Classification and Certification of High Integrity Protection Systems (HIPS)

November 2006

Guidance Note
NI 524 DT R00 E

17 bis, Place des Reflets – La Défense 2 – 92400 Courbevoie
Postal Address : 92077 Paris La Défense Cedex
Tel. 33 (0) 1 42 91 52 91 – Fax. 33 (0) 1 42 91 53 20
Email : veristarinfo@bureauveritas.com
Web : http://www.veristar.com

MARINE DIVISION
GENERAL CONDITIONS

ARTICLE 1

1.1. - BUREAU VERITAS is a Society the purpose of whose Marine Division (the "Society") is the classification ("Classification") of any ship or vessel or structure of any type or part of it or system therein collectively hereinafter referred to as a "Unit" whether linked to shore, river bed or sea bed or not, whether operated or located at sea or in inland waters or partly on land, including submarines, hovercrafts, drilling rigs, offshore installations of any type and of any purpose, their related and ancillary equipment, subsea or not, such as well head and pipelines, mooring legs and mooring points or otherwise as decided by the Society.
The Society:

- prepares and publishes Rules for classification, Guidance Notes and other documents ("Rules");
- issues Certificates, Attestations and Reports following its interventions ("Certificates");
- publishes Registers.

1.2. - The Society also participates in the application of National and International Regulations or Standards, in particular by delegation from different Governments. Those activities are hereafter collectively referred to as "Certification".

1.3. - The Society can also provide services related to Classification and Certification such as ship and company safety management certification; ship and port security certification, training activities; all activities and duties incidental thereto such as documentation on any supporting means, software, instrumentation, measurements, tests and trials on board.

1.4. - The interventions mentioned in 1.1., 1.2. and 1.3. are referred to as "Services". The party and/or its representative requesting the services is hereinafter referred to as the "Client". **The Services are prepared and carried out on the assumption that the Clients are aware of the International Maritime and/or Offshore Industry (the "Industry") practices.**

1.5. - The Society is neither and may not be considered as an Underwriter, Broker in ship's sale or chartering, Expert in Unit's valuation, Consulting Engineer, Controller, Naval Architect, Manufacturer, Shipbuilder, Repair yard, Charterer or Shipowner who are not relieved of any of their expressed or implied obligations by the interventions of the Society.

ARTICLE 2

2.1. - Classification is the appraisement given by the Society for its Client, at a certain date, following surveys by its Surveyors along the lines specified in Articles 3 and 4 hereafter on the level of compliance of a Unit to its Rules or part of them. This appraisement is represented by a class entered on the Certificates and periodically transcribed in the Society's Register.

2.2. - Certification is carried out by the Society along the same lines as set out in Articles 3 and 4 hereafter and with reference to the applicable National and International Regulations or Standards.

2.3. - **It is incumbent upon the Client to maintain the condition of the Unit after surveys, to present the Unit for surveys and to inform the Society without delay of circumstances which may affect the given appraisement or cause to modify its scope.**

2.4. - The Client is to give to the Society all access and information necessary for the performance of the requested Services.

ARTICLE 3

3.1. - The Rules, procedures and instructions of the Society take into account at the date of their preparation the state of currently available and proven technical knowledge of the Industry. They are not a code of construction neither a guide for maintenance or a safety handbook.

Committees consisting of personalities from the Industry contribute to the development of those documents.

3.2. - The Society only is qualified to apply its Rules and to interpret them. Any reference to them has no effect unless it involves the Society's intervention.

3.3. - The Services of the Society are carried out by professional Surveyors according to the Code of Ethics of the Members of the International Association of Classification Societies (IACS).

3.4. - The operations of the Society in providing its Services are exclusively conducted by way of random inspections and do not in any circumstances involve monitoring or exhaustive verification.

ARTICLE 4

4.1. - The Society, acting by reference to its Rules:

- reviews the construction arrangements of the Units as shown on the documents presented by the Client;
- conducts surveys at the place of their construction;
- classes Units and enters their class in its Register;
- surveys periodically the Units in service to note that the requirements for the maintenance of class are met.

The Client is to inform the Society without delay of circumstances which may cause the date or the extent of the surveys to be changed.

ARTICLE 5

5.1. - The Society acts as a provider of services. This cannot be construed as an obligation bearing on the Society to obtain a result or as a warranty.

5.2. - The certificates issued by the Society pursuant to 5.1. here above are a statement on the level of compliance of the Unit to its Rules or to the documents of reference for the Services provided for.

In particular, the Society does not engage in any work relating to the design, building, production or repair checks, neither in the operation of the Units or in their trade, neither in any advisory services, and cannot be held liable on those accounts. Its certificates cannot be construed as an implied or express warranty of safety, fitness for the purpose, seaworthiness of the Unit or of its value for sale, insurance or chartering.

5.3. - The Society does not declare the acceptance or commissioning of a Unit, nor of its construction in conformity with its design, that being the exclusive responsibility of its owner or builder, respectively.

5.4. - The Services of the Society cannot create any obligation bearing on the Society or constitute any warranty of proper operation, beyond any representation set forth in the Rules, of any Unit, equipment or machinery, computer software of any sort or other comparable concepts that has been subject to any survey by the Society.

ARTICLE 6

6.1. - The Society accepts no responsibility for the use of information related to its Services which was not provided for the purpose by the Society or with its assistance.

6.2. - If the Services of the Society cause to the Client a damage which is proved to be the direct and reasonably foreseeable consequence of an error or omission of the Society, its liability towards the Client is limited to ten times the amount of fee paid for the Service having caused the damage, provided however that this limit shall be subject to a minimum of eight thousand (8,000) Euro, and to a maximum which is the greater of eight hundred thousand (800,000) Euro and one and a half times the above mentioned fee.

The Society bears no liability for indirect or consequential loss such as e.g. loss of revenue, loss of profit, loss of production, loss relative to other contracts and indemnities for termination of other agreements.

6.3. - All claims are to be presented to the Society in writing within three months of the date when the Services were supplied or (if later) the date when the events which are relied on of were first known to the Client, and any claim which is not so presented shall be deemed waived and absolutely barred.

ARTICLE 7

7.1. - Requests for Services are to be in writing.

7.2. - Either the Client or the Society can terminate as of right the requested Services after giving the other party thirty days' written notice, for convenience, and without prejudice to the provisions in Article 8 hereunder.

7.3. - The class granted to the concerned Units and the previously issued certificates remain valid until the date of effect of the notice issued according to 7.2. hereabove subject to compliance with 2.3. hereabove and Article 8 hereunder.

ARTICLE 8

8.1. - The Services of the Society, whether completed or not, involve the payment of fee upon receipt of the invoice and the reimbursement of the expenses incurred.

8.2. - Overdue amounts are increased as of right by interest in accordance with the applicable legislation.

8.3. - The class of a Unit may be suspended in the event of non-payment of fee after a first unfruitful notification to pay.

ARTICLE 9

9.1. - The documents and data provided to or prepared by the Society for its Services, and the information available to the Society, are treated as confidential. However:

- Clients have access to the data they have provided to the Society and, during the period of classification of the Unit for them, to the **classification file** consisting of survey reports and certificates which have been prepared at any time by the Society for the classification of the Unit ;
- copy of the documents made available for the classification of the Unit and of available survey reports can be handed over to another Classification Society Member of the International Association of Classification Societies (IACS) in case of the Unit's transfer of class;
- the data relative to the evolution of the Register, to the class suspension and to the survey status of the Units are passed on to IACS according to the association working rules;
- the certificates, documents and information relative to the Units classed with the Society may be reviewed during IACS audits and are disclosed upon order of the concerned governmental or inter-governmental authorities or of a Court having jurisdiction.

The documents and data are subject to a file management plan.

ARTICLE 10

10.1. - Any delay or shortcoming in the performance of its Services by the Society arising from an event not reasonably foreseeable by or beyond the control of the Society shall be deemed not to be a breach of contract.

ARTICLE 11

11.1. - In case of diverging opinions during surveys between the Client and the Society's surveyor, the Society may designate another of its surveyors at the request of the Client.

11.2. - Disagreements of a technical nature between the Client and the Society can be submitted by the Society to the advice of its Marine Advisory Committee.

ARTICLE 12

12.1. - Disputes over the Services carried out by delegation of Governments are assessed within the framework of the applicable agreements with the States, international Conventions and national rules.

12.2. - Disputes arising out of the payment of the Society's invoices by the Client are submitted to the Court of Nanterre, France.

12.3. - Other disputes over the present General Conditions or over the Services of the Society are exclusively submitted to arbitration, by three arbitrators, in London according to the Arbitration Act 1996 or any statutory modification or re-enactment thereof. The contract between the Society and the Client shall be governed by English law.

ARTICLE 13

13.1. - These General Conditions constitute the sole contractual obligations binding together the Society and the Client, to the exclusion of all other representation, statements, terms, conditions whether express or implied. They may be varied in writing by mutual agreement.

13.2. - The invalidity of one or more stipulations of the present General Conditions does not affect the validity of the remaining provisions.

13.3. - The definitions herein take precedence over any definitions serving the same purpose which may appear in other documents issued by the Society.

GUIDANCE NOTE NI 524

Classification and Certification of High Integrity Protection Systems (HIPS)

November 2006

Section 1 General

Section 2 Organizational Methods and Procedures

Section 3 Hardware Analyses

Section 4 Software Analyses

Section 5 Tests Witnessing

SECTION 1 GENERAL

Symbols

β	:	Common cause factor (fraction of undetected failures that have a common cause)
λ	:	Failure rate
λ_D	:	Dangerous failure rate
λ_{DD}	:	Detected dangerous failure rate
λ_{DU}	:	Undetected dangerous failure rate
λ_S	:	Safe failure rate
CCF	:	Common cause failure
DC	:	Diagnostic coverage
ESD	:	Emergency shutdown
FAT	:	Factory acceptance test
FMEA	:	Failure modes and effects analysis
HIPS	:	High integrity protection system
HIPPS	:	High integrity pressure protection system
PFD	:	Probability of failure on demand
PLC	:	Programmable logic controller
PSD	:	Process shutdown
RAMS	:	Reliability, availability, maintainability and safety
SDV	:	Shutdown valve
SFF	:	Safety failure fraction
SIL	:	Safety integrity level.

1 Introduction

1.1 General

1.1.1 Application

The requirements of the present Rule Note apply to offshore units as defined in Part A, Ch 1, Sec 1 [4] of the Rules for the Classification of Offshore Units when the additional class notation **HIPS** is assigned.

1.1.2 The present Rule Note is subdivided into five Sections:

- Section 1: General
- Section 2: Organizational Methods and Procedures

  The Sec 2 describes the tasks to perform and the documents to produce for the verification of the HIPS system according to the requirement of the present Rule Note.
- Section 3: Hardware Analyses

  The Sec 3 describes the tasks to perform and the documents to produce related to Hardware for the verification of the HIPS system according to the requirements of the present Rule Note.
- Section 4: Software Analyses

  The Sec 4 describes the tasks to perform and the documents to produce related to Software for the verification of the HIPS system according to the requirements of the present Rule Note.
- Section 5: Tests Witnessing

  The Sec 5 describes the tests that the Society is to witness to validate the HIPS system before operation and during operation.

Note 1: The sections 2 to 5 are based on IEC 61508 and IEC 61511 requirements.

2 Scope of work

2.1 HIPS system

2.1.1 A HIPS system (High Integrity Protection System) may be used to avoid the following hazards:

- over-pressure hazards
- overheating hazards
- overflow hazards
- corrosive fluid hazards.

2.1.2 The HIPS system is to be a protection system made of multiple barriers:

- process shutdown system (PSD) and emergency shutdown system (ESD) barriers
- one or more independent barriers, named HIPS system.

2.1.3 The HIPS system is to be independent of other process systems.

2.1.4 The HIPS system is to:

- isolate the concerned equipment from the source of danger before the design conditions are exceeded
- mitigate the risk of the concerned equipment exposed to hazard before the design conditions are exceeded by means appropriate to the nature of the risk.

2.1.5 HIPS system is generally made up with the following components:

- inputs: transmitters such as pressure transmitters, level transmitters and temperature transmitters
- logic solver: solid state or PLC (programmable logic controller)
- outputs: solenoid valves and actuators and valves.

Note 1: The list of components is not exhaustive.

Note 2: HIPS system (High Integrity Protection System) may be noted HIPPS system (High Integrity Pressure Protection System).

2.2 Related standards

2.2.1 HIPS system is to be compliant with EN/IEC 61508 standard:

- Part 1 - 1998-12, 1st edition
- Part 2 - 2000-05, 1st edition
- Part 3 - 1998-12, 1st edition
- Part 4 - 1998-12, 1st edition
- Part 5 - 1998-12, 1st edition
- Part 6 - 2000-04, 1st edition
- Part 7 - 2000-03, 1st edition.

2.2.2 HIPS system is to be compliant with CEI 61511 Standard:

- Part 1 - 2003-01, First edition
- Part 2 - 2, First edition
- Part 3 - 3-3, First edition

Note 1: To build a HIPS system with sub-system(s) certified according IEC 61508 only is not a sufficient condition. The whole system is to be certified. Moreover, a company standard is to be defined. Especially, the use of a certified subsystem is not sufficient to reach the compliance with IEC 61508 standard, as the final validation has to be done in the same environment and for the overall safety function.

Table 1 : Definitions

Architecture	Specific configuration of hardware and software elements in the HIPS system
Common cause failure (CCF)	Failure, which is the result of one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure
Dangerous failure	Failure which has the potential to put the HIPS system in a hazardous or fail-to-function state
Diagnostic coverage (DC)	Fractional decrease in the failure rate of dangerous hardware failures resulting from the operation of the automatic diagnostic tests
Diagnostic test interval	Interval between on-line tests to detect faults in a safety-related system that have a specified diagnostic coverage
Detected	In relation to hardware, detected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation
E/E/PE	Electric / Electronic / Programmable Electronic system
Fault	Abnormal state that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function
Fault avoidance	Use of techniques and procedures which aim to avoid the introduction of faults during any phase of the safety life cycle of the HIPS system
Fault tolerance	Ability of a functional unit to continue to perform a required function in the presence of faults or errors
Failure	Termination of the ability of a functional unit to perform a required function
HAZOP	Hazard and operability analysis. Analysis lead to study a process and to identify hazards linked to this process
Impact analysis	Activity of determining the effect that a change to a function or component in a system will have to other functions or components in that system as well as to other systems
Proof test	Periodic test performed to detect failures in a HIPS system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition
PFD	Mean unavailability of safety instrumented systems. It must be understood as the Probability of not Functioning on Demand
PFDAVG	The average, PFDAVG, of this parameter is used to define safety integrity targets and safety integrity levels (SIL). It is often expressed as an average frequency of failure per year
Redundancy	Existence of means, in addition to the means which would be sufficient for a functional unit to perform a required function or for data to represent information
Safety integrity	Average probability of a SIS satisfactorily performing the required safety instrumented function under all the stated conditions within a stated period of time
Safety integrity level (SIL)	Discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the HIPS systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest
SIF	Safety Instrumented Function
Safety instrumented system (SIS)	Implementation of one or more safety instrumented functions. A SIS is composed of any combination of sensor(s), logic solver(s) and final element(s) (IEC 61511). Example: Emergency shut down system, process shut down system. HIPS are particular case of SIS
Safe failure	Failure which does not have the potential to put the HIPS system in a hazardous or fail-to-function state
Undetected	In relation to hardware, undetected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation

3 Definitions

3.1 Main definitions

3.1.1 The main definitions used in the present Rule Note are listed in Tab 1.

4 Documentation to be submitted

4.1 Overall HIPS system

4.1.1 The main documents or information to be submitted for the overall HIPS system are:

- Quality plan
- Project organization
- HIPS system philosophy
- HIPS system specification
- List of HIPS system components
- HIPS system dynamic simulation report
- HIPS system reliability report
- Safety logic diagrams
- HIPS system input/output list
- HIPS components data sheets
- HIPS system SIL assessment
- Tests plans/procedures: For FAT, on-shore tests, off-shore tests
- Tests reports
- Any certificate available
- HIPS operating manual
- HIPS guideline for testing
- HIPS guideline for maintenance.

4.2 HIPS components

4.2.1 The main documents or information for each HIPS component to be submitted are:

- quality plan and fabrication control plan
- all component certificates
- component specifications
- component reliability report
- tests procedures
- tests reports
- dimensional drawings.

SECTION 2 ORGANIZATIONAL METHODS AND PROCEDURES

1 Introduction

1.1 General

1.1.1 This Section presents the methods that are to be used and the main documents to be produced during the design, development, realization, verification, validation, maintenance and modification phases.

The methods and procedures listed in this Section have to be applied by the party applying to classification: that means that all the steps described hereafter have to be applied by all parts.

The basic requirements of this Rule Note are to comply with ISO 9001 requirements. Nevertheless, some additional steps described in the present Rule Note have to be fulfilled.

2 Methodology

2.1 Process

2.1.1 The project is to follow the following process:

- preliminary studies process
- design and development process
- realization process
- verification process
- validation process
- maintenance process
- modification process.

2.1.2 Each specific process mentioned in [2.1.1] is to be submitted and documented.

3 Preliminary studies process

3.1 Overview of the design and development process

3.1.1 The general process is given in Fig 1.

3.2 Step 1: Hazard and risk analysis

3.2.1 This step of the design and development process has to allow determining:

- the hazards and hazardous events of the process and associated equipment
- the sequence of events leading to the hazardous event
- the process risks associated with the hazardous event
- the risk reduction that has to be brought by the HIPS system.

3.2.2 The following methods may be used to help determining the outputs required:

- Preliminary risk analysis
- HAZOP: Hazard and operability study
- QRA: Quantitative risk assessment.

Any other alternative methods are to be submitted and justified.

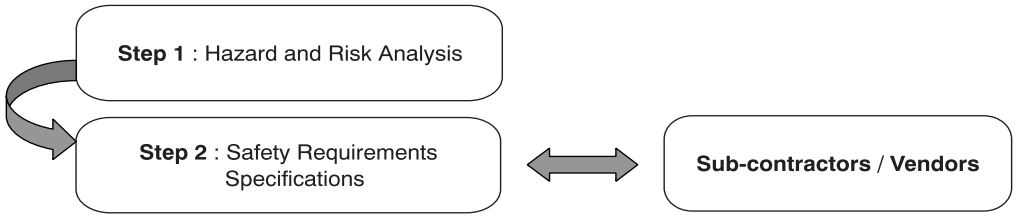
3.3 Step 2: Safety requirements specification

3.3.1 Safety requirements specification step has to:

- allocate the safety integrity level (SIL) to the HIPS system
- specify the other safety requirements concerning the HIPS system.

3.3.2 The minimum SIL required for a HIPS system is to be SIL 3.

Figure 1 : General process



3.3.3 SIL 3 level is to be justified by following the listed requirements:

- common cause failure is to be considered
- safe state of the process is to be defined
- proof-test intervals is to be defined and applied
- the response time requirements for the HIPS system is to be clearly defined
- a description of the process measurements and trip points is to be done
- a description of SIS process output actions and the criteria for successful operation is to be defined
- trip is to be ordered when system de-energises, except if a complete demonstration is given
- HIPS system is to be reset after shutdown
- procedure for starting-up and restarting the HIPS system is to be clearly defined
- all interfaces between the HIPS system and the other systems are to be carefully studied
- the software is to be compliant to SIL 3 level
- the mean time to repair which is feasible for the HIPS system is to be compliant with SIL 3 level
- evidence of compliance to these requirements is to be fully documented
- tests Procedures: Safe state, working procedures, etc.
- maintenance procedures.

3.3.4 Subsequent specifications of HIPS equipment are to be defined and provided to Vendors/Sub-contractors. Compliance to these specifications is to be reviewed during "realization process" (See [5]).

4 Design and development process

4.1

4.1.1 Design and Development process have to ensure that the design and implementation of the Electric/Electronic/Programmable Electronic (E/E/PE) safety related systems meet the specified safety functions and safety integrity requirements.

4.1.2 Design and development process are described in Sec 3 and Sec 4. All the requirements concerning this step of the project are given in these Sections.

5 Realization process

5.1

5.1.1 Realization process has to create a HIPS system compliant with the HIPS system safety requirements.

5.1.2 Realization process is described in Sec 3 and Sec 4. All the requirements concerning this step of the project are given in these Sections.

6 Verification process

6.1

6.1.1 The verification process has to demonstrate for each phase of the project (hazard and risk analysis, safety requirements specification, design and development, realization…) that the outputs meet all the objectives and requirements specified for the concerned phase.

6.1.2 The verification process requires that:

- for each phase, a plan for the verification is established concurrently with the development for the phase
- the verification plan refers to the criteria, techniques and tools to be used in the verification activities.

7 Validation process

7.1

7.1.1 The validation process has to validate, through inspection and testing, that the HIPS system achieve the requirements in every forecasted configurations (safe configuration, default configuration, alarm configuration, etc…) and situation.

7.1.2 The tasks to be performed during the realization process are described in Sec 5.

8 Maintenance process

8.1

8.1.1 Maintenance process has to:

- ensure that the safety level of the HIPS system is maintained during operation and maintenance or to take measures to ensure the same level or to describe all the differences
- operate and maintain the HIPS system so that the designed functional safety is maintained.

8.1.2 Maintenance process has to comply with all these maintenance requirements:

- an operation and maintenance planning (dedicated to the HIPS system) are defined and carried out
- the operators are trained on the function and operation of the HIPS system in their area: the operators have to understand how the HIPS system works, the hazards the HIPS system is protecting against, the operation of all bypass switches and under what circumstances these bypasses are to be used, etc…
- written proof-test procedures are developed.

8.1.3 The operation and maintenance planning have to contain:

- routine and abnormal operation activities
- proof testing, preventive and corrective maintenance activities
- the persons in charge of the activities.

9 Modification process

9.1

9.1.1 Modification process has to:

- ensure that any modification is planned, reviewed and approved by the Society prior to making the change
- ensure that the safety level of the HIPS system is maintained despite of any changes made to the HIPS system.

9.1.2 Any modification process has to comply with these requirements:

- impact analysis, verification and validation are to be carried out before any changes or procedures for authorising and controlling changes
- any document or modified document concerning the description of the modification, the reasons of the modification, the identified hazards which may be impacted, the impact analyses, the verification and validation activities is to be maintained.

9.1.3 Each modification is to be submitted to the Society with the complete file (impact analysis, verification and validation).

SECTION 3 HARDWARE ANALYSES

1 Introduction

1.1

1.1.1 The purpose of this Section is to demonstrate that the HIPS is designed according to applicable specification. Guidance to be applied for this demonstration is given hereafter.

Note 1: This Section is based on IEC 61508 Part II. If a doubt occurs, IEC 61508 Part II or any owner specification if acceptable is to be used.

2 Design and development of HIPS system

2.1 General Requirements

2.1.1 Design and development of HIPS system process aims at complying with SIL level.

2.1.2 Design and development outputs have to prove that the HIPS system is partially fail safe, which means that the HIPS will be put in a predetermined safe state in the event of failure of its components or of its power supplies.

2.1.3 Design and development outputs have to prove that the HIPS system is independent of other systems (PSD, ESD, etc.). When a component can be actuated by the HIPS system and by an other system (for example, a SDV), a dedicated means to actuate this component is to be used for the HIPS (in the example, a solenoid valve).

2.1.4 Design and development outputs have to prove that the design of the HIPS system takes account of human capabilities and limitations and be suitable for the tasks assigned to operators and maintenance staff.

2.1.5 Design and development outputs have to prove that manual means (such as emergency stop button), independent of the Logic Solver, is provided to actuate the HIPS final elements unless otherwise directed by the safety requirement specifications.

2.1.6 Design and development outputs have to prove that the detection of a dangerous fault by diagnostic tests, proof tests or by any other means results in a specified action to achieve or maintain a safe state or continued safe operation of the process while the faulty part is repaired.

2.1.7 Design and development outputs have to prove that the HIPS system is tolerant of one fault or will survive any single failure of its components without jeopardising the safety function.

2.1.8 Design and development outputs have to prove that the HIPS system is designed to facilitate periodic full and partial testing and to record all parameters required to validate any single activation as a formal full or partial test.

2.1.9 Design and development outputs have to prove that a failure of the power supplies will put the system in safe state (example: to close the valves controlled by the HIPPS system).

2.1.10 Design and development outputs have to demonstrate if the component is to be classed (including as a minimum the issuance of Bureau Veritas Marine certificate of inspection) or not.

2.2 RAMS (reliability, availability, maintenance and safety) studies

2.2.1 A functional analysis is to be performed on the HIPS system.

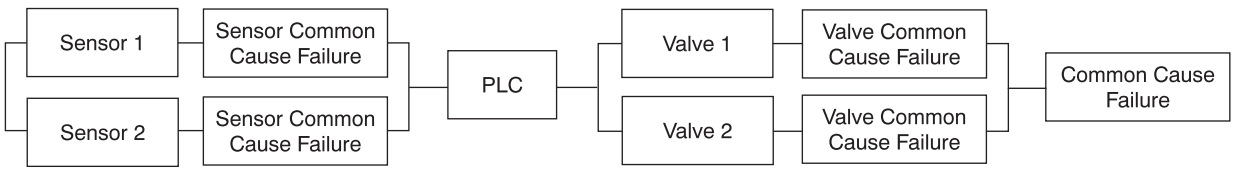
As an example, the system may be modeled with block diagrams in serial and in parallel.

2.2.2 Input/output lists have to be written and the conditions that allow the HIPS to trip is to be explained. The Functional Analysis is to be fully documented.

2.2.3 A document describing the hardware architecture is to be submitted and has to demonstrate that any single failure is not jeopardising the safety function.

2.2.4 A fault tree method may be used to demonstrate that no single event leads to the unwanted event "loss of safety function" and to show the impact of common cause failures.

Figure 1 : Example of block diagram



2.2.5 The HIPS system is to be tested periodically by two means:

- Diagnostic tests performed by the logic solver at fixed frequency. These diagnostic tests can cover a part of the HIPS system only
- Proof-tests performed or started manually at regular interval. These proof-tests have to cover the maximum components and failure modes of the HIPS system.

Note 1: The proof-tests described above are to be traced and documented in the operation and maintenance documentation.

2.2.6 All failure modes that are not detected by a diagnostic test or proof test are to be described. Protective and preventive measures to control these modes are to be taken.

2.2.7 A protective measure is to be taken when a failure is detected through a diagnostic test. All the "failure then detection then protection" scenarios are to be fully documented.

2.2.8 The diagnostic tests and proof-tests are to be described in a document giving, in particular, the detection percentage of each test (diagnostic coverage or DC). This diagnostic coverage is to be reported in the failure mode effect analysis (FMEA).

Examples of diagnostic tests and associated DC are given in IEC 61508 Part II Annex A.

2.2.9 The justifications of common cause failure (CCF) are subdivided into two axes:

- Axis 1: CCF management

  A document is to be prepared to explain the methods, techniques and measures to control and manage the CCF.

  The HIPS system has to include techniques and measures to minimise the CCF. These techniques are to be described and explained.

- Axis 2: Justification of the common cause factor

  The common cause factor is to be evaluated thanks to the document prepared in the axis 1. The common factor can be evaluated for each type of components included in the HIPS system.

  A list of common cause factor is given below:

  - temperature
  - power supply
  - EMC (Electromagnetic Compatibility)
  - software
  - technologies
  - cabling, path
  - fluids
  - corrosion
  - scale/sediment
  - etc.

  In addition of a study performed with the common cause factors evaluated, a sensitivity study is to be performed with a common cause factor equal to 10% ($\beta = 10\%$).

Note 1: The method given in IEC 61508 part VI may be used.

2.2.10 For the HIPS system and for each sub-system, a failure modes and effects analysis (FMEA) is to be documented (refer to IEC 61508 Part II §.7.4.7.4).

As an example, a FMEA can be documented by a table divided into three man parts: FMEA, self-diagnostic and proof-test. Each main parts of this table can be respectively detailed as defined in [2.2.11], [2.2.12] and [2.2.13].

2.2.11 FMEA part

FMEA part of the table describes the failure modes and effects:

- Function: Description of the function performed by the component
- Component: Type of the component
- Code/Reference: Reference number of the component
- Failure mode: Description of failure modes and distribution key, in %
- Cause: Description of failure cause
- Effect: Description of failure effect
- Total Failure Rate λ_T: Failure rate of the component (all failure modes included)
- Failure rate per mode λ: Failure rate per failure mode
- Remarks: Remarks
- Dangerous: 1 if the failure mode is dangerous (failure which has the potential to put the HIPS system in a hazardous or fail-to-function state) and 0 if the failure mode is safe.

Note 1:

If the failure mode is dangerous: $\lambda = \lambda_D$

If the failure mode is safe: $\lambda = \lambda_S$

2.2.12 Self-diagnostic part

Self-diagnostic part of the table describes the self-diagnostics and their effects:

- Test identification: Description of the self-diagnostic test
- Detection: Percentage of failures detected thanks to this self-diagnostic test, equal to DC (Diagnostic coverage)
- λ_{SD}: Safe detected failure rate:

  $\lambda_{SD} = \lambda_S$ DC
- λ_{SU}: Safe undetected failure rate:

  $\lambda_{SU} = \lambda_S$ (1- DC)
- λ_{DD}: Dangerous detected failure rate:

  $\lambda_{DD} = \lambda_D$ DC
- λ_{DU}: Dangerous undetected failure rate

  $\lambda_{DU} = \lambda_D$ (1- DC)

2.2.13 Proof-test part

Proof-Test part of the table describes the proof-tests and their effects:

- Test identification: Description of the proof-tests
- Detection: Percentage of failures detected thanks to this proof-test, equal to TC (Test Coverage)
- $\lambda_{DD'}$: Dangerous detected failure rate:

  $\lambda_{DD'} = \lambda_D$ TC
- $\lambda_{DU'}$: Dangerous undetected failure rate:

  $\lambda_{DU'} = \lambda_D$ (1-TC)

2.2.14 The failure rates indicated in this table are to be extracted from:

- A failure rate databases such as OREDA 2002 and UTE C 80810. If the components are not found in these databases, other databases can be used such as OREDA 1997, Mil-HDBK 217F, IEEE STD 500, etc.
- Field experience. In the case of use of field experience, a complete and documented study is to be available. This study has to describe:
  - the component analysed (Type, reference, environment)
  - the amount of components studied
  - the amount of failures and the type of failures
  - the observation period
  - the calculated failure rate
  - the minimum and maximum failure rates using a confidence level of 90% (using per example, the Khi-square Law - χ^2).

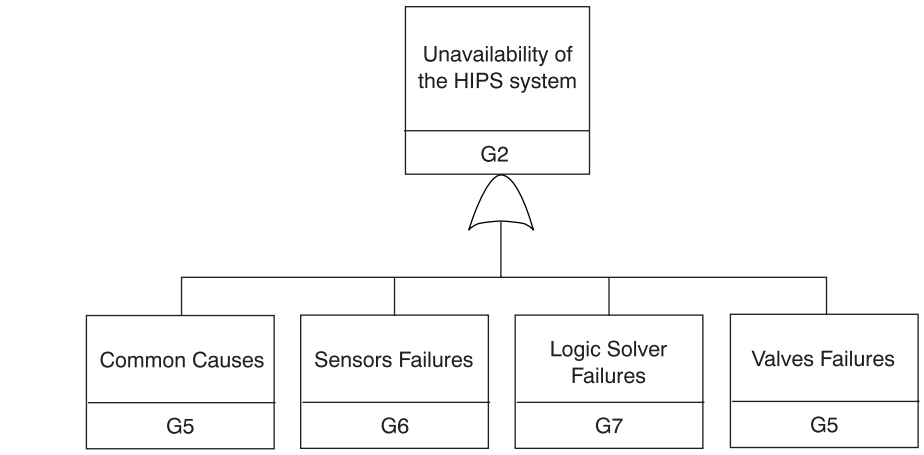
2.2.15 The average probability of failure on demand (PFD) is to be calculated for the overall HIPS system.

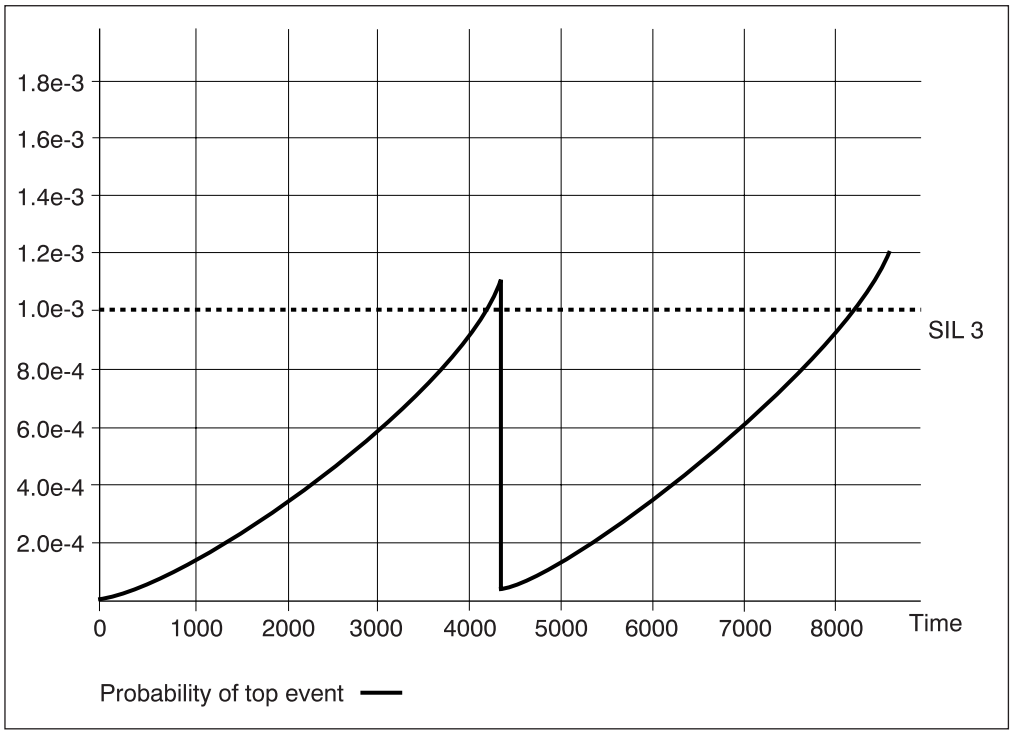
2.2.16 Two different calculations are to be performed:

- The first calculation is to calculate the average PFD with the evaluated
- The second calculation is to calculate the average PFD with β =10%, to obtain a sensitivity calculation.

The PFD calculation is to be submitted.

Figure 2 : Example of fault tree





2.2.17 Fault trees are to be used to calculate the PFD over the lifetime period of the HIPS system.

An example of fault tree and of calculation over the time is given in Fig 2.

The fault tree study is to be fully documented.

2.2.18 When calculating the PFD, two different values are to be given:

- mean value of PFD
- maximum peak value of PFD.

If the peak value is above the accepted limit, the time duration above limit, in%, is to be given.

2.2.19 The safe failure fraction (SFF) is to be calculated for individual component only. The results of the FMEA is to be used to calculate the SFF.

The safe failure fraction is to be equal to:

$SFF = (\Sigma\lambda_{SD} + \Sigma\lambda_{SU} + \Sigma\lambda_{DD}) / (\Sigma\lambda_{SD} + \Sigma\lambda_{SU} + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$

where:

λ_{SD}, λ_{SU}, λ_{DD}, λ_{DU}: Defined in [2.2.12]

2.2.20 The SFF objectives linked to the SIL level are given in Tab 1(refer to IEC 61508 Part II §7.4.3 for more details).

The SFF calculation is to be submitted.

2.2.21 Dynamic simulations are to be performed and documented to determine the needed response time of the system.

This response time is to be verified during the verification and validation stages.

3 Implementation of HIPS

3.1

3.1.1 The information issued during the design and development for each component is to be available during implementation.

3.1.2 All the proof tests taken into account in the calculations are to be fully documented in the operation and maintenance documents.

3.1.3 Each modification is to be traced and analysed (See Sec 2, [9]).

Table 1 : SFF objectives/SIL level

Safe failure fraction	Hardware fault tolerance
	1
SFF < 60%	SIL 1
SFF ≥ 60%	SIL 2
SFF ≥ 90%	SIL 3
SFF ≥ 99%	SIL 4

SECTION 4 SOFTWARE ANALYSES

1 Introduction

1.1

1.1.1 This Section applies only if software is used in the HIPS system.

Software may be used in a logic solver or in an electronic card, such an input card. In this case, this Section has to be followed.

This Section doesn't apply if there is no software used in the HIPS system, such as in a Solid State.

Note 1: This Section is based on IEC 61508 Part III. If a doubt occurs, IEC 61508 Part III is to be used.

2 Software development methodology

2.1 Main Requirements

2.1.1 Methods, techniques and tools are to be selected, applied and documented for each phase so as to:

- minimise the risk of introducing faults into the application software
- reveal and remove faults that already exist in the software
- ensure that the faults remaining in the software will not lead to unacceptable results
- ensure that the software can be maintained throughout the lifetime of the HIPS system
- demonstrate that the software has the required quality.

2.1.2 Test procedures are to be carried out. The following issues should be addressed:

- the policy for integration of software and hardware
- test cases and test data
- types of tests to be performed
- test environment including tools, support software and configuration description
- test criteria on which the completion of the test will be judged
- physical location(s) and its consequences

  (for example, factory or site)
- dependence on external functionality
- appropriate personnel

  (qualification and skills)
- non-conformances.

The methods and techniques to control faults introduced in the software are described in IEC 61508 Part III: refer to this part for more details and especially the tables given in the appendixes.

2.2 Application software requirements

2.2.1 In the case where application software is used, the following requirements have to be followed

2.2.2 The application software has to reach the maximum SIL between the targeted SIL of HIPS system and the targeted SIL of logic solver (if different).

2.2.3 Application software safety requirements (linked to the risk analysis) are to be developed.

2.2.4 Requirements for application software safety are to be sufficiently detailed to allow the design and implementation to achieve the required safety integrity and to allow an assessment of functional safety to be carried out.

The following is to be considered:

- the functions supported by the application software
- capacity and response time performance
- equipment and operator interfaces and their operability
- all relevant modes of operation of the process as specified in the SIS safety requirement specification
- action to be taken on bad process variable such as sensor value out of range, detected open circuit, detected short circuit. In addition, actions to be taken on states in series
- proof tests and diagnostic tests of external devices

  (for example, sensors and final elements)
- software self-monitoring

  (for example, includes application driven watch-dogs and data range validation)
- monitoring of other devices within the SIS

  (for example, sensors and final elements)
- enabling periodic testing of safety instrumented functions when the process is operational
- references to the input documents

  (for example, specification of the SIF, configuration or architecture of the SIS, hardware safety integrity requirements of the SIS).

2.2.5 The application software safety requirements specification has to provide information allowing proper equipment selection. The following is to be considered:

- functions that enable the process to achieve or maintain a safe state
- functions related to the detection, annunciation and management of faults in sub-systems of the SIS
- functions related to the periodic testing of safety instrumented functions on-line
- functions related to the periodic testing of safety instrumented functions off-line
- functions that allow the SIS to be safely modified
- interfaces to non-safety related functions
- capacity and response time performance, even when the system is in the default state
- the safety integrity levels for each of the above functions
- the evidences that the system is safe to be operated using the following methods:
  - software errors and effects analysis (SEEA)
  - critical code review (CCR)
  - formal proof.

SECTION 5 TESTS WITNESSING

1 Introduction

1.1

1.1.1 This Section describes the different steps to be performed and the main documents to be produced during the validation phase. The objective of the validation process is to validate, through inspection and testing, that the HIPS system achieves the requirements.

Inspections and testing witnessing are to be performed in different steps of the project, before and during operation.

This Section defines the tasks that have to be performed under survey of the Society.

2 Tests witnessing process

2.1

2.1.1 The general process may follow the diagram shown in Fig 1.

2.1.2 For all steps, a "test plan" is to be documented including all the inputs, the outputs and the criteria of acceptance and submitted to the Society.

2.1.3 The test plan is to be based on the studies performed during design and development and realization processes.

2.1.4 The steps 1, 2 and 3 shown on Fig 1 can be performed several times, until the criteria of acceptance are reached.

3 Step 1: Factory acceptance tests witnessing (FAT)

3.1 Description of step 1

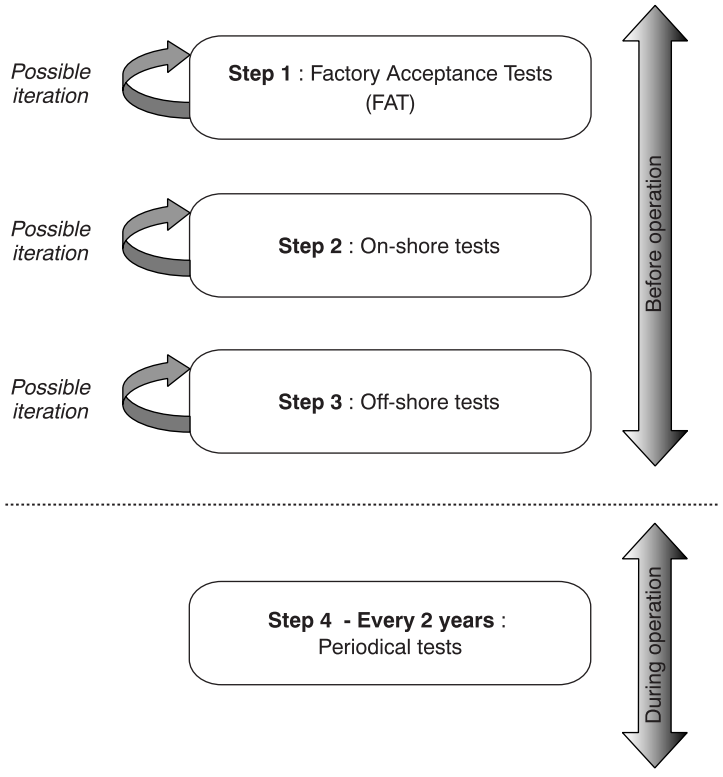
3.1.1 Factory acceptance tests are to be performed by each supplier at the end of the design and development step.

3.1.2 The Society is to be informed of each FAT session performed by a supplier

3.1.3 The Society will decide to witness or not according the safety specifications and the internal analyses.

3.1.4 FAT session is under the responsibility of the supplier. The supplier has the responsibilities to provide the necessary equipment, tools, simulators and qualified technicians/engineers to perform and witness the tests.

Figure 1 : General process



3.1.5 A detailed "FAT plan" is to be written and submitted to the Society before the beginning of the FAT sessions including:

- the references of the relevant documentation
- the exact references of the component tested (Hardware version and Software Version)
- the type of tests to perform: functional tests, performance tests, environmental tests, interface tests, degraded mode tests, etc.
- the description of the tests environment, the tool to use and the dependence on other systems
- the description of the functional tests to perform
- the description of the performance tests to perform according the project specifications and documentation
- the verification of diagnostic tests and proof-tests
- the description of connection and communication tests to perform
- the description of the test acceptance criteria on which the completion of the test is to be judged
- the description of the procedures for corrective action in case of failure of a test
- the description of the personnel involved in the FAT session.

3.1.6 A detailed "FAT report" is to be written and submitted by Society after each FAT session stating:

- the safety cases
- the FAT results for each test
- whether the objectives of the acceptance criteria are met and the final acceptance of the results.

3.2 Examples of FAT

3.2.1 FAT session for transmitters:

Functional tests, leakage tests, response time tests, etc.

3.2.2 FAT session for valves:

Functional tests, torque tests, hydrostatic tests, seat leakage test, etc.

3.2.3 FAT session for actuators:

Functional tests, torque tests, control panel leakage test, quick closing/opening tests, etc.

3.2.4 FAT session for actuator and valve:

Functional tests, hydrostatic tests, quick closing/opening tests, partial and/or full stroking tests, limit switches tests, etc.

3.2.5 FAT session for logic solver only:

Functional tests, inputs/outputs tests, auto-tests verification, etc.

3.2.6 FAT session for the cabinets:

Functional tests, cabling inspection, power supply tests, inputs/outputs tests, etc.

4 Step 2: On-shore tests witnessing

4.1 Description of step 2

4.1.1 On-shore tests are to be performed.

4.1.2 The Society is to be informed of on-shore tests session performed.

4.1.3 Society is to witness only the part related to the HIPS system. Society is to decide to witness 100% of the on-shore tests related to the HIPS or only a sample of the on-shore tests.

The sample depends on the confidence obtained by the Society after the different reviews performed during design and development and realization process (See other sections of the Rule Note).

4.1.4 A detailed "on-shore tests plan" is to be written and submitted to the Society before the beginning of the On-Shore tests sessions including:

- the references of the relevant documentation
- the exact references of the component tested (hardware version and software version)
- the type of tests to perform: functional tests, performance tests, interface tests, degraded mode tests, etc.
- the description of the tests environment, the tool to use and the dependence on other systems
- the description of the functional tests to perform
- the verification of diagnostic tests and proof-tests
- the description of the test acceptance criteria on which the completion of the test is to be judged
- the description of the procedures for corrective action in case of failure of a test
- the description of the personnel involved in the On-Shore session.

4.1.5 A detailed "on-shore tests report" is to be written and submitted to the Society after the session stating:

- the safety cases
- the results for each test
- whether the objectives of the acceptance criteria are met and the final acceptance of the results.

4.2 Example of on-shore tests

4.2.1 General Tests:

- to check HIPS system/other systems communication
- to check of power supply redundancy for each cabinet
- to check high temperature alarm for cabinets
- to check the behavior of the logic solver in replacing cards for example.

4.2.2 Pressure transmitters:

- to check the detection limits
- to check the capability to be protected against false operation.

4.2.3 Voting and safety bars:

To check the shutdown sequence.

4.2.4 To check 100% of the combinations for the voting functions:

- valves
- to check partial or/and full stroking
- to check opening and closing times
- to check solenoid valves commands.

4.2.5 Interlocks:

To check the interlocks.

5 Step 3: Off-shore tests witnessing

5.1 Description of step 3

5.1.1 Off-shore tests are to be performed.

5.1.2 The Society is to be informed of off-shore tests session performed.

5.1.3 The Society is to witness only the part related to the HIPS system. The Society is to decide to witness 100% of the off-shore tests related to the HIPS or only a sample of the off-shore tests.

The sample depends on the confidence obtained by the Society after the different reviews performed during design and development and realization process (See other sections of the Rule Note).

5.1.4 A detailed "off-shore tests plan" is to be written and submitted to the Society before the beginning of the off-shore tests sessions including:

- the references of the relevant documentation
- the exact references of the component tested (hardware version and software version)
- the type of tests to perform: functional tests, performance tests, interface tests, degraded mode tests, etc.
- the description of the tests environment, the tool to use and the dependence on other systems
- the description of the functional tests to perform
- the verification of diagnostic tests and proof-tests
- the description of the test acceptance criteria on which the completion of the test is to be judged
- the description of the procedures for corrective action in case of failure of a test
- the description of the personnel involved in the off-shore session.

5.1.5 A detailed "off-shore tests report" is to be written and submitted to the Society after the session stating:

- the safety cases
- the results for each test
- whether the objectives of the acceptance criteria are met and the final acceptance of the results.

5.2 Example of off-shore tests

5.2.1 General tests:

- to check HIPS system/other systems communication
- to check of power supply redundancy for each cabinet
- to check high temperature alarm for cabinets
- to check the behavior of the logic solver in replacing cards for example.

5.2.2 Pressure transmitters:

- to check the detection limits
- to check the capability to be protected against false operation.

5.2.3 Voting and safety bars:

- to check the shutdown sequence
- to check 100% of the combinations for the voting functions

5.2.4 Valves:

- to check Partial or/and Full stroking
- to check opening and closing times
- to check solenoid valves commands.

5.2.5 Interlocks:

To check the interlocks.