

GENERAL SPECIFICATION

SAFETY

GS EP SAF 361

SIL assignment

01	05/2015	Organisation change – January 2015
00	01/2012	First issue
Rev.	Date	Purpose of the revision

Owning entity: HSEQ/SIRM

Managing entity: HSEQ/SIRM

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 2 of 44

Contents

1. Scope	4
1.1 Purpose	4
1.2 Application	4
2. Reference documents	5
3. Terminology and definitions	6
4. Overall SIL Concept and Methodology	10
4.1 SIL Concept	10
4.2 SIL Assessment Methodology	12
4.3 SIL Assignment Methodology	12
5. Schedule of SIL Assignment	13
5.1 Pre-requisites/ Preparation works to SIL Assignment Workshop	13
5.2 SIL Assignment	13
5.3 Next steps	14
6. Identification of SIF	14
7. Calibrated Risk-Graph Methodology	15
8. LOPA Methodology	26
8.1 Objectives	26
8.2 Application	26
8.3 Methodology	27
8.4 LOPA Organization	30
9. Specific Requirements for HIPS	31
Bibliography	32
Appendix 1 SIF and SIL tables	33
Appendix 2 Rule sets	35
Appendix 3 Extracts from GS EP SAF 041	37
Appendix 4 Risk-graph calibration for production outage	39
Appendix 5 Conducting a SIL assignment workshop	40



General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 3 of 44

Appendix 6	LOPA Worksheet.....	43
Appendix 7	LOPA organisation	44

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 4 of 44

1. Scope

1.1 Purpose

The purpose of this General Specification is to define the methodology and the general principles to be adopted for the Safety Integrity Level (SIL) assignment of Safety Integrated Functions (SIF).

It is accepted the wording's "SIL assignment", "SIL classification", "SIL determination", "SIL targeting", "SIL rating", "SIL setting" have similar meanings, however in this document only the wording "SIL assignment" is used.

It is not the purpose of this document to define the methodology and principles for SIL demonstration or SIL achievement.

The purpose of SIL assignment is not to rework the design of installations, but to:

- Validate/ verify the design against the prescriptive requirements of Company's GS;
- Provide useful information to Operations to set their testing and maintenance philosophies and schedule;
- Define the performance standards of Safety Critical Elements/ Measures (SCE or SCM).

1.2 Application

This General Specification is applicable to any installation (including pipelines), existing or new, and to any of their modifications, where Safety Instrumented Functions (SIF) are handled by the Process Safety System (PSS) or the Emergency Shutdown System (ESD) or the Fire and Gas System (FGS) or to any package equipped with autonomous safeguarding including loading and offloading systems (buoys) and Emergency Release Systems (ERS).

In no case this GS may be used to alter the principles of segregation for Safety Instrumented Systems (SIS), or to down-grade the minimum prescriptive integrity levels as defined in **GS EP SAF 261**.

This GS is applicable, with special requirements set in chapter 9, to any High Integrity Protection Systems (HIPS), (refer to **GS EP SAF 260**).

This GS is applicable only to SIF, and is not applicable to non-instrumented risk-reduction measures e.g. operators training and response, passive protection such as bunds, explosion or fire-proofing.

This GS is applicable only where the design intent of the SIF is to reduce risks to Safety of human life (S), to the Environment (E), or to assets (A). It may be applicable to production loss or deferring (p). It is not applicable to protect Company's Image or Reputation, or to ensure regulatory compliance.

This GS is applicable to all process, utilities, storage and support systems serving the installation.

This GS is only applicable to the life time phase when the installation is handling hydrocarbons (HC), from start-up to decommissioning. It is not applicable to the fabrication, construction,

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 5 of 44

commissioning HC-free phases, and to the dismantling and disposing HC-free works, except if specified otherwise in contractual documents.

This first version of this GS has been developed, and the methods contained herein have been calibrated, for low demand mode, and non disastrous consequences.

In case a SIF is working in high or continuous demand mode, or its failure could result in disastrous consequences e.g. multiple fatalities, seek for Company specialists' advice.

This GS is not applicable:

- To Vendor packages where a prescriptive approach is set in relevant General Specifications and when the Vendor has already performed and supplied the package specific SIL assignment;
- To F&G systems, except executive actions outputs; e.g. extinguishing systems, fire pumps, package shutdown, etc. covered by [GS EP SAF 312](#);
- To all well equipment and flow-lines covered by [GS EP SAF 226](#);

To subsea-installed equipment; however, this GS does apply to all SIF related to SSIV or surface-installed subsea equipment e.g. HPU, HPU PLC, chemical injection.

2. Reference documents

The reference documents listed below form an integral part of this General Specification.

External Documents

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published at the effective date of this document.

Reference	Title
ISO 10418	Petroleum and natural gas industries – Offshore production installations - Basic surface process safety systems
IEC 61508 (Part 1;7)	Functional Safety of Electrical/Electronic/Programmable Electronic (E/E/PE) Safety Related Systems, Parts 1-7
IEC 61511-1	Functional safety – Safety instrumented systems for the process industry sector. Part 1: Framework, definitions, system, hardware and software requirements
IEC 61511-3	Functional safety – Safety instrumented systems for the process industry sector. Part 3: Guidance for the determination of the required safety integrity levels. First edition; incorporates Corrigendum 1 : 10/2004

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 6 of 44

Total General Specifications

Unless otherwise stipulated, the applicable version of these documents, including relevant appendices and supplements, is the latest revision published in the applicable yearly collection.

Reference	Title
GS EP INS 120	Control and Choke Valves
GS EP SAF 021	Layout
GS EP SAF 041	Technological Risk Assessment Methodology
GS EP SAF 226	Completed wells safety systems and safety rules
GS EP SAF 260	Design of High Integrity Protection Systems (HIPS)
GS EP SAF 261	Emergency Shutdown and Emergency De-Pressurisation (ESD & EDP)
GS EP SAF 312	Fire and Gas detection systems

3. Terminology and definitions

There are five types of **statements** in this specification, the “shall”, “should”, “may”, “can” and “must” statements. They shall be understood as follows:

Shall	Is to be understood as mandatory. Deviating from a “shall” statement requires a derogation approved by the Company.
Should	Is to be understood as strongly recommended to comply with the requirements of the specification. Alternatives shall provide a similar level of protection and this shall be documented.
May	Is to be understood as permission.
Can	Is to be understood as a physical possibility.
Must	Expresses a regulatory obligation

Note that “will” is not to be understood as a statement. It is only used when necessary in order to describe a sequence of events.

The following **abbreviations and acronyms** are frequently used in this document:

BPCS	Basic Process Control System
CCE	Central Critical Event
CoFoD	Consequence of Failure on Demand
DCS	Distributed Control System
ERS	Emergency Release System
ESD	Emergency ShutDown
ETP	Exposure Time Parameter

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 7 of 44

F&G	Fire and Gas (function)
FGS	Fire and Gas System
HAZOP	HAZard and OPerability review
HC	HydroCarbons
HIPS	High Integrity Protection System
HSE	Health, Safety and Environment
HPU	Hydraulic Production Unit
ICSS	Integrated Control and Safety System
IPL	Independent Protective Layer
LOPA	Layer Of Protection Analysis
PCS	Process Control System
PFD	Probability of Failure on Demand
PHA	Process Hazard Analysis
P&ID	Piping & Instrument Diagram
PLC	Programmable Logic Computer
PSS	Process Safety System
PSV	Pressure Safety Valve
RRF	Risk Reduction Factor
SCE	Safety Critical Element
SCM	Safety Critical Measure
SIF	Safety Instrumented Function
SIL	Safety Integrity Level (overall)
aIL	Asset Integrity Level
eIL	Environmental Integrity Level
pIL	Production Integrity Level
sIL	Safety to life Integrity Level
SIS	Safety Instrumented System
SLD	Shutdown Logic Diagram
SSIV	SubSea Isolation Valve
TAR	Time At Risk.

For the purpose of this document only, the following **terms and definitions** apply:

Availability/ Unavailability	Probability that an item is able/ not able to perform a required function under stated conditions at a given instant t.
---	---

SIL assignment

Rev.: 01

Effective date: 05/2015

Page: 8 of 44

**Average Availability/
Unavailability**

Mean value of the **availability/ unavailability**: it may be interpreted as the proportion of the total time during which a component, equipment or system is performing/ not performing in the desired manner.

Note 1: Average availability / unavailability may be measured (estimated) in operation by the ratio of the observed up or down times over the duration of observation.

Note 2: the average unavailability is named "**PFD average**" in 61508-4 section 3.6.17 standard.

Demand rate (W)

Number of times per year (i.e. frequency) where the activation of a protection system working in demand mode is required.

**Emergency Shutdown
(ESD)**

Control actions undertaken to shutdown equipment or process in response to a hazardous situation.

**Emergency shutdown
system**

Safety Instrumented System (SIS) consisting of manual release stations and automatic devices which, when activated, initiate installation shutdown ([ISO 10418](#)).

Failure

Termination of the ability of a device or equipment item to perform a required function.

Final element

A device or combination of devices that manipulate a process variable or attract the attention of the operator to achieve risk reduction. The final element includes output cards or output relays, solenoid valves and cabling. Examples are valves, switchgear (rotating equipment stop circuits) and alarms.

**Fire and Gas (FGS)
system**

Safety Instrumented System (SIS) which monitors the temperature or the energy flux (fire), the concentration of flammable or toxic gases (gas), and initiates relevant actions (alarm, ESD, EDP active fire-fighting, electrical isolation, etc.) at pre-determined levels (Company).

Hazard

A chemical or physical condition with the potential of causing damage (Company).

**High Integrity
Protection System
(HIPS)**

Ultimate Safety Instrumented System (SIS) designed to protect a particular part of the installation against a possible particular operating condition (e.g. pressure, temperature, flow, level) exceeding the design parameters of that part of the installation. It does not duplicate the PSS or ESD system, but provides a preferably independent additional layer of protection, with a sufficient reliability and response time faster than possible occurrence of the excessive operating condition, so as to make the probability of exceeding the design parameters lower than the target value (refer to [GS EP SAF 260](#)).

**High Integrity Pressure
Protection System
(HIPPS)**

A HIPS exclusively devoted to protection against over-pressurization.

Alternative terminology: Over-Pressure Protection System (OPPS).

SIL assignment

Rev.: 01

Effective date: 05/2015

Page: 9 of 44

Integrity	Probability of a system satisfactorily performing the required function under all the stated conditions within a stated period of time (ISO 10418).
Incident	Any event or a chain of events which has caused any or all of the following consequences: • occupational injury or fatality ; • damage to the environment ; • material/ production loss.
Independent Protection Layer (IPL)	A protection layer is a device, system, or human action which is capable of preventing an initiating cause from propagating into an identified hazardous event. For a protection layer to be considered independent, its performance should not be affected by the occurrence of the initiating cause, its consequences, or by the failure of another protective function used to reduce the risk of the same hazardous event.
Installation	Technical unit in which dangerous substances are produced, used, handled or stored, including all the equipment, structures, pipework, machinery, tools, private railway sidings, docks, unloading quays serving the installation, jetties, warehouses or similar structures, floating or otherwise, necessary for the operation of the installation (GS EP SAF 021).
Mitigation	Reduction of the effects of a hazardous event.
Package	Prefabricated process or utility self-contained unit, generally able to operate on its own, supplied fully tested and ready for immediate installation, being supplied by a designated package Vendor (GS EP INS 120).
Permanent SIL	A SIL is permanent if the whole PFD(t) remains under the upper bound of the required SIL (Company).
Prevention	Means intended to reduce the likelihood of a hazardous event. (Company).
Probability of Failure on Demand (PFD(t))	Probability that a system or a component does not operate when it is activated. For dormant systems, the PFD(t) is actually the unavailability of the system.
Probability of Failure on Demand – Average - (PFD_{avg})	Average unavailability over a given period [0, T]. It is the mean of PFD(t) over this period. <u>Note:</u> PFD _{avg} is used to determine the SIL of safety instrumented systems working in low demand mode as per 61508-4 section 3.6.17
Process Control System (PCS)	System to control normally automatically the operation of a process station.
Process Safety System (PSS)	Safety Instrumented System (SIS) dedicated to shutdown to a safe state of particular units or equipment (e.g. SD3) (Company).

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 10 of 44

Reliability/ Unreliability	The probability that an item is able/ not able to perform a required function under stated conditions for a stated period of time or for a stated demand (IEC 61508-4).
Risk	Two-dimensional entity characterizing an unwanted event by its likelihood of occurrence and the extent of consequences arising from the occurrence of this event (Company).
Safety Instrumented Function (SIF)	Safety function with a specified Safety Integrity Level (SIL) which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function (IEC 61511-1 section 3.2.71). Only the SIF having the response time rapid enough to provide effective safeguarding may be considered (Company).
Safety Integrity Level (SIL)	Discrete level (one of the four) for specifying the safety integrity requirement of the Safety Instrumented Functions (SIF) to be allocated to the Safety Instrumented System (SIS). Safety Integrity Level 4 has the highest level of safety integrity; Safety Integrity Level 1 has the lowest (IEC 61511-1). SIL is a measure of risk reduction provided by a Safety Instrumented Function (SIF), based on four levels. Each level represents an order of magnitude of risk reduction. Every Safety Instrumented Function (SIF) has a SIL assigned to it, the Safety Instrumented System (SIS) and equipment themselves do not have a SIL assigned to it (IEC 61511-1).
Safety Instrumented System (SIS)	A Safety Instrumented System (SIS) is a system comprising of dedicated sensors, logic solvers and final control elements for the purposes of taking a process automatically to a safe state when normal predetermined set points are exceeded, or when safe operating conditions are violated. (IEC 61511-1 section 3.2.72) Multiple independent SIS normally exist at one installation (e.g. PSS, ESD, F&G, HIPS), forming together the “safety shutdown system”. Each SIS is entirely independent (logic and hardware) of the Process Control System (PCS) or from another SIS as to avoid any common cause failure, meaning separate sensors, logic solvers and final control elements.
Severity of an incident	A measure of the consequences of an incident (human injury and/or environment damage and/or material loss and/or asset damage) with five levels (Company).

4. Overall SIL Concept and Methodology

4.1 SIL Concept

The principle of using Safety Integrity Levels (SIL) as part of an overall risk reduction process has been established for many years based on [IEC 61508-4](#) section 3.5.8 and

SIL assignment

Rev.: 01

Effective date: 05/2015

Page: 11 of 44

IEC 61511-1 section 3.2.74 standards. The SIL measures the reduction of risk to be obtained by the prevention barriers implemented by the Safety Instrumented System (SIS).

SIL shall be considered only for instrument based safety barriers. The non-instrumented based barriers and safety/relief valves are not considered as part of the SIL application. Also control functions and any function using PCS as logic solver are not part of the SIL application.

According to IEC 61511-1, a safety related loop is an instrumented system used to implement one or more Safety Instrumented Functions (SIF). It is composed of any combination of sensor(s), links input / output cards, logic solver(s) and final element(s).

A safety related loop can include either safety instrumented preventive functions or safety instrumented protection functions or both.

IEC 61511-1 states that the SIL is one out of the four possible discrete levels for specifying the safety integrity requirements of the SIF(s) to be allocated to a safety-related loop. Criteria adopted by Company restrict the choice to the following set:

- Not SIL
- SIL1
- SIL2
- SIL3
- SIL4 (Not recommended).

Where the SIF is 'not SIL', it can be considered that the SIF has no special safety requirement. However it may be kept in the SIF list on a case by case basis.

Where "SIL4" is required, it shall be considered as an unrealistic target to maintain that performance during the whole life cycle of the installation, and the design shall be revisited accordingly. Solutions to escape from a SIL4 requirement are a change in process parameters or sizing, a change in material selection or pressure rating, installation of PSVs or dikes or sufficient capacities, or supplementary independent SIF or any other independent safety barrier.

As the studied systems are normally not active systems, they are considered as "low demand mode of operation", as shown in IEC 61511-1. Therefore, SIL calculations are based on Probability of Failure on Demand (PFD_{avg}) according to the following table:

Table 1: SIL definition vs PFD_{avg}

SIL	Low Demand Mode of Operation Average Probability of Failure on Demand (PFD_{avg})
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$

Rq: Probability of failure on demand of a system also means Probability of failure to perform its design function on demand.

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 12 of 44

IEC 61511-1 proposes that SIL are assigned based on safety to life criterion only. Company has elected to assign SIL based on four criteria. The overall SIL of a SIF shall therefore be determined from the highest integrity level of:

- **sIL** Safety to life Integrity Level;
- **eIL** Environmental Integrity Level;
- **aIL** Asset Integrity Level;
- **pIL** Production Integrity Level.

4.2 SIL Assessment Methodology

The process of assessing integrity levels is split into 2 main parts:

- **Assignment**

The SIL assignment shall include the determination of the required SIL target for a Safety Instrumented Function. The result shall be a defined SIL for each SIF.

- **Demonstration**

The SIL demonstration shall then evaluate the proposed loop design and confirm it achieves the required SIL target for the associated test frequency. The demonstration shall cover the full loop from sensor to final element.

Only the first part, i.e. assignment, is covered by this present document.

If the assignment concludes that a SIF requires a lower SIL target than has previously been designed, then the design may only be changed with formal Company written approval.

The SIL assignment and SIL demonstration shall be fully documented.

4.3 SIL Assignment Methodology

The SIL assignment for each SIF shall be determined by a workshop made up from a multi-disciplinary team. All SIF are subjected to SIL assignment. In addition, Company recommends that SIL assignment workshop follows the HAZOP, and takes advantage of HAZOP recommendations.

IEC 61511-1 provides a number of different methods to enable the determination of SIL, namely:

- Safety layer method (qualitative);
- Risk graph method (qualitative);
- Calibrated risk graph method (semi-qualitative);
- Event trees method (semi-quantitative);
- Layers of protection (LOPA) analysis (semi quantitative).

All of the methods presented in IEC 61511-1 have merits and drawbacks. Among these methods, the calibrated risk graph shall be used for SIL assignment workshops. Thus the calibrated risk graph is focused upon in this document, see chapter 7. The criteria for calibration are those of **GS EP SAF 041**.

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 13 of 44

Additionally, where SIL3 are assigned, a more quantitative analysis is required to ensure that the SIL assignment is accurate. The Layer Of Protection Analysis (LOPA) shall be the method for the detailed analysis of SIL3 or any SIL targets difficult to implement or maintain. Thus the LOPA method is described in this document, see chapter 8.

5. Schedule of SIL Assignment

5.1 Pre-requisites/ Preparation works to SIL Assignment Workshop

The pre-requisites for the SIL assignment workshop are:

- P&IDs and Shutdown Logic Diagrams (SLD) issued and reviewed at least once;
- HAZOP completed;
- Manning distribution defined and validated by Operations;
- SIF table issued and reviewed by instrumentation (see chapter 6 and appendix 1 for information);
- Assumptions Register/ Rule Set validated (see appendix 2 for information);
- Calibrated Risk-Graph (see chapter 7 and annexes 3 and 4 for information);
- Workshop and venue prepared (see appendix 5).

The amount of preparation work required prior to entering a team-based SIL assignment workshop is often under-estimated. A lack of preparation time will result in insufficient information to complete the review, misaligned expectations, and thus extra time for the workshop and the requirement to address a multitude of clarifications and actions.

The following aspects are recommended prior to undertaking the SIL assignment workshop:

- The SIL assignment workshop should include part of the HAZOP team; however it is not recommended to carry-out HAZOP and SIL assignment at same time since the preparation level and objectives are different;
- It shall be checked in advance that the SIF table is part of the deliverables of the basic engineering / FEED contractor; if not, a third party e.g. HAZOP or SIL Consultant shall be designated in advance to prepare this essential document;
- A kick-off-meeting / discussion shall be held prior the commencement of SIL assignment workshop to align understandings, expectations and detailed procedures.

A very minimum duration required for the above activities is two weeks.

5.2 SIL Assignment

The SIL assignment workshop shall take place before the end of the basic engineering or FEED.

The SIL assignment for each SIF shall be determined by a workshop made up from a multi-disciplinary team. See appendix 5 for guidance how to conduct a SIL assignment workshop.

The SIL assignment report shall be approved by Company and the actions arising from the workshop shall be tracked till resolution.

General Specification		GS EP SAF 361
SIL assignment		
Rev.: 01	Effective date: 05/2015	Page: 14 of 44

In case of design modifications, the SIL assignment workshop shall be reworded after re-HAZOP.

5.3 Next steps

A preliminary SIL demonstration shall be made before the end of basic engineering in order to validate the architecture of the SIS and the configuration of the SIFs. At such time, equipment is not purchased yet and the preliminary SIL demonstration is based on generic reliability data.

SIL demonstration shall be reworked when the actual and guaranteed reliability data of the purchased equipment are available.

SIL demonstration and final SIL assessment shall be completed during detailed engineering.

SIL demonstration shall be the responsibility of EPC Contractor and shall be performed by Company approved Third Party.

Final SIL assessment shall be performed or validated by Company.

6. Identification of SIF

The Shutdown Logic Diagrams (SLD) are a basis for the SIL assignment workshop, with each safety function input being taken in turn. All safety functions shall therefore be examined. The first step in the SIL Assignment is the correct identification of the SIF.

A table identifying and describing all SIFs shall be prepared prior to the SIL assignment workshop.

An example of SIF table is provided in appendix 1, table 1.1 for information.

The SIF's intent is to prevent the hazardous situation to become a hazardous event.

A SIF consists of one or more initiators, the logic solver and the final elements. Only the SIF having the response time rapid enough to provide effective safeguarding may be considered

The initiators are all the sensors that detect one or more initiating events or the hazardous situation.

The final elements are all the devices that are required to bring the process to a safe state to avert the hazardous event. Final elements can be valves including their actuators and solenoids, circuit breakers, dampers, etc. The final element(s) of the SIF are chosen as those which directly meet its design intent. Thus, only one or two final elements are usually defined for any SIF.

In case of multiple sensors or final elements, it is necessary to define the "success criteria". Success criteria are defined as the number of initiators or final elements (N) working properly out of the total number of initiators or final elements (M) for successfully averting the hazardous event (i.e. NooM).

For a complete description of the SIF, the SIF table includes the description of the logic solver e.g. PSS or ESD, and the description of the input and transmission links e.g. hardwire, databus, radio link and the I/O cards e.g. dedicated or merged with others. This information is necessary to validate the independence of the SIF and Independent Protection Layers (IPLs).

For large installations it is useful to break down the SIF table by fire zones/ ESD1.