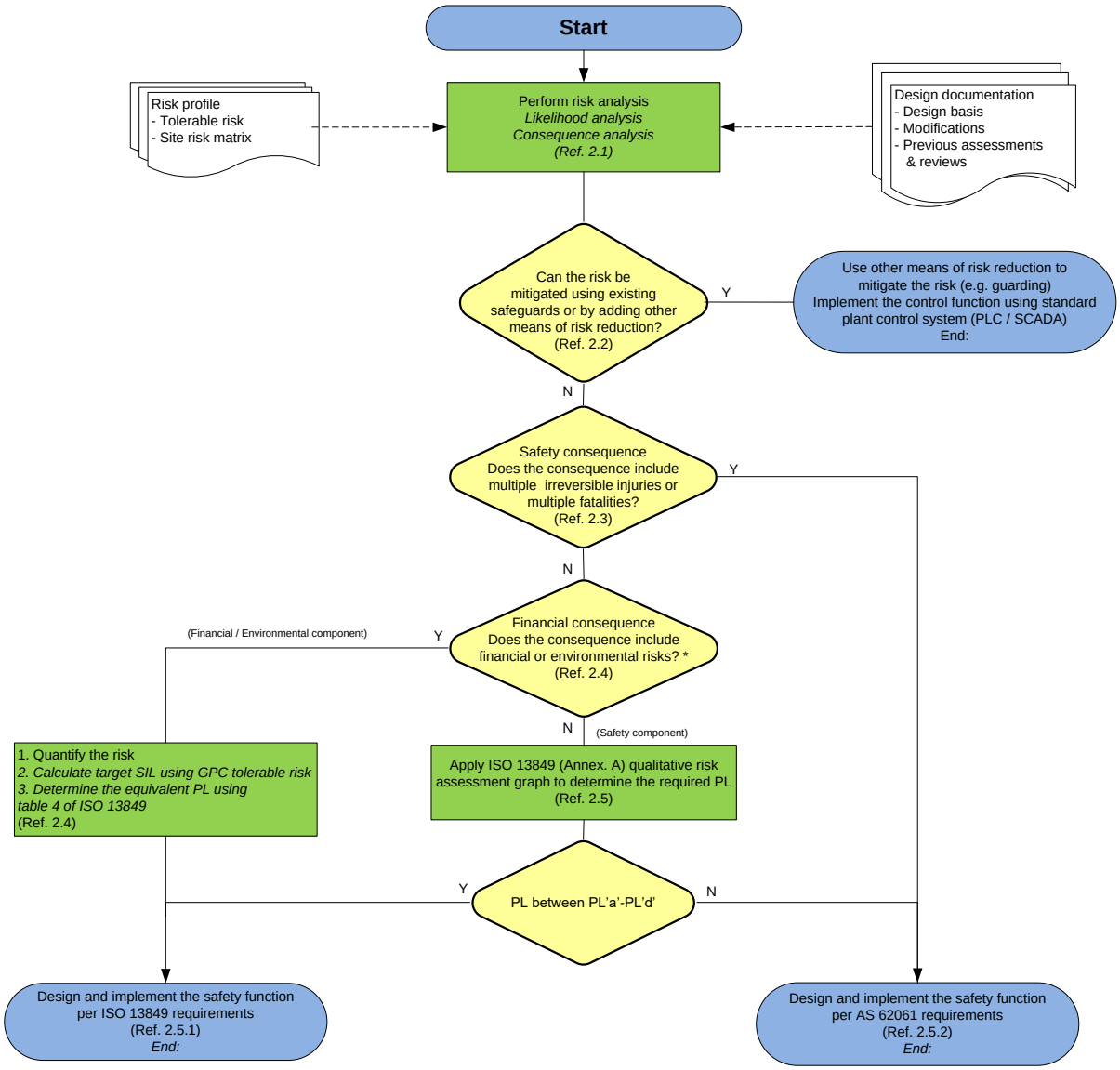
The following GPC documents were referenced while developing this document.

Reference	Title
DOCSCQPA # 829152 Rev. date 17-Oct-13	GPC Risk Management Standard

Table 3 Reference documents

2. Methodology

The overall methodology for assessment, design and implementation of a machine safety system is described in the following sections in accordance with Figure 1 below.



Notes:
* Splitting of safety and financial / environmental components of risk

Figure 1 Decision flowchart for selection of applicable standard

2.1. Hazard and Risk Assessment

A hazard and risk assessment study is the first step in identifying whether a control function is to be assessed as a safety function. In this phase, all hazardous events associated with the process and processing equipment are analysed. The associated risk is determined to see if additional measures of control are required to further mitigate the risk. Refer to section 3.2 for details of risk assessment activity.

2.2. Risk Mitigation Using Other Means of Risk Reduction

Risk mitigation through other means of risk reduction such as mechanical guarding will be considered prior to the implementation of an instrumented safety function. A safety function will only be considered for design and implementation if further risk reduction through other means is not reasonably practicable.

2.3. Safety Consequence

The qualitative risk graph of ISO 13849–1 (table 4) for the determination of performance level does not consider multiple irreversible injuries or multiple fatalities. Where the identified consequences are multiple irreversible injuries or multiple fatalities, AS62061 will be applied. Where the consequences are limited to a single irreversible injury or fatality, ISO13849 will be applied.

2.4. Financial and Environmental Consequence

ISO13849 does not provide a direct methodology for consideration of financial and environmental consequences. Both financial and environmental risks will be quantified according to GPC's tolerable risk criteria and the environmental consequences will be converted to financial consequences, refer to Appendix F for tolerable risk criteria.

The target performance requirements (PFH / SIL) for the safety functions will be calculated using the overall estimated risk and GPC's tolerable risk criteria. The tolerable value for the financial risk (or equivalent environmental risk) is provided in section 2.1.3 of Appendix F. Refer to the example in the appendix for calculation of target performance requirements (SIL / PFH) using the overall estimated risk and the tolerable risk value.

Once the target PFH/SIL requirements are calculated, the equivalent PL will be determined using table 4 of ISO13849–1 which provides a qualified relationship between the target SIL and the required PL values.

It is to be noted that the above method of determining PL using table 4 of ISO13849 will only be used for financial and environmental consequences. This table will not be applied for safety consequences.

2.5. Determination of the Required Performance Level

The outcomes of the hazard and risk assessment will be used with the qualitative risk assessment graph (ref. Figure 3) for determination of the required performance level.

The evaluated PL will determine which standard (ISO13849 or AS62061) the safety function will follow for implementation. Refer to below sections (2.5.1 & 2.5.2) for further details.

2.5.1. Safety Functions with PL Between PL 'a' and PL 'd'

If the determined performance level for the identified safety function is between PL'a' and PL'd', the safety function will be implemented using ISO13849. No further detailed analysis will be required, refer to section 3 for application of the standard.

2.5.2. Safety Functions with PL = PL 'e'

PL'e' is the highest performance requirement from ISO13849 and corresponds to a SIL 3 of AS62061 standard.

For all PL'e' safety functions, quantitative analysis will be performed and the safety function will be implemented using AS62061. Refer to section 4 for application of the standard.

2.6. Use of Mixed Techniques / Standards

The ISO13849 standard provides performance requirements to measure the ability of a safety function to perform its intended operation. The standard also maintains the category (CAT) requirements (of AS4024) as a measure of resistance of the safety function against fault situations.

AS62061 provides performance requirements for its compliance and allows flexibility in terms of the architecture. The prescriptive requirements for CAT compliance typically include the duplication or redundancy of components and fault detection which can be accounted within the framework of AS62061.

AS62061 additionally requires the implementation of a safety life cycle framework that has more stringent requirements than those required by ISO13849 during the design and operational phases of safety functions.

The safety functions which are assessed for implementation under ISO13849 can therefore be implemented in a SIL capable PLC (containing SIL rated safety software blocks). Table 4 of ISO13849 provides a correlation between PL and SIL requirements.

3. Safety of Machinery Using ISO 13849 PL Requirements

3.1. General

The ISO13849 standard will be applied to design and implement a safety function for the SL upgrade projects where safety consequences are limited to a single irreversible injury or single fatality or for all environmental and financial consequences.

The ISO13849 standard provides a structured approach for the identification, design, verification and validation of safety functions / systems.

It is anticipated that the designer will refer to the standard in full context as required. Figure 2 on the following page provides an overview of the iterative design process for a PL compliant safety system. The Figure 2 has been labelled 1 to 8 for referencing the following sections.

3.2. Identification of Safety Functions

3.2.1. Overview & Objectives

In this phase of the design process, safety functions will be identified and their resulting assessment will be documented. Refer to label 1 of Figure 2 for the context and timing of this phase.

3.2.2. Main Activities

Safety functions for the project will be identified through a hazard and risk assessment process. The hazard and risk assessment will be performed according to the guidelines provided in the following documents;

- Risk assessment guidelines per ISO12100 section 5
- GPC risk management procedure (Doc #829152)

GPC's is currently using Cintellate tool for managing site-wide hazards, however the outcomes of the risk assessment for projects will be managed separately by the project. Refer to Appendix D for a systematic approach of a risk assessment in accordance with ISO12100.

3.2.3. Deliverables

- A detailed report identifying safety functions will be produced

ISO 13849 Iterative process for design of safety functions

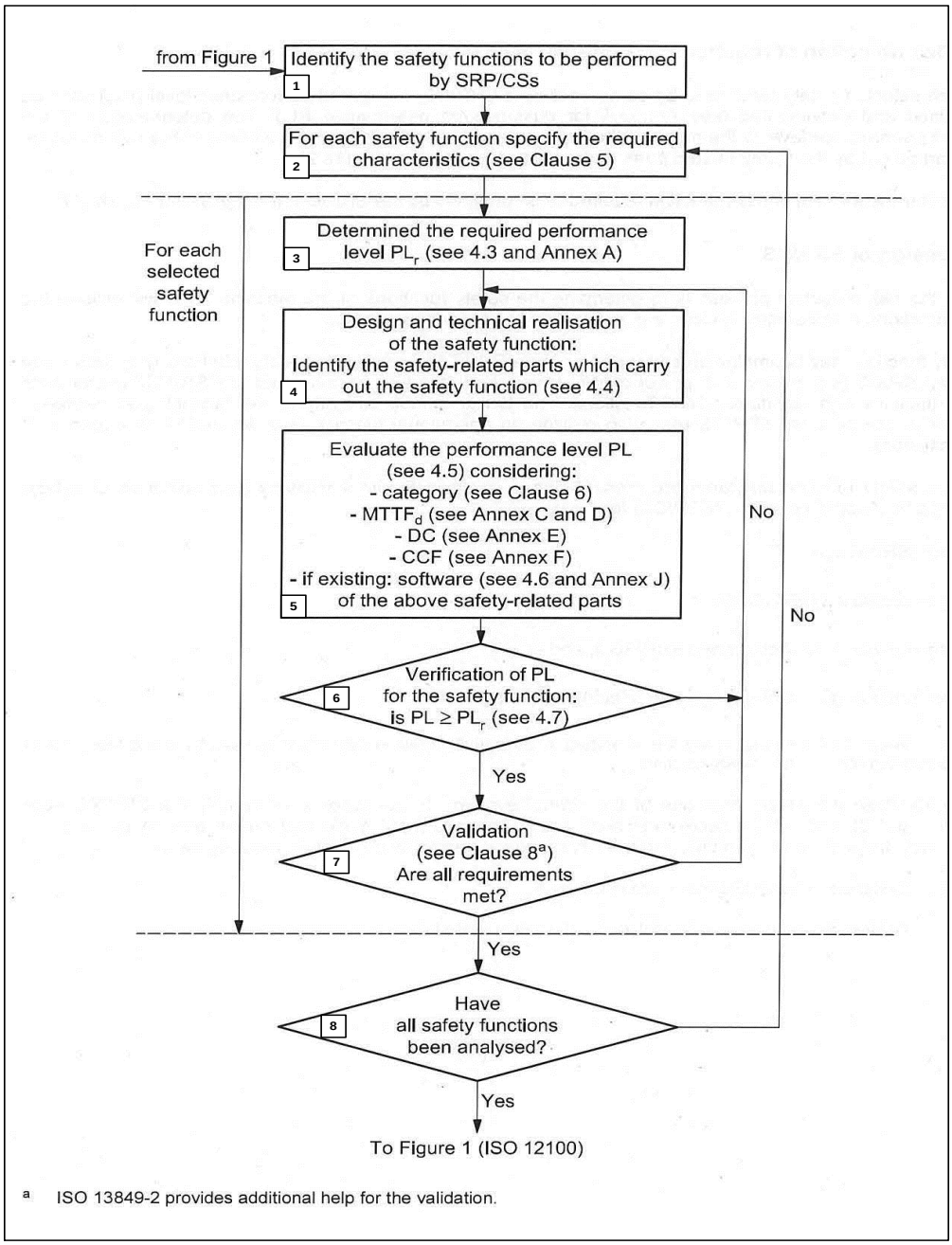


Figure 2 Iterative process for design of safety functions (ref. Figure 3 of ISO13849–1)

3.3. Specifications of Safety Functions

3.3.1. Overview & Objectives

In this phase of the design process, safety functions will be specified and documented. Refer to label 2 of Figure 2 for the context of this phase within the iterative design process.

3.3.2. Main Activities

During the specification phase, a detailed review of the machine safety functions will be completed and include details of the following:

- Risk assessment study
- Machine operating characteristics
- Emergency operation and
- Interaction of different working processes

Refer to section 5.2 of ISO13849–1 for further details.

3.3.3. Deliverables

- Safety requirement specification document containing a list of safety functions, review methodology and detailed safety function / system requirements.

3.4. Determination of the Required Performance Level

3.4.1. Overview & Objectives

In this phase of the design process, the required performance level will be assigned to each safety function. Refer to label 3 of Figure 2 for the context of this phase within the iterative design process.

3.4.2. Main Activities

The determination of the required performance level will be the result of the risk assessment.

ISO13849 risk graph (Figure 3) will be used for determination of the required PL. Calibration of the required parameters will be done according to Table 4 below.

Parameter	Value	Comment
Severity (S)	S1	Slight (normally reversible) injury – i.e. slip, trips and falls.
	S2	Serious (normally irreversible) injury – i.e. fatality.
Frequency and / or duration of exposure to hazard (F)	F1	Seldom to less often and / or exposure time is short
	F2	Frequent to continuous and / or exposure time is long
Possibility of avoiding hazard of limiting harm (P)	P1	Possible under specific conditions. Hazard can be recognised and allows adequate time for personnel to move away from the exposure area.
	P2	Scarcely possible Warning of hazard is insufficient to allow personnel to take action to move away from the exposure area.

Table 4 Calibration of parameters for PL selection

Selection of the required performance level will be performed according to the below risk graph. Refer to Annex A of ISO 13849 for detailed guidance on determination of PL.

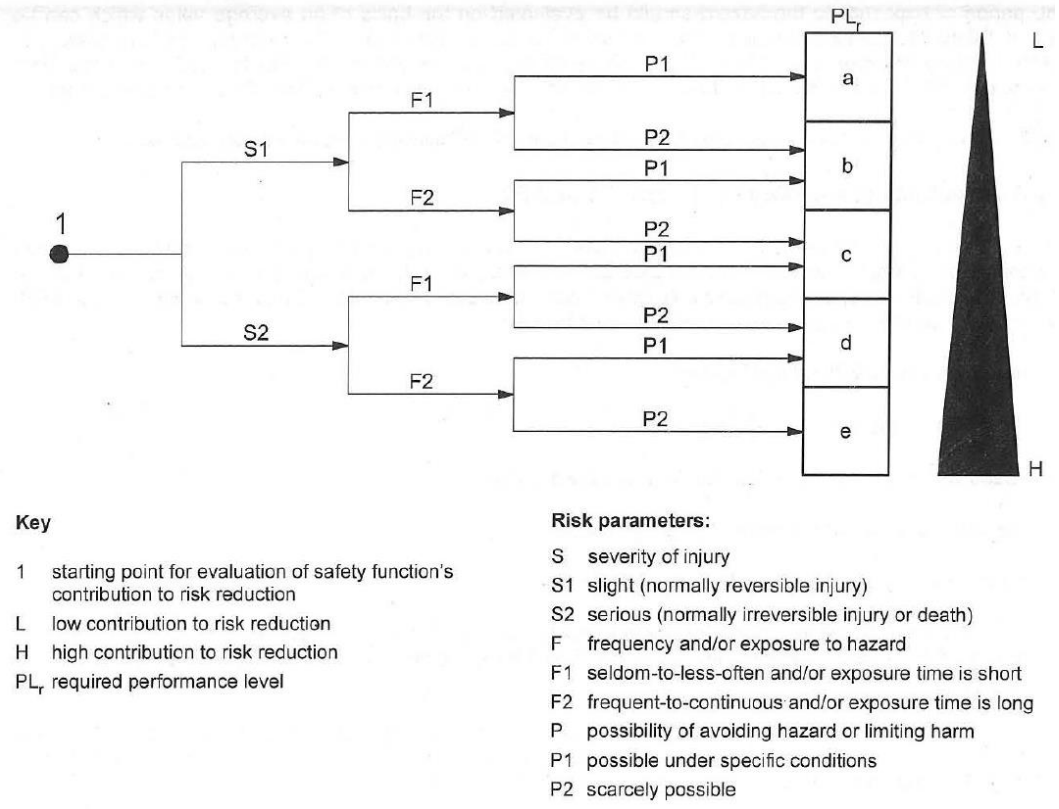


Figure 3 Selection of performance level (ISO13849–1, Annex A)

If the determined performance level is greater than PL'd' (ie. PL'e') then the safety function will be implemented using AS62061 standard. The risk will be evaluated using quantifiable techniques such as fault tree analysis and LOPA for likelihood and weighted average for consequence analysis. Once overall risk is estimated, the target performance requirements will be determined using GPC tolerable risk criteria, refer to Appendix F.

3.4.3. Deliverables

- Updated safety requirement specification document

3.5. Design and Technical Realisation of Safety Functions

3.5.1. Overview and Objectives

In this phase of the design process, safety function will be designed and realised using safety systems. Refer to label 4 of Figure 2 for the context of this phase within the iterative design process.

3.5.2. Main activities

The designer may use any of the technologies available to achieve the hardware and software PL requirements, refer to section 4.4 of ISO13849–1 for details.

3.5.3. Deliverables

- Detailed engineering design document

3.6. Evaluation of the achieved performance level

3.6.1. Overview and Objectives

In this phase of the design process, safety functions will be evaluated to determine the achieved performance level. Refer to label 5 of Figure 2 for the context of this phase within the iterative design process.

3.6.2. Main Activities

The achieved PL of safety functions will be determined by grouping of the design parameters (e.g. diagnostic coverage, common cause) by the following;

- Quantifiable aspects (e.g. MTTFd value for single components, DC, CCF, structure)
- Non-quantifiable, qualitative aspects which affect the behavior of the safety function under fault conditions such as systematic failure and environmental conditions

There are several methods for estimating the quantifiable aspects of the PL for any type of system such as Markov modeling and reliability block diagrams which can be used to demonstrate the achieved PL.

The simplified method based on the five designated architectures can also be used for evaluation purposes for safety functions up to PL'c'. Refer to section 4.5 of ISO13849–1 for details of achieved PL.

3.6.3. Deliverables

- A separate document is suggested to document the results of the evaluated PL

3.7. Verification of Performance Level

3.7.1. Overview and Objectives

In this phase of the design process, safety functions will be verified against the achieved performance level. Refer to label 6 of Figure 2 for the context of this phase within the iterative design process.

3.7.2. Main activities

The verification process will be in accordance with section 4.3 of the standard. If the achieved PL does not meet the required PL, the iteration process described in Figure 3 of the standard will be applied.

3.7.3. Deliverables

- Verification results can be included within the same document developed in section 3.6.

3.8. Validation of performance level

3.8.1. Overview and objectives

This phase is to confirm that the implemented design of the safety system supports the overall safety requirement specification for the machinery. Refer to label 7 of Figure 2 for the context of this phase within the iterative design process.

3.8.2. Main activities

Validation is an important and comprehensive phase which will be used to demonstrate that each safety function meets the requirements of ISO13849–2.

- Validation will be carried out by persons who are independent of the design of the safety system
- A validation plan will be prepared before carrying out the activity and will identify / describe the requirements for carrying out the validation process for the specified safety functions, their categories and performance levels
- The validation process will include both performance level and categories
- The validation process will review the generic and specific faults, relevant design documentation and previous test records

The validation process will include desktop studies, use of analysis tools and testing of the safety system hardware and software on site.

3.8.3. Deliverables

- Validation plan
- A validation report containing the results of validation

3.9. Maintenance

3.9.1. Overview and Objectives

This phase of safety life cycle is to ensure that the required preventive or corrective maintenance is performed to maintain the specified performance requirements.

3.9.2. Main Activities

A detailed maintenance plan will be developed including routine inspections, testing, preventative and breakdown maintenance. The provisions for the maintainability of the safety system will follow the principles given in ISO12100–2:2003, section 4.7. All information for maintenance will comply with ISO12100–2:2003, 6.5.1.e.

3.9.3. Deliverables

- Detailed maintenance plan with associated documentation

3.10. Technical Information

The purpose of this section in ISO 13849–1 is to ensure that the designer will include all the required safety related documentation in the design package. Refer to section 10 of the ISO13849–1 standard for the list of the required documentation.

3.11. Information for Use

The purpose of this section in ISO13849–1 is to ensure that the information which is important for the safe use of the safety system will be given to the user. Refer to section 11 of the ISO13849–1 standard for the list of the required information.

3.12. Modifications and Change Management

Any required modification in the system will be risk assessed and the results of the risk assessment will be applied to the decision flow chart provided in Figure 1 to determine the appropriate standard for the modified safety function.

Change management will be performed through GPC change management procedures.

4. Safety of Machinery Using AS62061 SIL Requirements

4.1. General

The AS62061 standard will be applied to design and implement a safety function / system for projects where safety consequences include multiple irreversible injury or multiple fatalities or the determined performance level for safety is PL'e'.

It is to be noted that AS62061 does not consider low demand mode for safety functions. As such, a conservative approach will be adopted by applying low demand mode safety functions as a high demand mode. Probability of failure on demand is used in low demand mode and probability of failure per hour is used for high demand mode. PFH values will therefore be used for any calculations while applying AS62061.

It is to be noted that some of the equipment (eg. limit switches) designed for high or continuous demand mode may not be suitable for low demand operation due to maintained status for longer duration (greater than one year). It is expected that the designer will consider the frequency of operation, purpose and environmental conditions

4.2. Introduction to Safety Life Cycle

The safety life cycle is an engineering process that starts from the concept stage and continues until the system is decommissioned. The purpose of the safety life cycle is to ensure that the safety instrumented system meets the safety requirements at all times.

A complete safety life cycle can be categorized into three major phases:

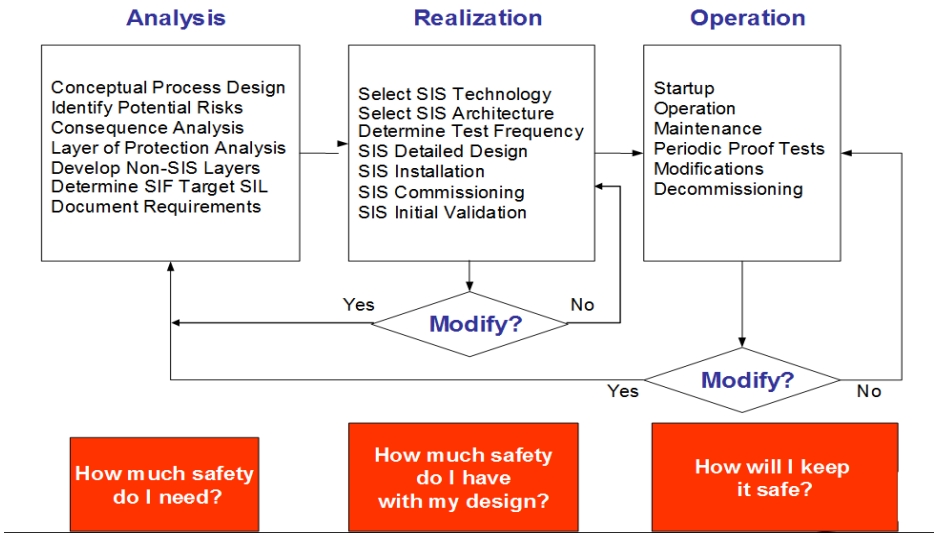


Figure 4 Overview of relationship between different phases of safety life cycle

4.3. Management of Functional Safety

4.3.1. Overview and Objectives

The main objective of this activity is to ensure that the required management and technical activities are specified.

4.3.2. Project Documentation

The Hummingbird document management system will be used for storage of all project documentation. A document numbering framework will be developed for the suite of documents required throughout the life of the system. Each document must be assigned with a number according to the instrument / tag numbering document. Documentation produced at each step will be verified according to GPC documentation system.

4.4. Analysis Phase

4.4.1. Overview & Objectives

This phase of the life cycle will identify the safety functions which are required to implement the risk reduction measures. The phase will also determine their respective level of integrity and specify the requirements of the safety functions.

The final outcome of this phase will be an analysis phase safety requirement specification (SRS). The purpose of the SRS will be to provide the broad requirements for a safety system design.

4.4.2. Main Activities

4.4.2.1. Safety Function Identification

Safety functions will be identified from the hazard and risk assessment study as outlined in section 3.2 (i.e. for multiple permanent injuries or multiple fatalities).

4.4.2.2. Safety Function Classification

The SIL level for each safety function will be classified on the basis of likelihood and consequence analysis. The estimated risk value will be used with the GPC tolerable risk values / criteria to determine the amount of risk reduction required for each safety function. Refer to Appendix F for GPC Tolerable risk criteria and the example for its application.

4.4.2.3. Preparation of the Safety Requirements Specification

The SRS will be comprehensive and will provide a single point of reference for the technical and functional requirements. The SRS will also consider requirements of operational and maintenance phases within the SLC.

The proof testing and maintenance strategy of all individual safety functions will be developed during this specification stage so that the necessary allowances can be made in the design of the hardware and software. Refer to AS62061 clause 5 for detailed requirements regarding what needs to be included in the SRS.

4.4.3. Deliverables

The deliverables in this phase will contain the following typical information;

- Hazard and risk assessment report
- SIL Classification study report
- Safety requirement specifications

Refer Appendix H for a typical SRS template

4.5. Realisation Phase

4.5.1. Overview & Objectives

The main objective of this phase will be to ensure that the hardware is designed to fully comply with the detailed requirements of the SRS. Figure 5 on the following page provides the design and development activities for the realisation phase.

4.5.2. System Architecture Design

4.5.2.1. Overview & Objectives

The objective of this activity will be to describe the functional and integrity requirements of each safety function and to define the required subsystems. Refer to label 2 of Figure 5 for the context and timing of this phase. Refer to AS62061 clause 6.6.2.1.1 and 6.6.2.1.2 for further guidance.

4.5.2.2. Main Activities

An initial concept level architecture of the safety system will be developed by decomposing each safety function to a structure of function blocks.

4.5.2.3. Deliverables

- Architecture block diagram for the safety system

4.5.3. Detail the Safety Requirements

4.5.3.1. Overview & Objectives

Each safety function will be designed in detail in this phase. Refer to label 3 of Figure 5 for the context and timing of this phase and to AS 62061 clause 6.6.2.1.6 for further guidance.

4.5.3.2. Main Activities

Update the initial analysis phase SRS with the details of each function block, including inputs and outputs of the block and internal logic.

4.5.3.3. Deliverables

- Updated SRS

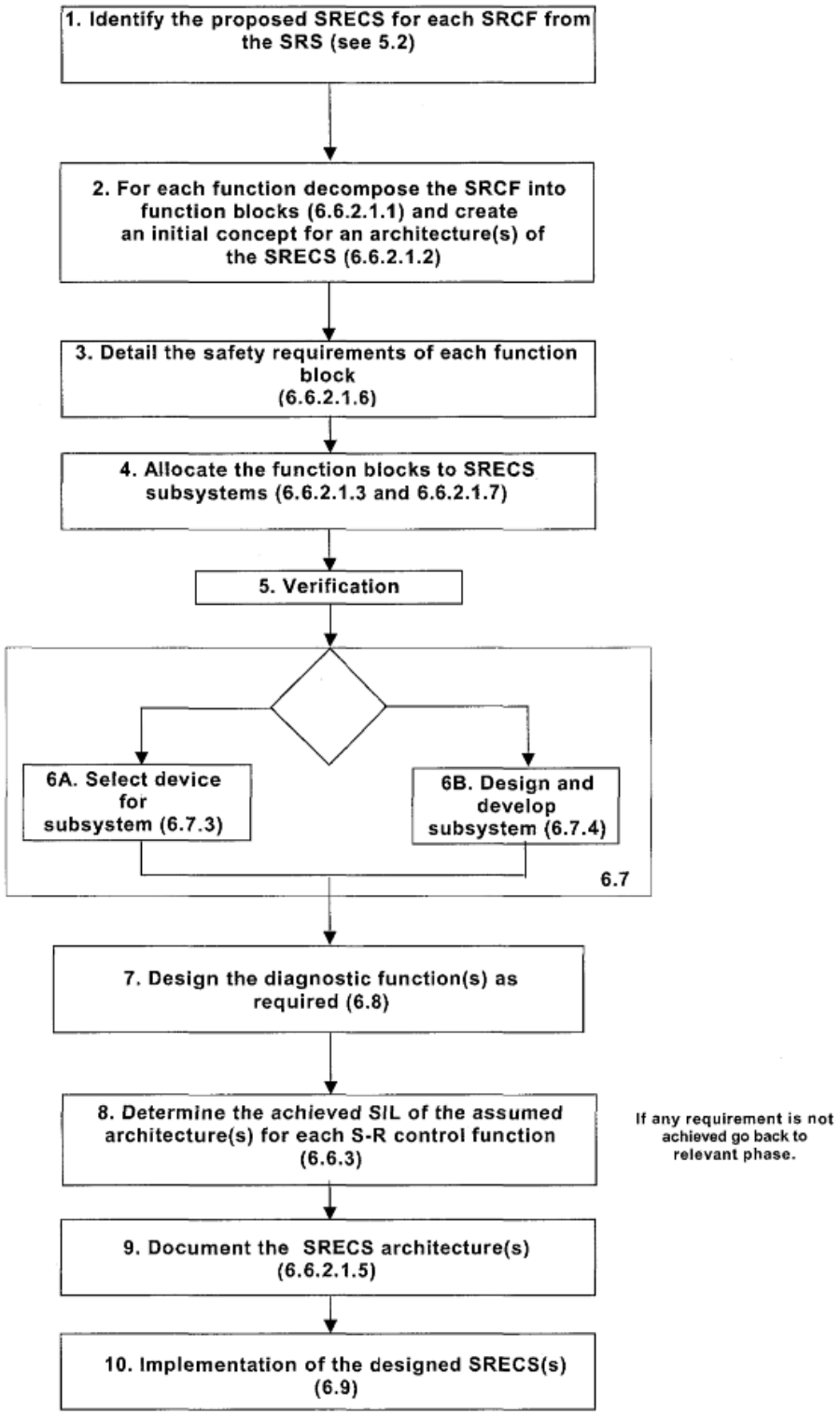


Figure 5 Safety system design and development overview (ref. AS 62061, Figure 2)

4.5.4. Allocate Function Blocks to Subsystems

4.5.4.1. Overview & Objectives

Each safety function will be allocated in the system hardware and software during detailed engineering. Refer to label 4 of Figure 5 above for the context and timing of this phase and to AS 62061 clause 6.6.2.1.3 and 6.6.2.1.7 for more guidance.

4.5.4.2. Main Activities

Allocate each function block to a subsystem within the safety system architecture. More than one function block can be assigned to a subsystem. The highest integrity requirement of multiple function blocks will be applied to the subsystem.

4.5.4.3. Deliverables

- Updated SRS

4.5.5. Design Verification

4.5.5.1. Overview and Objectives

The main objective of this activity will be to verify that the actual design complies with the engineering level design. The verification phase provides a check on how effectively the SIS is being managed. AS62061 shows verification as a hold point following architectural design of the safety system. Verification should also be a recurring activity and will be conducted throughout the design and development of the safety system. Refer to label 5 of Figure 5 above for the context and timing of this phase.

4.5.5.2. Main Activities

Progress review meetings

A schedule will be in place to review the progress of each activity against its agreed completion date or frequency. This is essentially a go/no go review, suitable evidence will be provided to justify the close-out of any item.

4.5.5.3. Deliverables

The following will be the deliverables of this phase.

- A progress report for each verification activity
- An approved close-out report for each action - containing documented evidence that the action has been completed, e.g. report or memorandum.

4.5.6. Selection or Design of Subsystems (hardware)

4.5.6.1. Overview and Objectives

The objective of this phase will be to realize a subsystem that fulfills all safety requirements of the allocated function blocks. Refer to label 6 of Figure 5 above for the context and timing of this activity.

4.5.6.2. Main Activities

The required design activities are contained in AS62061 clause 6.7. As a summary, the key items to address in the design and selection of subsystems will be:

- Architectural constraints (AS62061 clause 6.7.6)
- Probability of dangerous random hardware failures (AS 62061 clause 6.7.8)
- Requirements for systematic integrity (AS62061 clause 6.7.9.1 and 6.7.9.2) or evidence that the equipment is ‘proven in use’ (AS61508.2 clause 7.4.7.5 to 7.4.7.12)
- Requirements for subsystem behavior on detection of a fault (AS62061 clause 6.3)

4.5.6.3. Deliverables

- A detailed safety system design with all relevant documentation / dossiers

4.5.7. Design and Engineer Safety System Application Software

4.5.7.1. Overview & Objectives

Although Figure 5 does not show software design explicitly, it is a key activity of the workflow. The main objective of this task is to set criteria to ensure that the application software has been designed in full compliance with the safety requirement specifications. The software used to program a safety PLC will be SIL certified.

4.5.7.2. Main Activities

Software Specifications

The specification of the application software will be derived from the SRS and will be included in an overall SIS technical specification document. The specification will clearly indicate how the SRS will be translated into configured software. More detailed guidance is available in AS62061 clause 6.10

Application Software Design and Development

Software design and development requirements are given in AS62061 clause 6.11.3, and are based on AS61508.3.

Software Integration Testing (FAT)

The safety system software will be tested comprehensively during the factory acceptance and integration testing. See AS62061 clause 6.11.3.8 for further details.

Software Auditing

The application software will be verified at appropriate stages throughout the development phase. Testing will be the main verification method, and will be planned with the results fully documented. Refer to AS62061 clause 6.11.3.2 for more details.

4.5.7.3. Deliverables

The following deliverables are expected in this phase:

- Software safety requirements specification
- Specific software test plans and results
- Software architecture design (including functional block diagrams of the final software and I/O data list)
- A report that sets out the techniques and measures necessary to meet the specification (AS62061 clause 6.11.3.3.3 and 6.11.3.3.4)
- Application software , including information required by AS62061 clause 6.11.3.4.5

4.5.8. Design of the Diagnostic Function(s)

4.5.8.1. Overview & Objectives

The objective of this phase will be to realise the diagnostic functions that maybe required to fulfil the requirements for architectural constraints and PFH. Refer to label 7 of Figure 5 above for the context of this phase. Further detail is provided in AS 62061 clause 6.8.

4.5.8.2. Main Activities

Design and document the necessary diagnostic functions including description of each diagnostic function, what failures it detects, its reaction to a failure, and an analysis of the contribution it makes to the safety integrity of its respective safety function is to be provided.

4.5.8.3. Deliverables

- Updated realisation phase SRS including the necessary information for the diagnostic functions

4.5.9. Determine the Achieved SIL

4.5.9.1. Overview & Objectives

The objective of this activity will be to confirm that each safety function can achieve the required level of risk reduction that it has been assigned. Refer to label 8 of Figure 5 for the context of this activity. Refer to AS 62061 clause 6.6.3 for further guidance.

4.5.9.2. Main Activities

Review of each safety function to confirm that it meets the hardware integrity requirements in terms of:

- Probability of dangerous failures per hour
- Architectural constraints
- Systematic safety integrity

4.5.9.3. Deliverables

- Methodology for estimating the PFH for each safety function
- PFH results for each safety function
- An assessment for each safety function in terms of architectural constraints and systematic safety integrity

4.5.10. Document the Safety Function Architecture

This phase of the safety life cycle confirms that the safety function can achieve the required level of safety. Refer to label 9 of Figure 5 for the context and timing of this phase. Refer to AS62061 clause 6.6.2.1.5 for more guidance.

4.5.11. Implementation of the Designed Safety System

4.5.12. Overview & Objectives

The objective of this phase will be to implement the safety system in accordance with the documented design and to validate that the installed system meets all the requirements of the SRS. Refer to label 10 of Figure 5 above for the context and timing of this phase. Further detailed guidance is available in AS 62061 clause 6.9.

4.5.13. Main Activities

4.5.13.1. Planning

A comprehensive plan will be prepared for the installation, commissioning and validation activities.

4.5.13.2. Installation

The installation of the safety system will include:

- Physical installation of safety system and safety function components
- Inspections according to checklists
- Punch-listing of deficiencies

4.5.13.3. Commissioning

All commissioning records showing the results of activities and resolution of any failures or non-conformances will be produced and retained.

4.5.13.4. Validation (function testing)

The safety system will be fully function tested to validate that it meets the requirements specified within the SRS. Appropriate function test records in the form of test sheets will be produced and retained for future records.

4.5.13.5. Management of Change during Installation, Commissioning and Validation

Any change which is necessary as a result of the installation, commissioning or validation activities will be implemented according to the approved change management procedures and will be managed as a modification.

4.5.14. Deliverables

- Updated safety management plan with details of installation, commissioning and validation plans
- Signed and approved installation, commissioning and validation records
- Dossier containing all relevant “Information for use” as per AS 62061 clause 7

4.6. Operation and Maintenance Phase

4.6.1. Overview & Objectives

The main objective of this phase will be to ensure that the safety system will meet the required SIL throughout its operational life. This phase will commence at the point of handover / acceptance and will continue until final decommissioning of the safety system.

4.6.2. Operation and Maintenance

4.6.2.1. Overview & Objectives

The main objective of this phase will be to ensure that the safety system will meet the required SIL level after handover and during operational life.

4.6.2.2. Main Activities

Competence Management

A system will be established to develop, assess and maintain the competence of operational, maintenance and engineering personnel in all aspects of the SLC. The system will have a blend of formal staff trainings and field experience, refer to section 1.7 for details.

Preventative and Predictive Maintenance

The preventative and predictive maintenance of the safety system components should be controlled by the Maintenance Management System and defined according to experience and the manufacturer's recommendations.

Corrective Maintenance

The initial corrective action (operational and / or maintenance) on any safety system component failures will be clearly defined and documented in procedures.

Trip Reporting

A procedure will be in place to report plant trips following a safe failure of any SIS components. The report will capture as a minimum the following causes of any trip:

- Intended operation (real demand)
- Equipment failure
- Human error
- Other (unknown) cause

Incident Investigation

A procedure will be in place to investigate and report any safety function related incidents which actually lead to, or have potential to lead to, a hazardous event. The investigation reports will contain detailed findings and recommendations for the improvement and include action parties, target completion dates and plans for implementation follow-up.

Failure Rate Data Collection

Clear definitions mentioning what constitutes a failure for safety system components will be established. Actual safe and dangerous failure rates of safety system components (initiators, logic solver and final elements) will be compiled for input into a 5 yearly SRS review.

Safety Requirements Specification Review

The ongoing validity of the SRS will be reviewed in line with the requirement for 5-yearly reviews of the Hazard and Risk Analysis and SIL Classification.

4.6.2.3. Deliverables

- Maintenance Management System records of safety function components
- Updated SRS
- Reports showing level of compliance with proof testing schedule
- Trip reports for trips caused by safe failure of safety function components
- Investigation reports for safety function related incidents
- Audit reports

4.6.3. Modification

4.6.3.1. Overview & Objectives

The main objective of this section is to ensure that the safety system will meet the required SIL level both during and after the modification phase. The modification or decommissioning of the SIS will prompt a review of the earlier stages of the safety life cycle. The specific safety life cycle activities will need to be revisited for the particular modification or decommissioning activity (Figure 4). Refer to AS62061 clause 9 for more detailed requirements.

4.6.3.2. Main Activities

Risk Analysis

The hazards arising either during or as a result of modification will be analysed.

Design and Development

The requirements for modifications will be the same as those for the design and development phases. Procedures for authorising and controlling changes to a safety system will be developed according to the requirements specified in AS62061 clause 9.3. These procedures will also consider decommissioning of a safety system.

Installation, Commissioning and Validation

The requirements for implementation of a modification will be the same as those for installation, commissioning and validation phases.

Documentation and Close-out

The documentation relating to safety functions, including the SRS will be updated after modification.

4.6.3.3. Deliverables

The GPC change management procedure will be followed; a change record will be created with the following information:

- Description of change and reason for implementation
- Hazards or hazardous situations that may arise either during or as a result of a modification
- Validation test results
- Updated documentation including drawings and the SRS

4.6.4. Decommissioning of Safety System

4.6.4.1. Overview and Objectives

The main objective of this phase is to ensure that a safety function will meet the required SIL both during and after decommissioning. The decommissioning of one or all safety functions may fall within the scope of a replacement or major upgrade. The deletion of one or more functions would normally be considered as a modification. In general, requirements for the modification phase are applicable.

4.6.4.2. Main Activities

Risk Analysis

The hazards associated with decommissioning will be analysed either by a new risk analysis or through a revision of an existing risk analysis for the relevant sections of the process.

Design and Development

The detailed design of decommissioning requirements will be the same as those for the design and development phases.

Installation, Commissioning and Validation

The requirements will be same as those for installation, commissioning and validation phases.

Documentation and Close-out

The documentation relating to functions including the SRS will be updated and if necessary made redundant following the decommissioning.

4.6.4.3. Deliverables

The GPC change management procedure will be followed and a change record will be created with the following information:

- Description of the change and the reason for decommissioning
- Hazards or hazardous situations that may arise either during or as a result of decommissioning
- Updated documentation including drawings and the SRS

Appendices

Appendix A: Definitions

General

The following definitions below will be applicable throughout this document.

The **Contractor** is the party that carries out all or part of the design, engineering, procurement, construction, commissioning or management of a project, or operation or maintenance of a facility. The Company may undertake all or part of the duties of the Contractor.

The **Manufacturer / Supplier / Vendor** is the party that manufactures or supplies equipment and services to perform the duties specified by the Contractor.

The **Company** is the party that initiates the project and ultimately pays for its design and construction. The Company will generally specify the technical requirements. The Company may also include an agent or consultant authorised to act for, and on behalf of, the Company.

The words **shall / must / will** indicate a mandatory requirement.

The word **should** indicate a recommended course of action.

The words **may / can** indicate one acceptable course of action.

Technical

Basic Process / Plant Control System

The system which responds to input signals from the process and generates output signals to maintain operation of the process in a desired state. The system does not perform functions assessed as SIL 1 or higher. This includes Plant PLC or DCS and any other control system not used for safety related functions.

Beta Factor

The number of common mode failures (of redundant initiators or final elements), expressed as a fraction of all possible failures.

Common Mode Failure

A failure with the potential to affect all duplicated components in a redundant configuration due to common characteristics.

Dangerous Failure

A failure which has the potential to place a safety function in a state in which it will fail to perform its function. Dangerous failures are usually only revealed when the system has to perform a certain action or through testing.

Dangerous Failure Rate

It is the number of dangerous failures occurring per unit of time.

Demand

A process or equipment condition or event which requires a safety function to take action to prevent a hazardous situation.

Demand Rate

The frequency at which a demand occurs, i.e. the number of demands per unit time.

Diagnostic Coverage Factor

The number of dangerous failures that the diagnostic features are capable of detecting expressed as a fraction of all possible failures.

Dossier

Collection of documentary evidence for a facility, which is used to support a claim for compliance with this standard.

Fault Tolerance

A configuration in which plant integrity is not compromised by the dangerous failure of a single safety component.

Failure

An abnormal condition that may cause a reduction in, or loss of the capability of the safety function to perform its intended function.

Function Test

Test of safety function during installation and commissioning that demonstrates its correct functioning.

Function Block

The smallest element of a safety function whose failure can result in a failure of the safety function.

Functional Safety Assessment

Investigation based on objective and documented evidence to judge the level of functional safety achieved.

Hazard or Hazardous Situation

A situation or an object that has potential to cause harm, including ill health and injury, damage to property, products or the environment, production losses or increased liabilities.

High Demand or Continuous Mode

Mode of operation in which the frequency of demands on a safety function is greater than one per year or greater than twice the proof-test frequency.

Logic Solver

It is the portion of safety function which performs the application logic. These may include electromechanical relays, solid state/magnetic core logic and the central processing unit (CPU) section of programmable electronic systems.

Machinery

The assembly of linked parts or components, at least one of which moves, with the appropriate machine actuators, control and power circuits, joined together for a specific application, in particular for the processing, treatment, moving or packaging of a material. The terms “machinery” and “machine” also cover an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

Machine control system

A system which responds to an input from, for example, the process, other machine elements, an operator, external control equipment, and generates an output(s) causing the machine to behave in the intended manner.

PL

Discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions.

Probability of Failure on Demand (PFD)

Probability of a safety function failing to respond to a demand.

Probability of dangerous Failure per Hour (PFHD)

Average probability of dangerous failure within 1 h.

Project Safety Management Plan

A project specific management plan that identifies the applicable phases of the safety function life-cycle and details how the objectives for those phases will be achieved in practise.

Proof test

A test carried out on safety components against an approved procedure to confirm that all requirements detailed in the safety requirements specification are met; primarily a strategy to find dangerous failures.

Proof Test Coverage Factor

Number of dangerous failures detected by the proof test expressed as a fraction of all possible failures.

Residual Risk

Risk remaining after protective measures have been taken.

Risk

Frequency at which a hazardous situation occurs multiplied by the consequence of the hazardous situation.

Risk Evaluation

Judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved.

Safe Failure

A failure whose occurrence does not have the potential to place the safety function in a dangerous state.

Safe Failure Rate

The number of safe failures per unit of time.

Safe Failure Fraction

The fraction of all failures that drive the sub-system (e.g. initiator or final element) to the safe state.

Safety Instrumented Systems (SIS)

The electromechanical, electronic and/or programmable electronic logic solver component of the safety instrumented function, including the input and output cards.

Safety Instrumented Function (SIF)

A function comprising the initiator function, logic solver function and final element function for the purposes of early warning, prevention or mitigation of hazardous situations.

Safety Integrity Level (SIL)

Discrete level for specifying the safety integrity requirements of the safety function to be allocated to the safety system.

Safety-Related Control Function (SRCF)

A control function implemented by a SRECS with a specified integrity level that is intended to maintain the safe condition of the machine or prevent an immediate increase of the risk(s).

Safety-Related Electrical Control System (SRECS)

Electrical control system of a machine whose failure can result in an immediate increase of the risk(s).

Safety Requirements Specification (SRS)

A document describing the detailed functional and technical requirements of safety functions. The safety requirements specification is an input to the detailed design of safety functions.

Subsystem

An entity of a top-level architectural design for a safety function where a failure of any component will result in a failure of a safety function.

SRP/CS

Part of a control system that responds to safety-related input signals and generates safety-related output signals.

Trip

The safety action to bring the final element(s) to a safe state.

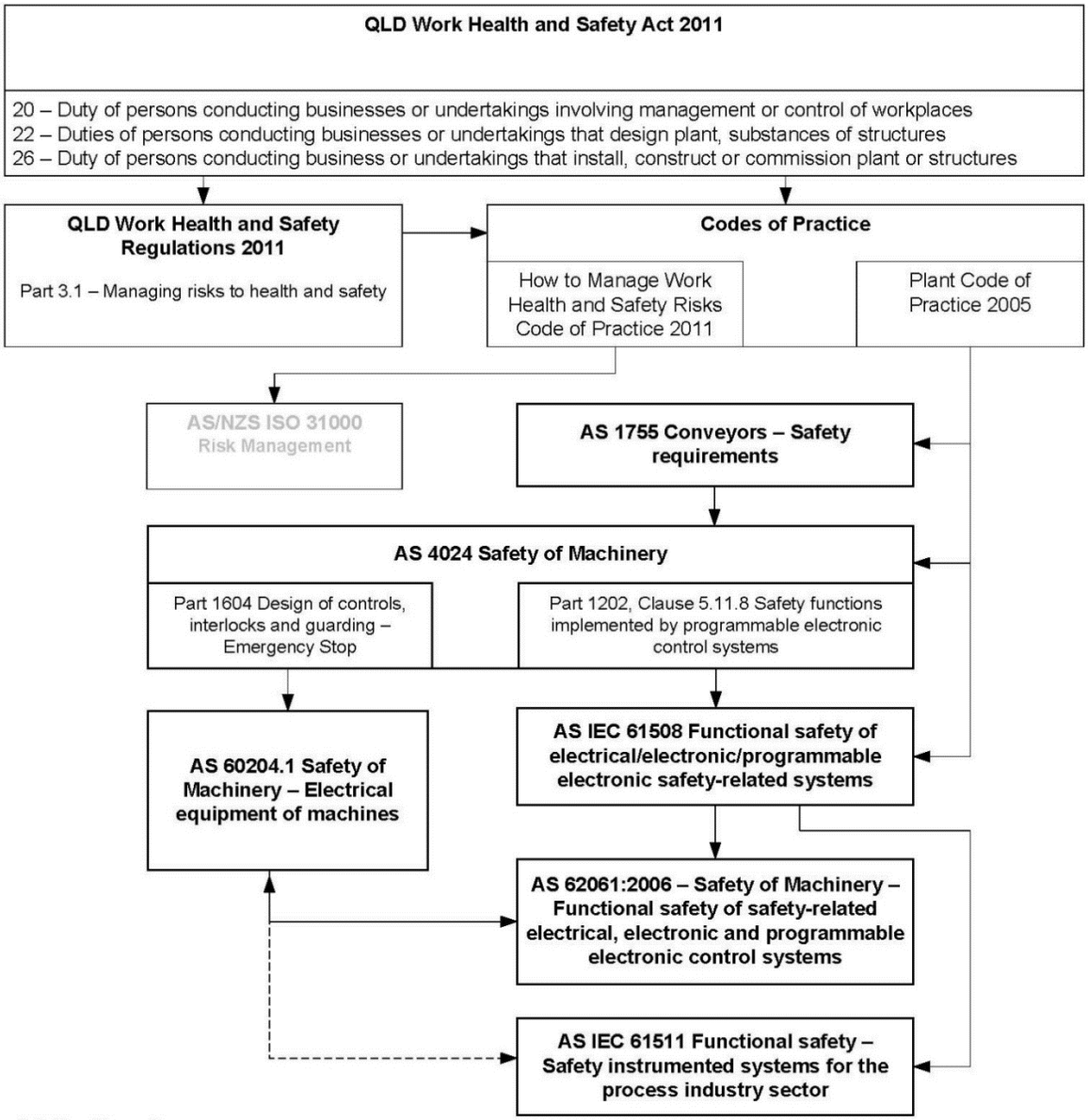
Validation

Confirmation that the system under consideration fully meets the integrity requirements set forth in the associated safety requirements specification.

Verification

Demonstration for a particular life-cycle phase that all deliverables (documents, software and hardware) meet the objectives set for that phase.

Appendix B: Safety of machinery legislative flow chart



Legislative Compliance

Under the Act, there are three types of instruments to help you meet workplace health and safety obligations – regulations, ministerial notices and codes of practice.

If there is a regulation or ministerial notice about a risk, you **must** do what the regulation or notice says.

If there is a code of practice about a risk, you **must** either:

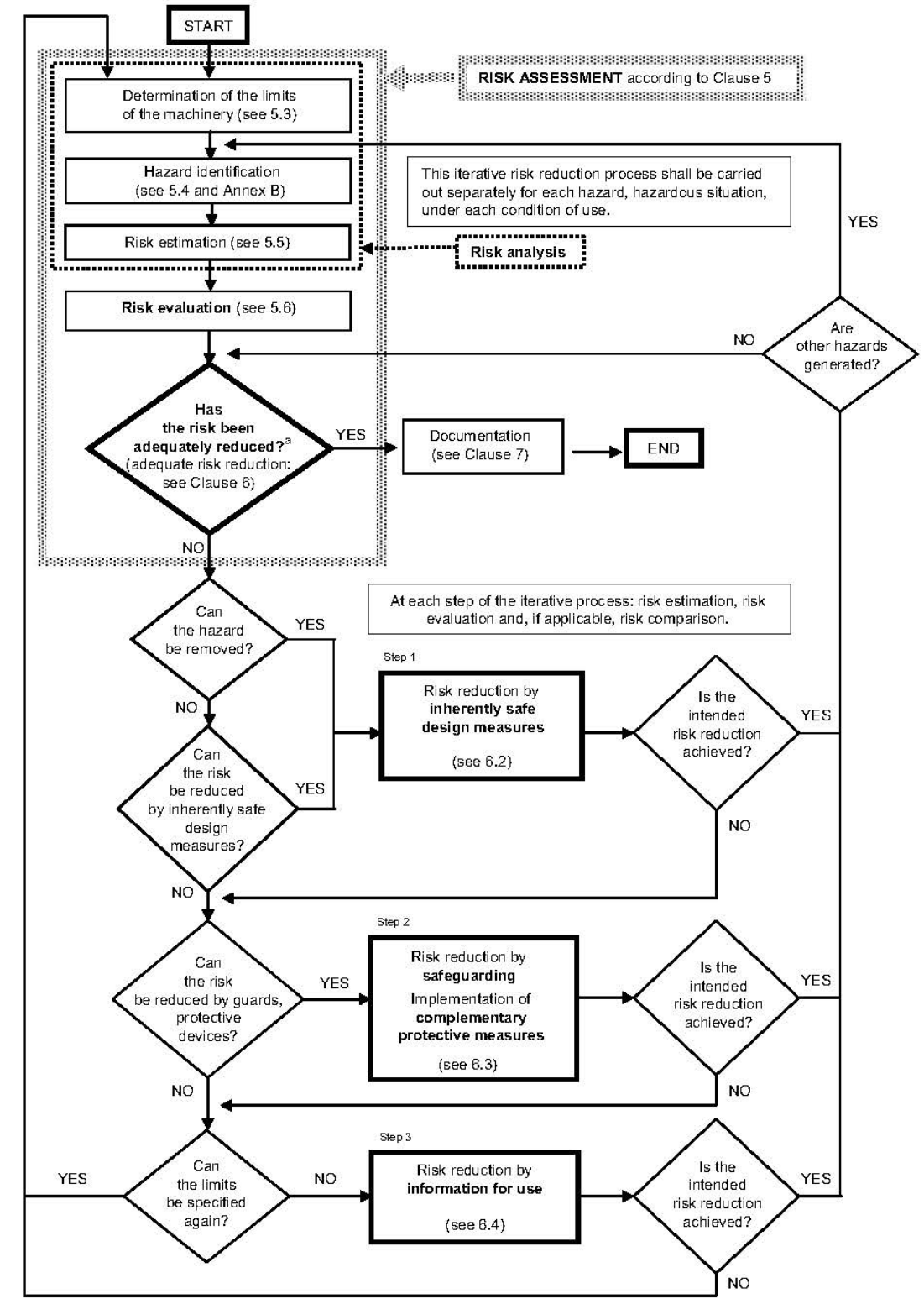
(a) do what the code says, or

(b) do all of the following:

- adopt and follow another way that gives the same level of protection against the risk
- take reasonable precautions, and
- exercise proper diligence.

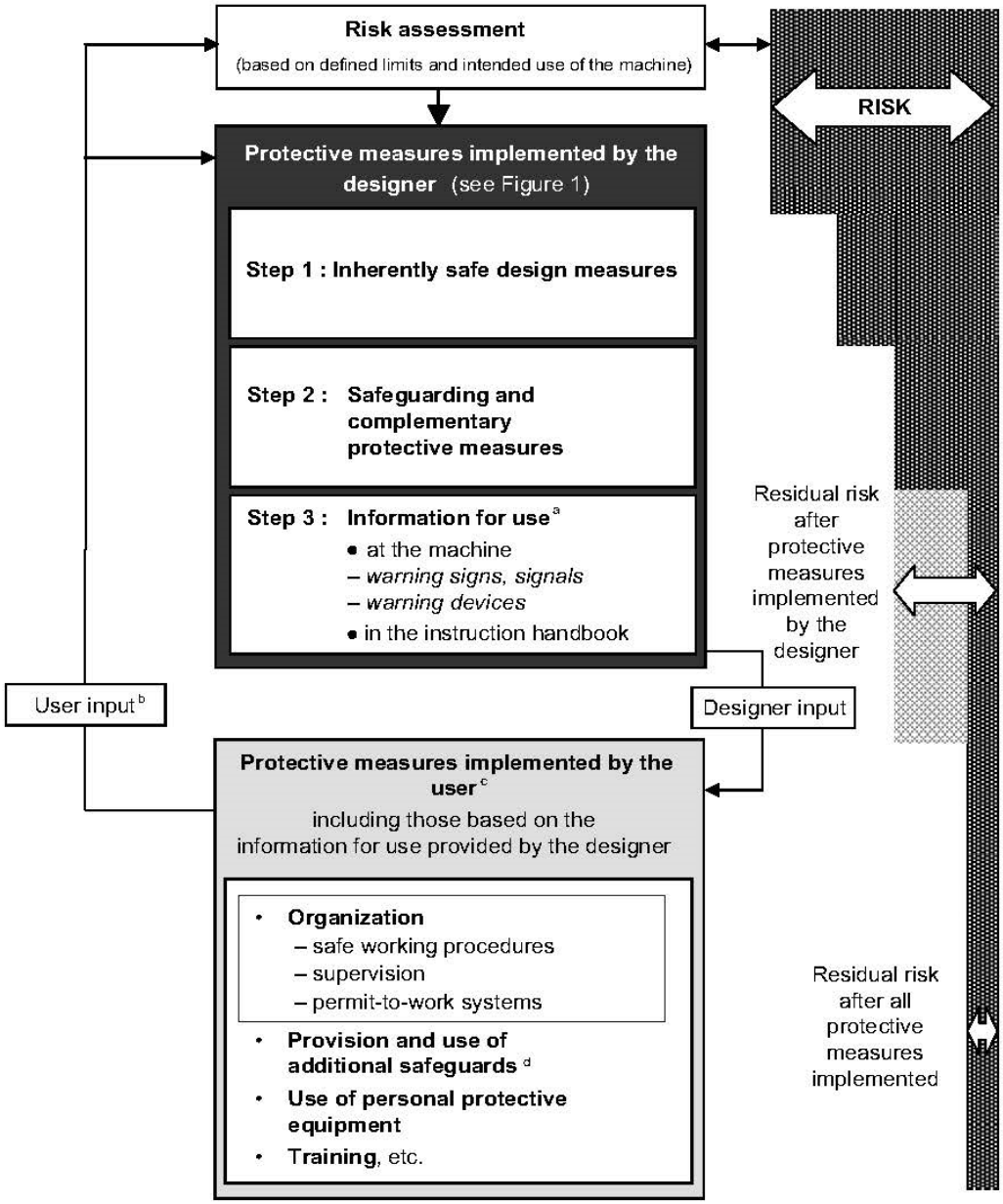
If there is no regulation, ministerial notice or code of practice about a risk, you must choose an appropriate way to manage exposure to the risk and take reasonable precautions and exercise proper diligence to ensure that your obligations are met.

Appendix C: ISO 12100 Risk Assessment Process Overview



a The first time the question is asked, it is answered by the result of the initial risk assessment.

Figure 1 — Schematic representation of risk reduction process including iterative three-step method



[a] Providing proper information for use is part of the designer's contribution to risk reduction, but the protective measures concerned are only effective when implemented by the user.

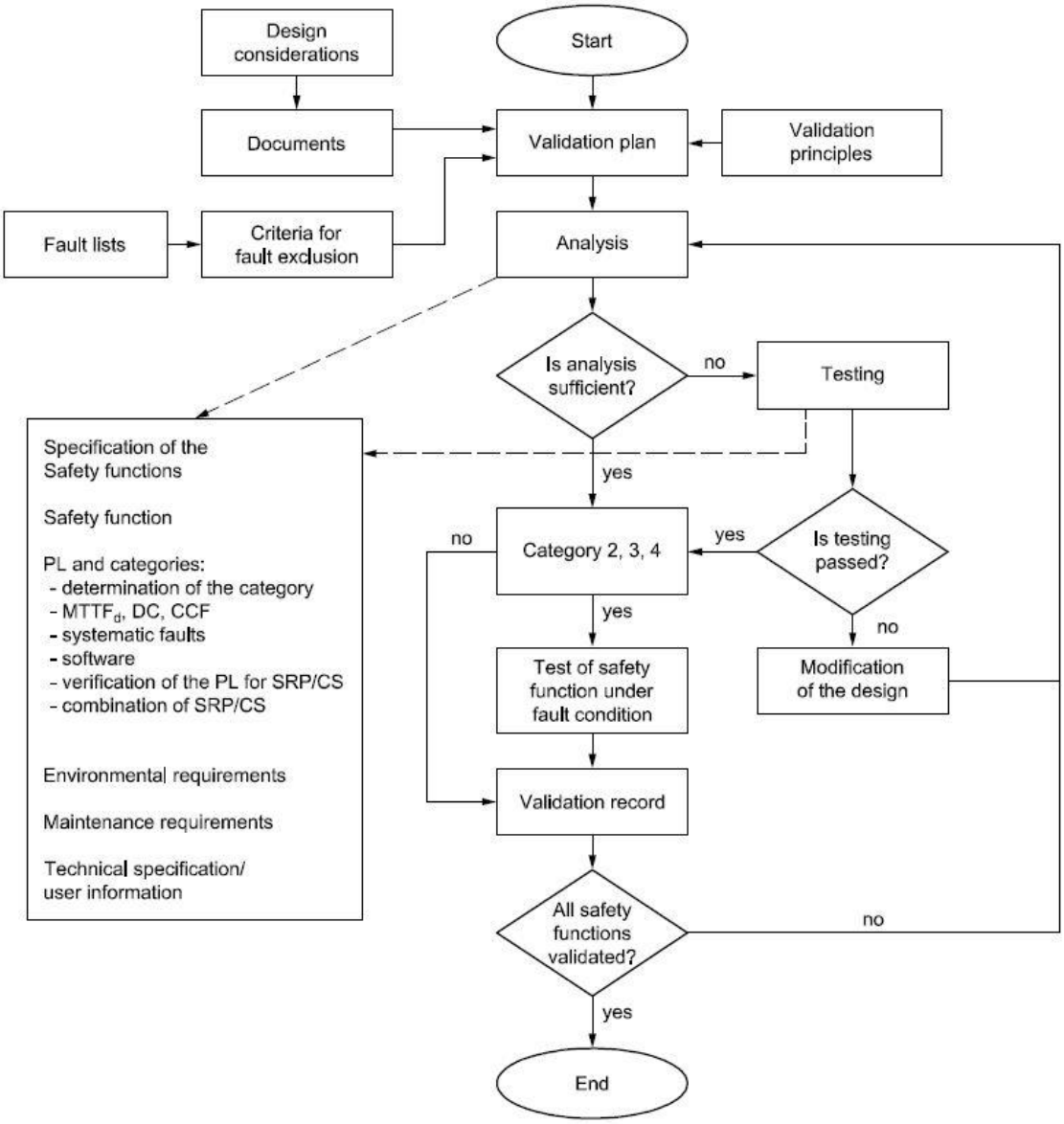
[b] The user input is that information received by the designer from either the user community, regarding the intended use of the machine in general, or from a specific user.

[c] There is no hierarchy between the various protective measures implemented by the user. These protective measures are outside the scope of this International Standard.

[d] These are protective measures required due to a specific process or processes not envisaged in the intended use of the machine or to specific conditions for installation that cannot be controlled by the designer.

Figure 2 — Risk reduction process from point of view of designer

Appendix D: ISO 13849–2 Validation Process Overview



Appendix E: GPC Tolerable Risk Report

Refer to docs # 992180

Appendix F: GPC Risk Matrix

Consequence	Minor (1)	Moderate (2)	Significant (3)	Major (4)	Critical (5)
WH&S (Injury or illness)	First aid treatment, low level short term physical effects. No medical treatment.	Short term reversible disability; or impairment & /or medical treatment injury.	Reversible disability or impairment; &/or medical treatment injuries requiring hospital admission.	Moderate irreversible disability; or impairment requiring specialist treatment &/or intensive care.	Single or multiple fatality; or severe or total irreversible disability & severe impairment.
Environment	Localised & controlled incident with nil or rapidly reversible harm / nuisance.	Localised & controlled with short term reversible harm / nuisance requiring no additional resources.	Significant, localised incident requiring additional resources to remediate harm / nuisance on site; or off site short term reversible harm.	Large uncontrolled event requiring additional resources. Residual onsite harm; or medium term remediation / recovery offsite.	Large offsite event triggering significant response by external agencies; or major onsite residual environmental harm requiring permanent dedicated resources.
Security	Breach of GPC site & maritime security zone - no identified intent for disruption or damage.	Intentional breach of site – no interruption to operations; or repairable vandalism to, theft (<$10,000) of, GPC property.	Intentional breach of restricted access areas - significant damage / business disruptions; or significant theft (>$10,000).	Intentional breach of restricted access - major damage / business disruption; or poses threat to workers, customers or public.	Major extensive damage to critical infrastructure & personnel by terrorist attack or issue motivated groups.
Regulatory Compliance	Regulatory non-conformance warning; or penalty <$10,000.	Court action – fine $10,000 to $75,000.	Court action – fine $75,000 to $250,000.	Court action – fine >$250,000.	Court action – jail sentence; or order to cease major component of GPC operations.
Financial Impact	Losses of $100,000 to $1million.	Losses of $1 to $2.5million.	Losses of $2.5million to $5million.	Losses of $5 million to $10million.	Losses of greater than $10million.
GPC Reputation	Isolated community complaint.	Multiple community complaints on issue / activity; &/or issue reported in local media.	Community concerns / complaints &/or issue reported in state media.	Influence of community / interest groups result in major delay to operations or approvals; or feature in national/ international media.	Influence of community / interest groups curtail critical business operations or major development proposals.
Cargo Handling / Service Delivery	Minor unloading / stockpiling delays – no impact on product availability; or ship loading delay < 1 hr.	Unloading / stockpiling delay – routine management of business impacts; or ship loading delay 1 hour to 1 shift.	Product supply delay causing multiple service disruptions; or ship loading delays 1 shift to 1 day.	Breach of customer contracted capacity & performance; or ship loading delays 1 day to 1 week.	Loss of current & potential significant service contracts due to performance; or ship loading delays > 1 week.
Project Delivery (< $10m)	Project cost overrun < 2%; or < 3% delay.	Project cost overrun 2 - 5%; or 3 - 8% completion delay.	Project cost overrun 5 – 10%; or 8 – 17% completion delay.	Project cost overrun 10 – 15%; 17 – 50% completion delay.	Project cost overrun > 15%; or >50% completion delay.

Appendix G: Typical SRS Template

Refer to docs #1032673 – “Safety Requirements Specification – Shiploader 2”.