



Safety Integrity Level (SIL) Studies

Procedure

Document No.: 0000-AH-PRC-70002
Security Classification: Unrestricted

Revision	Date	Issue Reason	Prepared	Checked	Endorsed	Approved
4	03/04/2025	For Use	M Macoboy	-	B Oranje	S Coull
5	19/06/2025	For Use	M Macoboy	-	B Oranje	S Coull
6	20/01/2026	For Use	M Macoboy		B Oranje X Bi	S Coull

RECORD OF AMENDMENT

Revision	Section	Amendment
A	All	N/A – First Revision
0	Various	Updates as per Rev A Review comments
1	6.2	Revised requirements for mechanical devices which inherently protect against hazardous scenarios.
1	6.4	Re-instated omitted requirement that prohibits SIL 4 SIFs and require TA-1 acceptance of SIL 3 SIFs.
1	App C	Use of different occupancy levels than those specified if approved by the Technical Safety TA-1.
1	App D - Table 6	Updated SRD Check Valve PFD to include 20 yr interval
1	App D - Table 6	Added the minimum PFD to be assigned for permanent stops and adjustable movement limiting devices.
2	App B/D	Updated credit for human errors where a locked valve or interlock or spec blind arrangement are employed
2	App B	Added Initiating Event frequencies for high demand check valves
2	App B	Added clarification note where multiple BPCS loop failures lead to same Initiating Event
2	6.2	Revised text for LOPA exclusions
3	4, 6.1, 6.4.e & App B	Updated sections for requirement for review of historic SIF demand incidents
4	6.2	Removed requirement for LOPA where SIF or Critical Alarm provided but Consequence level does justify
4	7	Updated guidance about criteria for closing recommendations
5	App D	Added IPL for opening and closing restrictions on actuated valves
6	App H	Added Appendix H for guidance on LOPA recommendations for facilities in Operational Phase

DOCUMENT DISTRIBUTION

	Name
00	Document Control
01	Steve Coull
02	Xiongfei Bi
03	Bob Oranje
04	Rodney Gornall
05	Virgilio Bonardi
06	Lee Cunningham
07	Greg Slater
08	Tim Aldridge
09	Chris Blackburn
10	Andy Rigg
11	Amanda Smith
12	Michael Wegg
13	Matthew Brooks
14	Vaughan Bregger
15	Nathan Hogan

NOTICE

All information contained within this document has been classified by INPEX as **Unrestricted** and must only be used in accordance with that classification. Any use contrary to this document's classification may expose the recipient and subsequent user(s) to legal action. If you are unsure of restrictions on use imposed by the classification of this document you must refer to 0000-A9-STD-60008, Sensitive Information Protection Standard or seek clarification from INPEX.

Uncontrolled when printed.

TABLE OF CONTENTS

1	INTRODUCTION	6
1.1	Purpose	6
1.2	Scope.....	6
1.3	Exclusions.....	6
1.4	Background.....	8
1.5	Abbreviations and Definitions	9
2	REGULATIONS AND STANDARDS	11
2.1	INPEX Documents	11
2.2	Regulatory Framework	11
2.3	Standards	12
2.4	Other References	12
3	SIL ASSESSMENT MANAGEMENT	13
3.1	General	13
3.2	SIL Assessment: LOPA v Fault Tree Analysis	15
4	LOPA TERMS OF REFERENCE	16
5	LOPA RESPONSIBILITIES	17
5.1	LOPA Sponsor	17
5.2	LOPA Coordinator	17
5.3	LOPA Facilitator	17
5.4	LOPA Scribe	18
5.5	LOPA Workshop Team	18
6	LOPA METHODOLOGY.....	20
6.1	Readiness/Documentation.....	20
6.2	Scenario Selection	20
6.3	LOPA Specific Requirements.....	21
6.4	LOPA Sequence of activities/steps.....	21
6.5	Recording the LOPA Minutes.....	24
6.6	LOPA Recommendations	25
6.7	LOPA Reporting	25
7	LOPA RECOMMENDATION CLOSEOUT	27
8	SIL ASSESSMENT AUDIT	30

LIST OF TABLES

Table 1 - Safety & Environmental TMELs.....	31
Table 2 - Financial TMELs	31
Table 3 - Initiating Event Frequencies	32
Table 4 - Human Error Rates.....	34
Table 5 - Generic Ignition Probabilities	37
Table 6 - Equipment Probability of Failure on Demand	38

Table 7: SIL vs PFD	43
Table 8: SIL vs Frequency of Failure	43

LIST OF FIGURES

Figure 1 - Risk Reduction and SIL	8
Figure 2 - Functional Safety Lifecycle Flowchart.....	14
Figure 3 - LOPA Flowchart	22

TABLE OF APPENDICES

APPENDIX A: TARGET MITIGATED EVENT LIKELIHOODS	31
APPENDIX B: INITIATING EVENT FREQUENCIES.....	32
APPENDIX C: ENABLING EVENTS / CONDITIONAL MODIFIERS	35
APPENDIX D: IPL PROBABILITY OF FAILURE ON DEMAND.....	38
APPENDIX E: SIL DEFINITIONS.....	43
APPENDIX F: HIGH DEMAND MODE	44
APPENDIX G: AUDIT CHECKLIST/QUESTIONS	45
APPENDIX H: OPERATIONAL PHASE RECOMMENDATIONS ADDITIONAL GUIDANCE ..	48

1 INTRODUCTION

1.1 Purpose

This Procedure sets out the requirements for conducting Safety Integrity Level (SIL) assessments. These are typically workshop-based sessions in which the Risk Reduction Factor (RRF), or SIL rating, of one or more Safety Instrumented Functions (SIFs) are determined.

The SIL assessment methodology applied in this Procedure is consistent with the requirements of the Functional Safety Standards (see section 2.3).

The methodology in this procedure can inherently be utilised as a means of determining acceptability of existing/proposed safeguards employed for process safety hazards whether or not there is a Safety Instrumented Function (SIF) included as a safeguard.

1.2 Scope

This Procedure applies to all SIL assessments on any equipment on any of the facilities (onshore and offshore) operated by INPEX. This procedure shall be applied directly by INPEX or by Contractors involved in the design of process systems, and is primarily focused on Layers of Protection Analysis (LOPA) as the means of performing a SIL assessment.

SIL assessments are essentially risk assessments and shall be performed:

- Whenever a SIF (see definition in section 1.5) is included in the design; or
- Whenever a determination of a process safety risk is required to confirm appropriate safeguards are in place, or to assign a safeguard (a SIF or other protection layer) should a risk gap be identified.

This Procedure should not be used for general risk assessments that are unrelated to process safeguarding systems.

This Procedure does not address the content of the Safety Requirements Specification (SRS) nor the methodology for quantification of random hardware failures (i.e. the SIL calculations) – see section 3.1.

Any deviation from this Procedure requires approval from INPEX Technical Safety TA-1.

1.3 Exclusions

1.3.1 Hazard Scenarios

Hazard scenarios that are not expected to be taken forward to SIL Assessment are identified in section 6.2.

1.3.2 SIL 4

This procedure does not address equipment assessed as SIL 4. Any assessment that results in a SIL > 3 shall be revisited to reduce the hazard and/or provide more independent layers of protection. SIL 4 shall not be assigned to any SIF.

1.3.3 Mitigation Systems

Mitigative systems are not to be accounted for in SIL assessments, as the emphasis is required to be on prevention not mitigation. Typically a mitigative function is expected to achieve a layer of protection in preventing the overall hazard consequence but allowance for mitigative protections is accounted in the TMELs and ALARP demonstration. Refer to "Generic SIL Requirements For Mitigative Controls" (X075-AH-REP-10010) for the INPEX targets for mitigative systems.

It is not considered practical to conduct a SIL assessment for mitigative systems such as Fire & Gas (F&G) Systems, Emergency Shut Down (ESD) systems, Public Address General Alarm (PAGA) systems etc.

This is primarily due to the difficulties in quantifying the escalation impact over and above the initial event that requires a mitigation system to function. For example, if a flammable gas release has ignited and the F&G system detects the fire and isolates the inventory etc, it can be difficult to determine the additional safety, environmental and financial impacts if the F&G system does not function as intended.

An additional complication is if the mitigative system is manually activated in response to an event. In these instances, assigning a probability of failure on demand (PFD) to the human being (as part of the sensor sub-system) is problematic as the situation is inherently stressful and novel which implies a high PFD.

It is therefore recommended that mitigative systems be installed, maintained and tested in line with good industry practice and regulatory requirements. SIL assessment should not be used to determine a test interval for a mitigative function.

1.3.4 Quantification of Random Failure

This procedure does not address the quantification of random failure of SIFs. For details and requirements for quantifying the random failure of a SIF, refer to Safety System Performance Analysis Specification (X810-AJ-SPC-70004).

In summary, the design of each SIF needs to be verified to confirm that it meets the requirements documented in the relevant SIL assessment report.

The calculations are required to confirm for each SIF that:

- The required PFD is achieved for a SIF in Demand Mode; or
- The required Dangerous Undetected Failure Frequency is achieved for a SIF in High Demand Mode.

The variables that can be adjusted to achieve the above are:

- The Dangerous Undetected Failure Frequency of the sub-system equipment (i.e. select sub-system equipment with better dangerous undetected failure rate);
- The function test interval (except for a 1oo1 voted device in high demand mode as test interval is not relevant);
- The voting architecture of the sub-system equipment (i.e. introduce redundancy into the sub-system equipment)

The following shall be finalised for the SIF design by nature of the calculation output:

- The make/model of the SIF sub-system equipment.
- The test interval for each SIF sub-system equipment;
- The number of SIF sub-system devices and their voted architecture.

1.4 Background

The risks associated with operating process systems shall be managed by providing a range of controls that act to prevent a hazardous event from occurring and to mitigate its potential consequences should it occur. Implementation of these controls is required to reduce residual risks associated with the equipment to levels that are As Low As Reasonably Practicable (ALARP). The concept of risk reduction and safety integrity is illustrated in Figure 1 below.

To ensure that risks are appropriately managed, a systematic approach is required to:

- Identify hazards associated with operating process equipment;
- Evaluate the risks based on existing process system safeguards;
- Compare evaluated risks with target risk criteria;
- Determine the additional risk reduction required to meet target risk criteria;
- Implement additional controls to ensure that target risk criteria is met; and
- Assess the risk to confirm the risk is As Low As Reasonably Practicable (ALARP).

The SIL assessment for a SIF is one of the initial steps in the overall management of the Functional Safety lifecycle as described in AS IEC 61511. See section 3 for the overall Functional Safety Lifecycle.

The SIL assessment for each SIF provides an input to the facility's Safety Requirement Specification (SRS). The SRS documents the IPLs required to achieve the tolerable risk target.

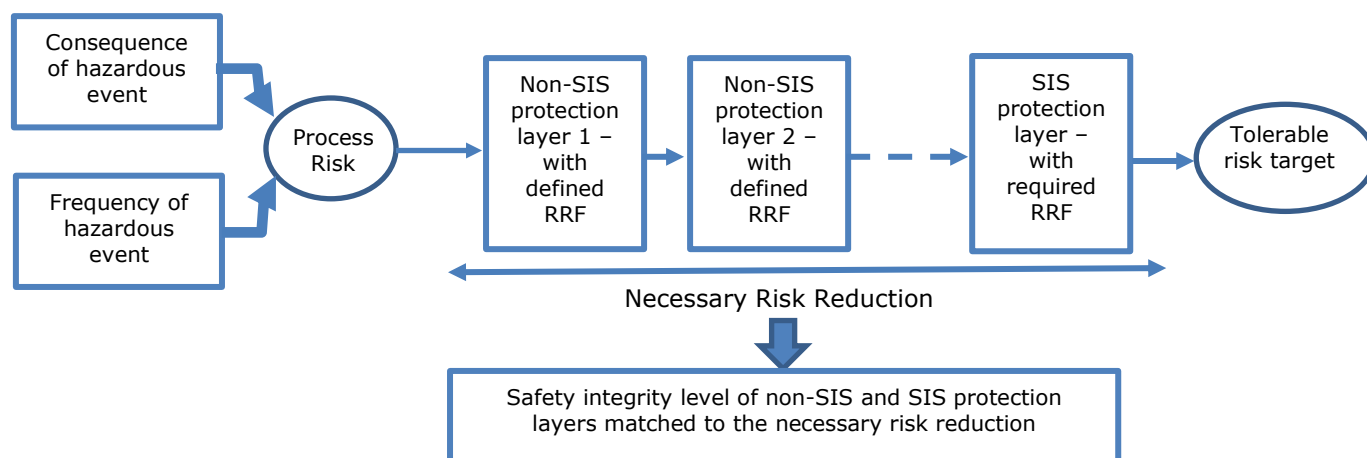


Figure 1 - Risk Reduction and SIL

1.5 Abbreviations and Definitions

	Description
Action	Performed after the SIL/LOPA workshop in response to a SIL/LOPA Recommendation.
ALARP	As Low As Reasonably Practicable.
BPCS	Basic Process Control System (AS IEC 61511 term for the equipment under control including operator interaction).
Compliance	Ensuring that the requirements of safety and environmental laws, regulations, industry codes and organisational standards are met.
Demand Mode	Where the specified SIF action (for example, closing a valve) is taken in response to process conditions or other demand occurring at a frequency less than once per year, then the SIF is operating in "Demand Mode". See also Note 1.
ESD	Emergency Shut Down
FEED	Front End Engineering Design.
F&G	Fire and Gas
FTA	Fault Tree Analysis
FSMP	Functional Safety Management Plan
HAZOP	Hazard and Operability (Study)
High Demand Mode	Where the specified SIF action (for example, closing a valve) is taken in response to process conditions or other demand occurring at a frequency more than once per year. See also Note 2.
IEC	International Electrotechnical Commission.
IPL	Independent Protection Layer – a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario.
LOPA	Layers Of Protection Analysis.
NPV	Net Present Value.
PAGA	Public Address General Alarm
P&ID	Piping & Instrumentation Diagram.
PCHE	Printed Circuit Heat Exchanger
PFD	Probability of Failure on Demand.
PL	Protection Layer
PST	Process Safety Time
RBI	Risk Based Inspection

	Description
Recommendation	Made during the SIL/LOPA workshop, recommendations are generated for further investigation/review/activity etc after the SIL/LOPA workshop.
RRF	Risk Reduction Factor.
SIF	Safety Instrumented Function, which is an action implemented by means of instruments that is intended to achieve or maintain a safe state for the process system in respect of a specific hazardous event. See also Note 3.
SIL	A Safety Integrity Level is a rating from 1 to 4 which indicated the acceptable failure rate of the SIF. This determines the design requirements of the SIF.
SIS	Safety Instrumented System.
SRD	Safety Related Device
SRS	Safety Requirements Specification
TA-1	Technical Authority Level 1.
TA-2	Technical Authority Level 2.
TMEL	The Target Mitigated Event Likelihood (TMEL) defines the hazardous event tolerable frequency based on the event consequences.
ToR	Terms of Reference.
TSO	Tight Shut-Off

Notes :

1. This is the normal 'mode' for a SIF in a process application, as usually there is a BPCS providing satisfactory continuous control to prevent demands on the SIF.
2. High Demand Mode and Continuous mode are treated as the same in this Procedure. See APPENDIX F: for further explanation.
3. A SIF loop consists of one or more sensors (including all components from the process connection to the associated logic solver input card), the logic solvers and one or more final elements (including all components from the SIS output card to the actuated device) and utilities such as power and instrument air supplies required to perform the SIF.

The sensors of a SIF are the initiators that are required to detect the cause of a potentially hazardous event. This may be a single sensor or multiple sensor architecture measuring the same parameter, or in some cases, multiple sensors that measure different parameters that together give an indication of a potentially hazardous event.

One or more of the individual sensors in a particular function may also be part of another SIF.

2 REGULATIONS AND STANDARDS

2.1 INPEX Documents

This Procedure shall be read in conjunction with the following INPEX documents:

- Health and Safety Policy (0000-AH-POL-60001)
- HSE Hazard and Risk Management Standard (0000-AH-STD-60003)
- Functional Safety Management of Safety Instrumented Systems (0000-AH-STD-60008)
- Assurance Standard (0000-A00-STD-60031)
- Risk Matrix (0000-A0-TPL-60003)
- Hazard and Operability Studies Procedure (0000-AH-PRC-70001)
- ALARP Demonstration Guideline (0000-AH-GLN-60021)
- Register of Approved HAZOP / SIL Study Leaders (0000-AH-LIS-60001)
- Safety System SIL Performance Analysis Specification (X810-AJ-SPC-70004)
- Machinery Protection Systems (X091-AM-SPC-70001)
- Generic SIL Requirements For Mitigative Controls (X075-AH-REP-10010)
- Actuated Valve Maintenance Strategy (X060-A1-STR-60094)
- LOPA Gaps Identified in Operate Phase Decision Note (X060-A1-DCN-70010)
- Prioritisation Matrix (X060-A0-DAT-60001)

2.2 Regulatory Framework

This Procedure forms part of INPEX compliance with the following regulations:

- Federal Legislation and Regulations:
 - Offshore Petroleum and Greenhouse Gas Storage Act 2006 – Schedule 3; and
 - Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009.
- Western Australia Legislation and Regulations:
 - Occupational Health and Safety Act 1984;
 - Occupational Health and Safety Regulations 1996;
 - Petroleum (Submerged Lands) Act 1982 – Schedule 5; and
 - Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 2007.
- Northern Territory Legislation and Regulations:
 - Northern Territory Work Health and Safety (National Uniform Legislation) Act 2011;
 - Northern Territory Work Health and Safety (National Unified Legislation) Regulations 2011;
 - Petroleum (Submerged Lands) Act 1982 – Schedule 4; and
 - Petroleum (Submerged Lands) (Application of Commonwealth Laws) Regulations 2004

- Energy Pipelines Act 1981
- Energy Pipelines Regulations 2001

2.3 Standards

- AS 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems.
- AS IEC 61511, Functional Safety – Safety Instrumented Systems for the Process Industry Sector.

2.4 Other References

- DNV OREDA Offshore Reliability Data Handbook
- American Institute of Chemical Engineers (AIChE) CCPS Concept Book, Layer of Protection Analysis, Simplified Process Risk Assessment, Centre for Chemical Process Safety 2001.
- Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2013 Edition, SINTEF, ISBN 978-82-536-1334-5
- Reliability Prediction Method for Safety Instrumented Systems, PDS Method Handbook, 2013 Edition, SINTEF, ISBN 978-82-536-1333-8.
- Safety Equipment Reliability Handbook, exida.
- Reliability, Maintainability and Risk, David J Smith.
- Energy Institute Guidelines for the Safe Design and Operation of Shell and Tube Heat Exchangers to Withstand the Impact of Tube Failure, 2nd Ed, Nov 2015.
- American Institute of Chemical Engineers (AIChE) CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis, 2015 Edition, Appendix D.

3 SIL ASSESSMENT MANAGEMENT

3.1 General

SIL Assessment is one part of the overall Functional Safety Management. By reference to Figure 2 below, SIL assessment is Phase 2 of the AS IEC 61511 Safety Lifecycle.

SIL Assessments shall be planned and conducted at the appropriate time in the project or facility lifecycle. They shall be carried out for all new process system designs or significant modifications of existing process designs, including vendor packages.

The precursor to SIL Assessment is a hazard study (refer to Figure 2, Phase 1) which would normally be a hazard and operability (HAZOP) study or other hazard identification process.

A hazard study for a new scope/project will be conducted during FEED and a SIL assessment shall be conducted after that hazard study to determine expected SILs of any identified SIFs and/or reduce the risks via inherently safe design principals.

The FEED hazard study for a new scope/project shall be revisited in the detailed design phase. The detailed design HAZOP on a project is the final and the most important HAZOP before a facility enters the Operational phase. It has regulatory implications, it must be rigorously completed and account for the full design. Similarly and subsequently the SIL Assessment performed during detailed design is essential for demonstrating adequate process safeguarding is in place at start up.

SIL Assessments shall be scheduled to occur within 1 month of the relevant hazard study. A delay in timing will only be accepted if the hazard study identifies major issues which must be corrected before a valid SIL Assessment can be completed. With appropriate preparation it is acceptable to have the SIL Assessment follow directly after the relevant hazard study.

During Phase 6 (the operational phase) of the Safety Lifecycle a SIL Assessment may be initiated due to:

- Periodic "Revalidation" of a HAZOP (refer HAZOP Procedure 0000-AH-PRC-70001) affecting one or more Independent Protection Layers (IPLs); or
- A HAZOP, or other hazard identification methodology, being conducted in between "Revalidations" with new or modified hazards documented; or
- A change to one or more IPLs, including any conditional modifiers, used in a SIL Assessment; or
- A change in a SIF's demand rate as experienced during operations.

The SIL Assessment output shall be documented in the SIL Assessment report (see section 6.7 for the requirements for a LOPA report). It is used as an input into the Safety Requirements Specification (SRS), and subsequently the required SIL is to be confirmed via calculation (see section 1.3.4). The SRS and the SIL calculations are Phase 3 and Phase 4 (respectively) of the AS IEC 61511 Safety Lifecycle and are not discussed further in this Procedure, however it shall be recognised that a change to a SIL assessment will have an impact to the rest of the safety lifecycle documentation including the SRS and the SIL calculations.

A SIL Assessment shall not be used, on its own, as a justification to permanently deviate from normal industry practice nor used to remove existing safeguards. Refer to the ALARP guideline referenced in section 2.1.

The INPEX Functional Safety Management Plans (FSMPs) shall contain the overall requirements for the management of the Functional Safety Lifecycle.

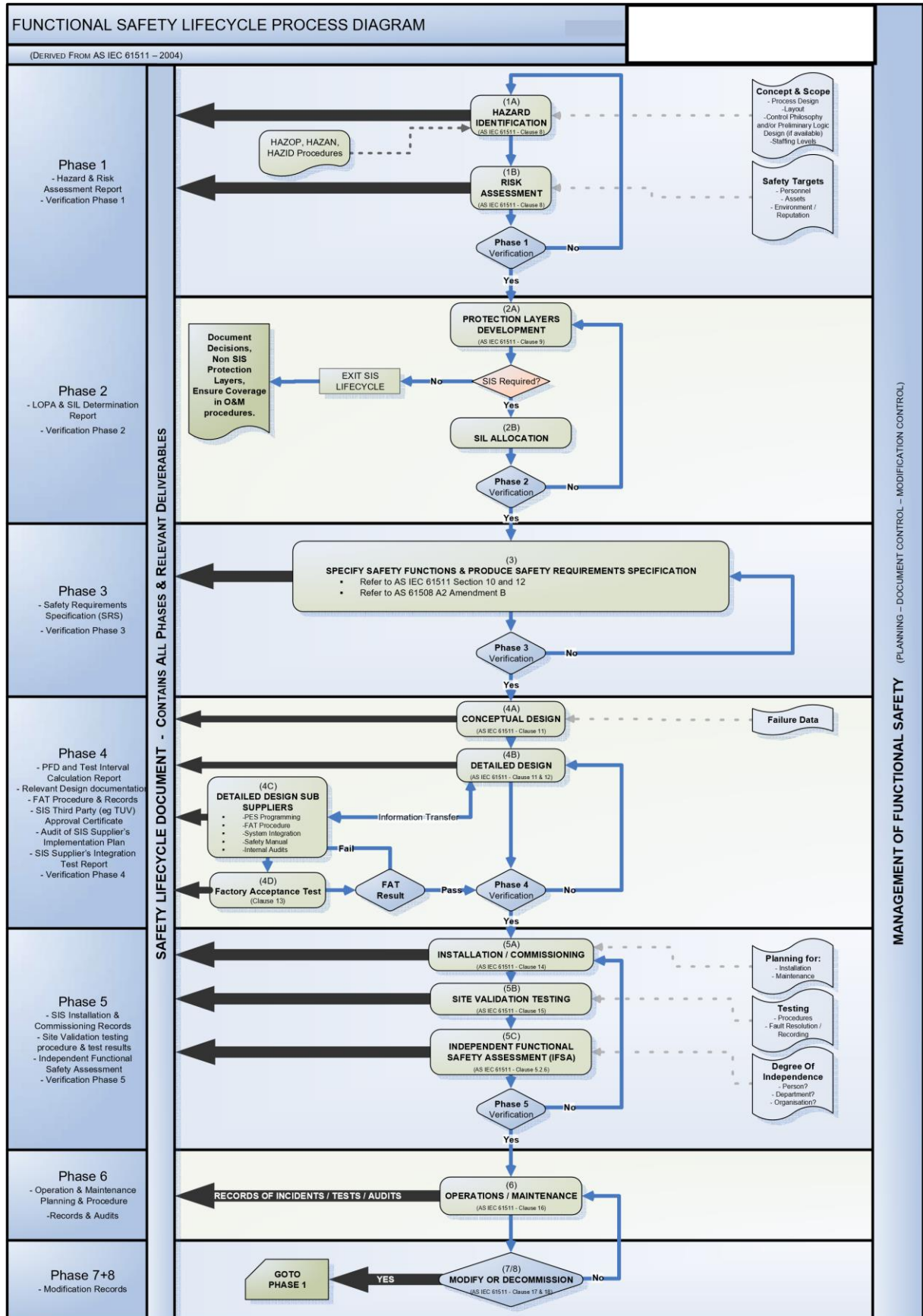


Figure 2 - Functional Safety Lifecycle Flowchart

3.2 **SIL Assessment: LOPA v Fault Tree Analysis**

The preferred approach to SIL Assessment is the use of LOPA and the rest of this procedure is primarily focused on LOPA. However, LOPA may not be a valid approach in the following situations:

- The hazard scenario is considered to be too complicated to be analysed via LOPA; or
- There is significant commonality between IPLs such that LOPA is likely to be overly conservative; or
- There are multiple causes leading to the same consequence that require more accurate summation; or
- A more accurate and/or quantitative analysis is needed to better analyse and/or determine where the main contributors are, or where additional improvements need to be applied.

In these instances the LOPA will be superseded by the more rigorous analysis. The Technical Safety TA-1/2 should be consulted to advise and determine an appropriate approach (e.g. use of Fault Tree Analysis (FTA)).

4 LOPA TERMS OF REFERENCE

Where a LOPA workshop is used (in whole or in part) for SIL Assessment, a formal Terms of Reference (ToR) shall be developed, approved and distributed (unless agreed otherwise by the Technical Safety TA-1). As a minimum the ToR shall include:

- Objectives;
- Scope;
- Methodology (i.e. as per this Procedure);
- Review of historic SIF demand incidents (refer to Section 6.1);
- Any specific assumptions, TA-1 agreed rule sets or deviations to this procedure, and/or clarifications;
- Attendees;
- References to information such as :
 - This Procedure
 - Relevant hazard information
 - P&IDs
 - Cause and Effect diagrams
 - Any specific consequence information (such as Financial impact rules of thumb / guidance) where the hazard scenario and consequences need to be developed as part of the LOPA
- Deliverables;
- Action tracking and close-out requirements; and
- Administrative information (timing, duration, location, etc.).

The ToR shall be:

- reviewed/agreed by the LOPA Facilitator;
- reviewed by the INPEX Technical Safety and Process TA-1s (or delegates) including endorsement of the engineering participants;
- approved by the LOPA sponsor prior to distribution.

For a major LOPA (ie FEED, detailed design & revalidation) the ToR shall be distributed to the HAZOP team a minimum of 2 weeks in advance of the workshop start date. For an operational phase LOPA this may not be feasible, however a ToR must be agreed prior to commencement of a workshop.

The ToR may be combined with the HAZOP ToR to form a comprehensive ToR dealing with these steps in the IEC 61511 lifecycle.

5 LOPA RESPONSIBILITIES

The following roles and responsibilities are applicable where a LOPA is used for SIL Assessments at design or operational phases.

5.1 LOPA Sponsor

Each LOPA shall have a clearly identified Sponsor. The Sponsor shall understand the importance of the SIL Assessment generally, and shall:

- Identify the individual responsible for completion of the LOPA Co-ordinator role.
- Approve the LOPA Terms of Reference (ToR) and ensure it complies with the minimum requirements of this Procedure, and approve the LOPA report;
- Ensure appropriately qualified and competent resources are assigned to complete the LOPA;
- Assign resources to address the recommendations that arise out of the LOPA and implement outcomes in the design as necessary;
- Ensure an INPEX approved action tracking system is in place that meets the requirements of this standard;
- Ensure that all LOPA recommendations are appropriately closed out prior to operation, or in an agreed timeframe; and
- Report LOPA and LOPA close-out progress
- Approve the LOPA and LOPA close-out reports.

5.2 LOPA Coordinator

The LOPA Coordinator shall be a delegate of the LOPA Sponsor and shall be familiar with the requirements for SIL assessment at the relevant stage in a project or lifecycle of the facilities. The Co-ordinator shall:

- Prepare the LOPA Terms of Reference (ToR);
- Ensure appropriate arrangements are in place to allow the LOPA to take place efficiently;
- Ensure necessary documentation is ready and available during the LOPA;
- Ensure the LOPA is accurately recorded and suitably reported;
- Ensure that recommendations are transferred to the INPEX approved action tracking system;
- Report LOPA progress to the Sponsor on a regular basis, including quality issues, feedback on/from attendees and key findings; and
- Stop the LOPA, all or in part, if the required information is not available or the team dynamic/participation is unacceptable.

5.3 LOPA Facilitator

Each LOPA workshop shall have a Facilitator. To provide adequate independence, the Facilitator shall not be a member of the design team nor have operational responsibility for the subject of the LOPA. The Facilitator shall:

- Be approved by INPEX per 'Register of Approved HAZOP / SIL Study Leaders' (0000-AH-LIS-60001) or Technical Safety TA-1;

- Review and agree with the ToR;
- Advise the LOPA Sponsor / Coordinator on the team make-up and competency to ensure an effective review is carried out;
- Identify, based on the hazard study and associated records, of all process hazards and SIFs to be subject to LOPA;
- Conduct appropriate facilitation of the LOPA workshop including maintaining team motivation / focus and session time management;
- Explain the LOPA methodology concepts to the Team as/if required at the start of the workshop;
- Ensure that the LOPA methodology is adhered to including;
 - Ensuring appropriate SILs are assigned to the SIFs;
 - Guiding selection of initiating event frequencies and IPL PFDs.
- Ensure the accuracy of LOPA workshop records and associated documentation; and
- Prepare the LOPA report.

Ideally the Facilitator of the relevant hazard study should also be the LOPA Facilitator.

5.4 LOPA Scribe

LOPA studies conducted via a workshop shall be recorded by a Scribe. The Scribe shall:

- Accurately prepare the meeting records (minutes).
- Assist the Facilitator during the LOPA sessions.
- Be familiar with the LOPA methodology.
- Be experienced in minute taking with suitable technical knowledge relevant to the scope.
- Be experienced in the software used to record the LOPA.

The Scribe would also normally be expected to produce, or be involved with, the production of the LOPA report under the guidance of the Facilitator.

5.5 LOPA Workshop Team

A LOPA workshop shall be attended by an experienced multidisciplinary team. The LOPA Team shall be responsible for participation in, and completion of the LOPA under the direction of the LOPA Facilitator, and shall consist of a minimum of four people.

The core disciplines to attend an INPEX LOPA are:

- Process Engineer;
- Instrumentation & Control Engineer;
- Technical Safety Engineer; and
- Operations representative.

Team members shall be selected based on the scope and complexity of the LOPA. The LOPA Sponsor shall ensure that the LOPA Team has sufficient knowledge to undertake the LOPA and determine the required team members and additional specialist expertise. The relevant Team members will need to:

- Understand and describe the process system and relevant hazard(s);

- Understand and describe the process control and safeguarding systems in place; and
- Describe the functionality of each SIF.

Part-time attendance for specialists relevant to specific areas of the plant design or vendor equipment shall be planned for in advance and scheduled accordingly. Part time attendees may include:

- Mechanical engineers (rotating, static, thermal equipment);
- Equipment package engineers;
- Electrical engineers;
- Drilling / Reservoir / production engineering representation;
- Flow assurance specialists;
- Subsea engineers;
- Environmental engineers;
- Vendor technical representatives;
- Production chemists;
- Metallurgists; and
- Additional Operations maintenance representation.

6 LOPA METHODOLOGY

LOPA is a relatively simplistic method of determining a risk gap and SIL required of a SIF that adopts a semi-quantitative approach using 'orders of magnitude' Risk Reduction Factors (RRFs). Consequently, it is a relatively quick and efficient means of SIL assessment albeit may result in a conservative SIL value. A LOPA should normally be performed as a workshop exercise (with the LOPA workshop adequately resourced and planned i.e. included in the project schedule). In some circumstances (to be agreed with Technical Safety TA-1) it may be appropriate to do the LOPA as a desktop exercise or as a hybrid desktop/workshop exercise. Refer also to section 5.1 and 5.2 above.

6.1 Readiness/Documentation

A LOPA shall be performed as per SIL Assessment requirements stated in section 3.1.

It is extremely important that the subject of the LOPA is suitably mature/developed and ready for LOPA examination and may require one or more HAZOP recommendations to be closed out where the close out affects the understanding of, or the IPLs assigned in, the LOPA.

Experience has shown that if the design is not mature, or if the hazard scenario is not sufficiently well understood, then the LOPA duration will extend, and/or more recommendations get raised. There is also the distinct possibility that the LOPA will need to be redone in whole or in part.

A review of historic SIF demands applicable to the scope of LOPA is required. This ensures the initiating event frequency is accurate and "high demand mode" for a SIF is applied in ExSILentia where appropriate. See APPENDIX F.

6.2 Scenario Selection

The process system HAZOP is expected to be the primary source of hazard identification for the process facility with the relevant hazards and associated safeguards extracted from the HAZOP record for LOPA.

Regardless of the hazard study source, hazard scenarios shall be selected for LOPA where either of the following apply (unless covered by exclusion items below):

- The safety or environmental consequence ranking is "C" or greater; or
- The financial consequence is B or greater (noting also that financial consequences may not always be included in the LOPA – this shall be determined during preparation of the ToR).

The following hazard scenarios are not expected to be taken forward to LOPA:

- Where a consequence can result in a reputation, cultural and social heritage or legal impact only;
- Personnel initiated hazards where the primary safeguard is the Integrated Safe System of Work (ISSOW). Note prepare for maintenance or return from maintenance activities, which may be executed in line with procedure, are not typically ISSOW related LOPA exclusions;
- Personnel initiated hazards where the only safeguard is operator competence, procedure or similar, and an industry best practice configuration is employed, where conducting a LOPA adds no benefit. For example, loss of containment caused by operator removing a blind flange and opening a vent / drain valve during maintenance activities without ensuring appropriate boundary isolation, or

inadvertently leaving opening a vent / drain valve and failing to replace the blind flange after maintenance;

- Time based hazards that align with a chronic (i.e. long term) failure mechanism such as corrosion/erosion (where Risk Based Inspection (RBI) or other monitoring safeguards are typically employed for such scenarios);
- Blocked in piping thermal overpressure due to ambient conditions where the safeguard is a correctly sized/selected thermal relief valve; and
- Where there is a permanent feature of the design which inherently protects against the hazardous scenario of concern that cannot be adjusted or modified without replacing equipment. Examples of such devices include restriction orifices and pump impellers sized to prevent scenarios. This does not include valves equipped with a permanent mechanical stop, these shall be assigned a minimum probability of failure on demand, this shall be increased if there are inherent weakness in how the mechanical stop is implemented and ease of adjustment. Minimum PFDs are defined in Appendix D.

Where a LOPA is initiated separate from a distinct hazard study, the hazardous scenario and consequence is still required to be documented (perhaps as part of the LOPA). Estimation of the consequence ratings (for Safety, Environmental and Financial) for a hazardous event can be developed prior or during the LOPA. Refer to the HAZOP Procedure 0000-AH-PRC-70001 for additional guidance on consequence categorisation.

6.3 LOPA Specific Requirements

A LOPA has specific requirements regarding the assignment of Protection Layers (PLs) as safeguards, particularly regarding independence. This is a key difference from a hazard study (such as a HAZOP) where all relevant safeguards can be listed without undue consideration as to the levels of independence from each other or from the cause/initiating event. For PLs to be applied in a LOPA they shall comply with the following (as per AS IEC 61511):

1. Specificity: The PL functionality shall prevent the specific unique event identified from reaching the stated final consequence.
2. Independence: The PL shall be independent from all other protection layers associated with the hazardous event (i.e. it shall be independent from the initiating event and from other PLs). Performance shall not be affected by failure of another PL or the conditions that caused the other PL to fail. Where it is suitable and correct to apply more than one PL with a common element then the collective risk reduction of the common element shall be taken into account (e.g. where more than one SIF is applied using the same SIS, then the summated SILs for each SIF shall not exceed the SIS SIL). At this point the PL can be considered to be an Independent Protection Layer (IPL).
3. Dependability: The PL reduces the risk by a known and specified amount. A dependable/realistic PFD shall be assigned to each IPL.
4. Auditability: The PL is able to be periodically tested/proven to ensure ongoing validation of performance.

6.4 LOPA Sequence of activities/steps

The core LOPA process shall follow the sequence of steps (a to o) below (refer also to step clarifications below the flowchart).

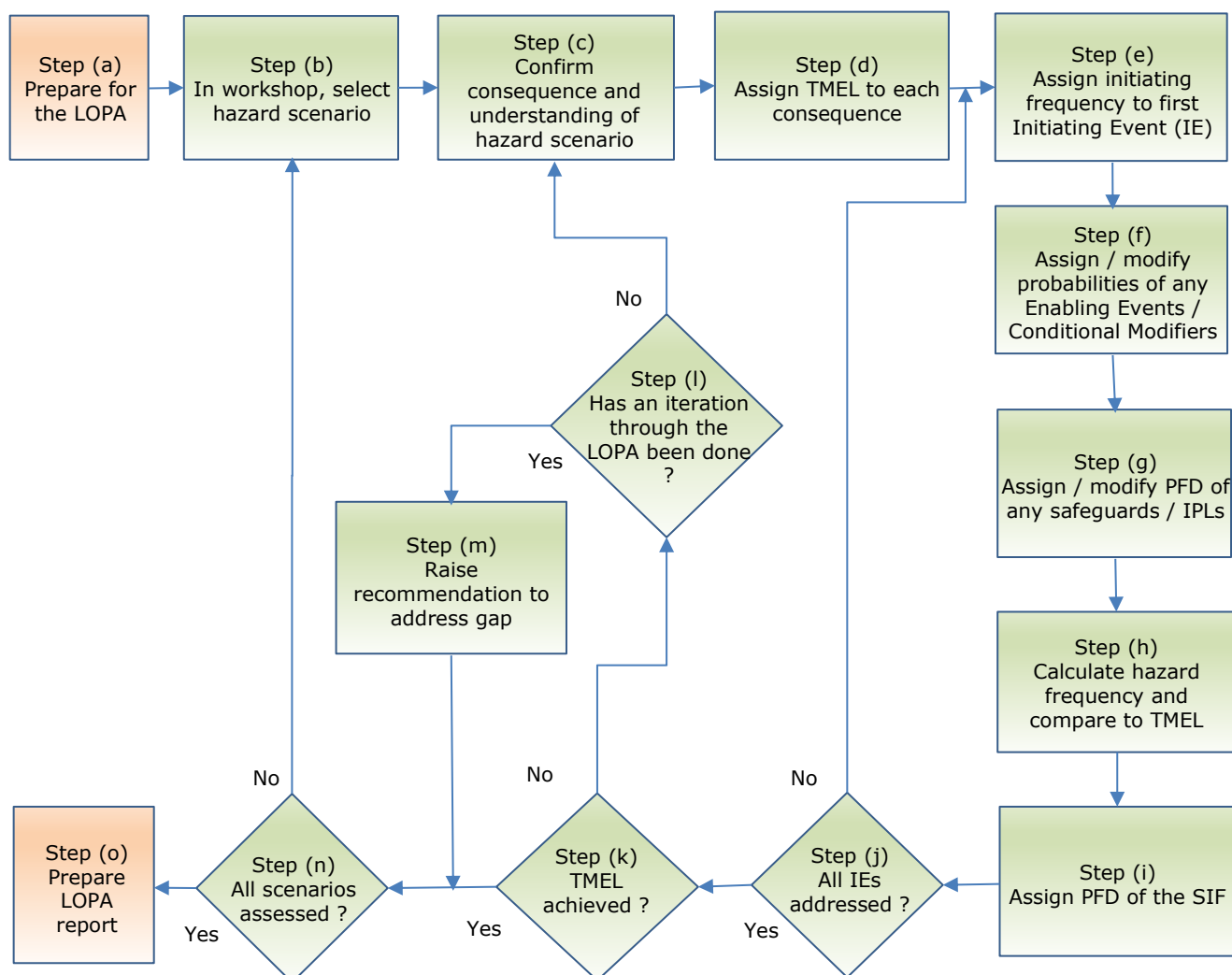


Figure 3 - LOPA Flowchart

Flowchart Step clarifications:

- Identify the hazardous scenario(s) that require further assessment via LOPA (This is normally based on information from a hazard study record (see section 6.2)), prepare the ToR, organise the workshop (see sections 4 and 5) and pre-populate the LOPA with hazard scenarios.
- In the workshop, select the hazardous scenario to be examined, either the first scenario or subsequent scenario (depending on the iteration through the flowchart).
- Confirm understanding of the hazardous event and consequence from the hazard study (including that the consequence reflects the credible worst case consequence – i.e. the unmitigated consequence).
- Assign the TMEL for each consequence in terms of Safety, Environment, and Financial impacts (see APPENDIX A:).
- Determine and assign the first Initiating Event (IE) frequency (see APPENDIX B: for IE frequencies). Historic SIF demands should be reviewed to validate the IEF used for the hazard scenario. If this frequency is more than once per year then the next 'layer of defence' is in "high demand mode" and it is this 'next layer' (and its frequency of failure)

that should be used as the IE frequency. See also section 1.5 for High Demand Mode definition in relation to a SIF, and APPENDIX F: for an example.

- f. Assign any relevant Enabling Events and/or Conditional Modifiers and their respective probabilities (see APPENDIX C:).
- g. Assign the other IPLs (if any) and their respective PFDs (see APPENDIX D:). The IPLs need to meet the criteria as per section 6.3 and any other requirements stated in APPENDIX D:.
- h. The overall hazardous event frequency (considering the IE(s) and the relevant Enabling Events and/or Conditional Modifiers and IPLs, but excluding the SIF being examined) is calculated.

$$\text{Haz. Event Freq.} = \sum_{i=1}^n (IE_i \times (P_{1i} \times P_{2i} \times \dots \times P_{yi}) \times (PFD_{1i} \times PFD_{2i} \times \dots \times PFD_{yi}))$$

Where: n=number of IEs

y=number of Conditional Modifiers/Enabling Events or IPLs per IE

P_{1i}=the probability of the first Conditional Modifier/Enabling Event for IE_i

PFD_{1i}=the PFD of the first IPL for IE_i

This is then compared against the TMEL to identify if a risk gap remains.

$$\text{Risk gap or RRF required} = \frac{\text{Haz.Event Freq}}{\text{TMEL}}$$

- i. If there is an existing SIF then it shall be assigned with a PFD matched (if possible) to the RRF required from step (h). Refer to APPENDIX E: for the relationship between RRF, PFD and SIL.

The following shall be adhered to:

- As the SIF hardware implementation may restrict the PFD that can be assigned, a check of the PFD achieved by the existing SIF should be performed by reference to the existing SIL calculations.
- Where the RRF required is ≤1 then the PFD assigned to any SIF shall be 1 (i.e. essentially no SIF is required to meet TMEL).
- Where the RRF required is <10 and can be applied to an existing SIF then the SIF should stay in the SIS but is not expected to need function testing. The SIF should not be removed from the SIS in case the LOPA changes in the future and to save effort (and risk) in de-commissioning the logic etc.
- Where the RRF required is <10 without an existing SIF, then either a BPCS based function can be considered (unless maximum credit for BPCS functions has already been applied for the scenario, including the initiating event – refer APPENDIX D: Note 1), or a SIS based function with RRF<10 can be considered along with other options (see also APPENDIX C:).
- A SIL 4 rated SIF shall not be accepted, the process design shall be revisited to provide additional layers of protection
- Where a SIL 3 rated SIF is identified:
 - the process design shall be revisited to determine if additional layers of protection can be provided or the rating shall be fully justified through the preparation of a specific report.
 - it can only be accepted with approval of Technical Safety Technical Authority (TA-1) and the Instrument & Controls Technical Authorities (TA-1).

- Where the highest SIL rating relates to a financial consequence these may be reduced based on cost benefit arguments in consultation with the Technical Safety Technical Authority TA-1.

Each SIF assigned shall:

- Have a unique identification via the SIF's sensor sub-system tag number.
 - Identify the relevant final element(s) that prevents the specific hazardous condition (or brings it to a safe state), and note any specific requirements (e.g. TSO valve).
- j. Where more than one IE has been identified for the same consequence then it shall be added to the same hazardous scenario with the relevant steps above repeated as shown in the flowchart.
- k. If there is an identified risk gap (i.e. essentially step (i) has failed to reach TMEL after all IEs, IPLs etc and the SIF have been accounted for) then the LOPA shall be examined by iterating through the steps as shown in the flowchart.

Where the TMEL is achieved, and particularly where 'human error' is the IE or human response is considered an IPL, the LOPA shall be examined by iterating through the steps as shown in the flowchart to check if anything else can practicably be done to reduce the risk further and ensure risk is ALARP. Note this is not intended to be an exhaustive or analytical examination but rather a 'sense check' that the IPLs are sufficient and robust and if any other IPLs should be applied (e.g. avoiding reliance on human response by implementing additional instrumented controls).

- l. A decision is to be made whether it is worthwhile reiterating through the steps in whole or in part to see what, if anything, can be modified (e.g. improve PFD of an IPL) to help achieve TMEL, or whether a recommendation needs to be raised.

If TMEL(s) is not achieved then raise a recommendation to investigate/review/address as necessary. Consideration should also be given to improving the design to eliminate the hazard (i.e. adopt an inherently safe design), or implement engineering controls as a priority over administrative controls. The LOPA scenario will need to be revisited at some stage to update it according to the recommendation closeout (also see section 6.5).

Refer to APPENDIX H: for additional guidance on Operational Phase LOPA recommendations.

- m. If there are more hazardous scenarios to address then repeat the steps for each one in turn.
- n. When the LOPA is finished, a report shall be produced as per section 6.7.

6.5 Recording the LOPA Minutes

The LOPA minutes shall be recorded using a suitable software package. The current preferred software for INPEX is LOPAx within exida's exSILentia software suite.

For each LOPA scenario the worksheet as a minimum shall record the hazard scenario (cause and consequence), Target Mitigated Event Frequency (TMEL), IPL description and relevant PFD, residual risk gap, recommendations (and actionee), and any supporting comments.

It is good practice to save the minutes frequently during the LOPA, with periodic saving to a different file name (in case a file becomes corrupted). As a minimum, at the end of each day, the minutes will be saved as a new/unique file (e.g. "LOPA abc – End of Day 1"), and at the conclusion of the LOPA the file shall be saved so as to indicate that it is the final minutes viewed and agreed by the LOPA Team as a whole (e.g. "LOPA abc – End of Workshop"). Any changes (even spell checking) after the workshop shall be saved as a separate file so as to preserve the integrity of a 'end of workshop' record.

During the LOPA the minutes shall be visible to all LOPA team members so as to ensure group agreement to the records being made.

Equipment tag numbers / identification shall be recorded for all relevant equipment to provide traceability and ready recognition during future reading etc of the LOPA record.

It is imperative that the minutes adequately describe the scenario that gives rise to a recommendation as follow-up may continue for some time after the LOPA and involve additional parties not present at the LOPA.

6.6 LOPA Recommendations

A LOPA recommendation can be made as a temporary recommendation to get further information during the LOPA workshop with the aim that it is resolved before LOPA completion and so prevent a formal recommendation being raised.

Recommendations arising out of a LOPA shall be clear and standalone. It is of critical importance that the text of a recommendation clearly conveys the requirements such that it can be addressed by personnel who were not in attendance at the LOPA.

A recommendation shall be assigned to one person who is in attendance at the LOPA.

Refer to APPENDIX H: for additional guidance on Operational Phase LOPA Recommendations. See also section 7 for recommendation closeout.

6.7 LOPA Reporting

A report shall be prepared for each LOPA. The Facilitator is responsible for preparation of the report detailing the findings of the study. This shall be retained for future reference as it is key documentation outlining the basis and findings for determining the SIL of each relevant SIF and also the documentation of all the PLs that need to be maintained to achieve tolerable risk.

The report content may vary depending on the size/scope of the LOPA but will typically include the following (the main consideration should be as to the readability, traceability of information, and awareness that this report will be used to produce or update the relevant Safety Requirements Specification (see section 3.1 and Phase 3 of the flowchart)):

- Executive Summary;
- Scope of Study;
- Methodology;
- Project Input References (e.g. ToR, list of P&IDs, this Procedure, other data);
- Source Data References (for initiating events, PFDs etc.);
- Any assumptions;
- LOPA record sheets that include:
 - Unique identification for each SIF (via the SIF's sensor sub-system tag number), IPL (e.g equipment / tag number), and relevant PFDs/RRFs

- Hazardous scenario description, consequence(s) and TMEL(s)
- Initiating cause and frequency
- Demand mode
- Enabling factors and conditional modifiers
- IPLs and associated PFDs
- Mitigated event frequency with total RRF calculated
- Unique identification for each SIF and its SIL/PFD/RRF
- Other requirements such as PST, TSO etc
- Summary SIF listing, description and SIL Level (or PFD) of each SIF;
- Summary PL listing, description and PFD for each PL;
- Attendance record; and
- Recommendations.

7 LOPA RECOMMENDATION CLOSEOUT

All LOPA recommendations shall be tracked to closure using a transparent, robust and fully auditable action management system/process approved by INPEX.

Recommendations shall be assigned to the relevant engineering discipline to determine approaches and work required for close-out. It is recommended that these be discussed and agreed with the relevant INPEX discipline Technical Authority Level 1 or 2.

Recommendation resolution statements shall clearly explain the actions to be taken with associated justification. Relevant studies/technical notes or other documentation shall be referred to and relevant extracts attached (by document number, revision & date) within the action party response.

All LOPA close-outs shall be signed by the individual primarily responsible for producing the close-out.

Where a Contractor is tasked with LOPA close-out the Contractor's discipline lead/supervisor shall be responsible for ensuring that necessary quality assurance and engineering checks have been conducted and documented to support the close-out.

Unless specified in an Inpex approved TOR, irrespective of who is responsible for completion of the LOPA recommendation closeout, the following INPEX representatives are, as a minimum, required to approve all LOPA recommendation resolutions:

1. Relevant discipline Technical Authority Level 2 (as TA-1 delegate) who provides:
 - confirmation that the technical aspects of the response are acceptable and consistent with Inpex design standards, philosophies and specifications; and
 - confirmation that the necessary design/procedural documentation has been appropriately updated to implement any potential change.

For internal LOPAs the TA-2 is also responsible for quality assurance and engineering checks that have been conducted and documented to support the close-out.

The Process TA-2 shall sign-off recommendations allocated to Operations personnel.

2. Relevant Engineering Manager (optional for Operational Phase) who provides:
 - Agreement on the recommended course of action is accepted from a cost and schedule perspective.
3. Technical Safety concurrence on recommendation close-out is required for all LOPA recommendations, the intent of this is to verify that:
 - The action taken clearly addresses the intent of the LOPA Recommendation;
 - The action taken is consistent with managing the associated risks to ALARP; and
 - The action has been implemented, demonstrated through inclusion in the relevant design documentation / drawings.

Refer to APPENDIX H: for additional guidance on Operational Phase LOPA Recommendations.

Where a change results from a LOPA recommendation, the recommendation shall only be considered closed with final acceptance by INPEX when:

- For Project phase - it has been verified that the recommendation has been implemented within the issued design documentation/drawings.

- For Operational phase - recommendations can be closed when the item is addressed **or** once the risk is being managed via another mechanism. The below are examples are specifically defined as acceptable scenarios for closure:
 - An existing risk is identified but the required changes relate to documentation updates only (ie no hardware or software impact).
In this case a LOPA recommendation shall be deemed closed when the updated document is approved (there is no requirement for backdrafting to be completed prior to closure).
 - An existing risk is identified and changes or acceptance are being managed by MOC or SCR processes (ie are not covered by Operations Projects / Brownfields processes).
In this case a LOPA recommendation shall be deemed closed when the relevant MOC has been endorsed and submitted for approval.
Note the MOC must clearly document the LOPA recommendation and response (including any action tracking details) to ensure that endorsers/approvers are aware that the issue has been raised at a LOPA. If the MOC approver rejects the MOC the LOPA recommendation can only be closed if sufficient justification is provided from the approver. If this is not provided, the LOPA recommendation shall be re-visited and alternative solution sought.
 - An existing risk is identified and changes are being managed by Operations Projects (Brownfields) processes.
In this case a LOPA recommendation shall be deemed closed when the relevant MOC has progressed to 'Define Solution' status and the Project Initiation Notice (PIN) has been raised and approved.
Noting the MOC cannot progress to endorsement stage until engineering is complete, and project execution and/or CAPEX allocation is managed by Operations Projects with Risk Owner input.
Note the MOC must clearly document the LOPA recommendation and response (including any action tracking details) to ensure that endorsers/approvers are aware that the issue has been raised at a LOPA. If the MOC approver rejects the MOC the LOPA recommendation can only be closed if sufficient justification is provided from the approver, if this is not provided the LOPA recommendation shall be re-visited and alternative solution sought.
 - A risk is identified that relates only to a proposed change, for example a LOPA is completed for an Operations Project or MOC where equipment is to be added and the LOPA recommendation is only applicable if the project is executed (ie there is no existing risk).
In this case recommendations are deemed closed when changes are identified on the documentation/drawings associated with the change (eg variant). Noting that if the change does not proceed then the risk does not materialise, and there is no change in risk for the facility.

The LOPA Sponsor shall monitor and report the status of all LOPA recommendations to Project Management (or Operations Management if in Operational phase) on a monthly basis.

A LOPA close-out report shall be issued to formally record close out of relevant LOPA recommendations. Recommendations that are not closed at the point of issue of the LOPA close-out report (for whatever reason) shall be transferred into, and managed by, an INPEX approved action tracking management system.

Project LOPA recommendations shall be closed out and the close out process verified prior to operations, start-up or before the relevant hazard(s) are introduced to the facility. In specific cases, recommendations may be considered for carryover, however this will be subject to prior approval by the relevant Technical Authorities (Level TA-1). Recommendations arising out of Operations stage LOPAs shall be assessed on a case-by-case basis to determine if sufficient safeguards are in place to continue operating the facilities.

Operational Phase LOPA recommendations shall be closed out in line with assigned priority and/or agreed timeframes.

LOPA recommendations and close out responses relating to a single facility shall be retained in a searchable electronic database.

8 SIL ASSESSMENT AUDIT

SIL Assessments shall be subject to audit processes to ensure they are fit for purpose via an established SIL Assessment assurance framework which examines:

- SIL Assessment inputs including planning, scope, timing, organisation, terms of reference and quality/maturity of input drawings/documentation relative to the specific SIL Assessment objectives.
- SIL Assessment process including rigor in application of the SIL Assessment methodology, competence of the study facilitator/team, and quality of study recording and reporting.
- SIL Assessment outputs including processes implemented for SIL Assessment action tracking, appropriate assignment of recommendations, quality and appropriateness of recommendation resolution and final close-out of recommendations by implementation in design documentation.

Project/Operations managers shall establish internal review mechanisms to assure initial and ongoing compliance with the minimum requirements established in this Procedure.

An independent audit should be considered:

- Prior to initial start-up, the SIL Assessments shall be reviewed to confirm they are representative of the as-built process facilities and that there are no SIL Assessment gaps due to omission or as a result of changes in design.
- Prior to initial start-up of a facility, the status of all outstanding SIL Assessment recommendations shall be reviewed to confirm that no safety related recommendations remain outstanding.
- Prior to facility re-start following a process system modification or change, the status of all relevant SIL Assessment recommendations shall be reviewed to confirm that no safety related recommendations remain outstanding.

Independent audits shall (as a minimum) be completed for detailed design and vendor SIL Assessments.

To avoid a conflict of interest, audits shall be conducted by a person or persons independent from the LOPA and Project. The auditor shall be approved by INPEX Technical Safety TA-1.

Independent 3rd party SIL Assessment audits may be considered where there may be real or perceived conflicts of interests or INPEX resource constraints.

Refer to APPENDIX G:for suggested audit questions.

The output of the audit (depending on the focus and timing of the audit) should:

- Identify shortfalls that can provide lessons learnt for future SIL Assessments (perhaps by way of revising this procedure, and/or as direct feedback to the LOPA Sponsor, Facilitator etc);
- Identify shortfalls that may require a re-visit of the SIL Assessment;
- Identify shortfalls that may require a revisit of recommendation close-outs.

APPENDIX A: TARGET MITIGATED EVENT LIKELIHOODS

The Target Mitigated Event Likelihood (TMEL) shall be determined based on the credible worst case consequence of the hazardous event.

TMEL criteria for safety and environmental events shall be defined based on the consequence ranking provided in the INPEX Risk Matrix (refer section 2.1), and as defined in Table 1 below. Note that TMELs are not defined for consequence rankings E and F since these relate to minor injuries that are not consistent with the credible worst case consequences of a process related accident.

Table 1 - Safety & Environmental TMELs

Consequence Ranking	Consequence Category		TMEL (/yr)
	Safety	Environment	
A	> 20 fatalities or permanent total disabilities	Regional scale event, permanent impact on environment	1×10^{-6}
B	2 - 20 fatalities or permanent total disabilities	Large scale event, long term impact on environment	1×10^{-5}
C	Single fatality or permanent total disability	Medium to large scale event, medium term impact on environment	1×10^{-4}
D	Major injury or illness or permanent partial disability or lost time case.	Local to medium scale event, short to medium term impact on environment	1×10^{-3}
E	Minor injury or illness, alternate injury case or medical treatment case.	Local scale event, short term impact on environment	-
F	Slight injury or illness, first aid case.	Local scale event, with temporary impact on environment	-

TMEL criteria for financial events shall be defined based on the consequence ranking in the INPEX Risk Matrix, and as defined in Table 2 below:

Table 2 - Financial TMELs

Consequence Ranking	Financial NPV (USD)	TMEL (/yr)
A	> \$1B	1×10^{-5}
B	\$100M - \$1B	1×10^{-4}
C	\$10M - \$100M	1×10^{-3}
D	\$1M - \$10M	1×10^{-2}
E	\$100K - \$1M	1×10^{-1}
F	<\$100K	1

APPENDIX B: INITIATING EVENT FREQUENCIES

The following shall be used for assigning a frequency to an initiating event during SIL Assessment. Where the relevant failure is not listed in Table 3 below, or more reliable data is sourced (or required to be sourced including human error rate refinement, or from historic SIF demands), then other data can be utilised and referenced with prior approval of the Technical Safety TA-1:

Table 3 - Initiating Event Frequencies

Initiating Event	Frequency (year)
BPCS Loop Failure (or Loss of Control) (from AS IEC 61511). This includes any APC (Advanced Process Control) related failure modes, which should not be treated as a separate initiating event.	0.1
Mechanical Self-Regulating Regulator Failure (from CCPS - refer section 2.4) (whether the regulator fails closed or open depends on failure mechanism and construction of the regulator – use the stated value for either fail closed or open)	0.1
Exchanger tube or PCHE leak (no moving parts, no vibration, non-corrosive) (estimated based on Energy Institute Guidelines for the Safe Design and Operation of Shell and Tube Heat Exchangers to Withstand the Impact of Tube Failure Section 2.5)	0.01
Exchanger tube rupture (no moving parts, no vibration, non-corrosive) (based on Energy Institute Guidelines for the Safe Design and Operation of Shell and Tube Heat Exchangers to Withstand the Impact of Tube Failure Section 2.5)	0.001
Single equipment failure (e.g. Pump failure, Rotating equipment failure, pump seal failure, hose failure in non-vibrating service). (typical/estimated value) Note that if multiple/redundant equipment failures are relevant then they shall be treated as an IPL.	0.1
Pump seal failure – single mechanical seal (typical/estimated value)	0.1
Pump seal failure – double mechanical seal – with seal failure detection of either seal. (typical/estimated value)	0.01
Relief valve spuriously opens (refer to OREDA 2015 Ed 6 taxonomy 4.4.12 - upper calendar time failure rate)	0.01
Fail closed shutdown ball valve spuriously closes (rounded down from 0.02/yr – refer to OREDA 2015 Ed 6 taxonomy 4.4.5.1 - upper calendar time failure rate). Also to be applied for spurious opening of a BDV.	0.01

Initiating Event	Frequency (year)
Strainer blockage – team to select frequency based on process conditions and operational experience	(team decision – typically 0.1 or 0.01)
Check valve stuck closed (0.364 failures per 1000 demands and assuming < 10 demands per year = <0.00364 - Refer to CCPS Guidelines for Process Equipment Reliability Data 1989 taxonomy 3.5.1.2 - upper failure rate)	0.001
High Demand Mode SIF - Refer to APPENDIX E: for range of values. Values listed here reflect the higher value of the dangerous undetected failure rate for a SIL rated system that has not yet been verified - they therefore present a conservative estimate of the failure frequency. The frequency can be modified if the quantification of random failure calculation has been done. Where one or more SIFs are also applied as IPLs in one hazardous scenario, any common sub-systems shall be accounted for and the PFD of the IPL reduced accordingly.	0.1 (for SIL 1 SIF) 0.01 (for SIL 2 SIF) 0.001 (for SIL 3 SIF)
High Demand Mode single check valve - fail to close – clean service and valve. Note check valves are credited to prevent significant flow, but cannot be credited to prevent small leakage / pressurisation cases. No requirement to be periodically functionally checked or replaced to ensure functionality as operates in high demand mode. (Refer to CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis - Appendix D). Note valves shall be designated as SRDs.	0.020
High Demand Mode multiple dissimilar check valves - fail to close – clean service and valves are to be periodically functionally checked or replaced to ensure functionality. Note check valves are credited to prevent significant flow only, but cannot be credited to prevent small leakage / pressurisation cases. To periodically functionally checked or replaced to ensure functionality as both check valves cannot be proved by operating in high demand mode. (Refer to CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis - Appendix D, frequency extrapolated for 10/20 year intervals). Note valves shall be designated as SRDs.	0.0033 (10 yr test interval) / 0.0066 (20 yr test interval)

Human Error rates

With reference to Table 5-1 in the AIChE CCPS Concept Book, Layer of Protection Analysis, Simplified Process Risk Assessment, Centre for Chemical Process Safety 2001, a range of 0.1 to 0.001 per opportunity for a well-trained, unstressed, not fatigued Operator is given. Therefore a value of 0.01 per opportunity is applied in this Procedure when the following conditions are met:

- The task/procedure is a routine activity – not complicated; and
- Operator is well trained in the task; and
- Operator is not stressed or fatigued during the task.

Clarification notes:

1. If these conditions are not met then the values in the table below may be increased by a factor 10.
2. If there is an independent check that the task has been completed correctly then the values in the table below may be reduced by a factor of 10, typically applied as a 'Conditional Modifier'.
3. If a spectacle blind / spacer / spool piece or locked / interlocked manual valves are required to be manipulated (and design position would protect against the hazard) this can also be credited as an IPL, as per Appendix D.
4. If multiple steps in the same procedure address the particular hazardous event under consideration, no further credit shall be applied if the same Operator is performing the steps (i.e. the Operator is considered to be the 'common mode of failure').

Table 4 - Human Error Rates

Human error - task frequency	Frequency (year)
Human error - task performed fortnightly or more frequently.	1
Human error - task performed once or twice per month.	0.1
Human error - task performed less than once per month but more than once per year.	0.05
Human error - task performed once per year or less frequent.	0.01

APPENDIX C: ENABLING EVENTS / CONDITIONAL MODIFIERS

Modification Factors can be applied where relevant to do so. Such factors include 'Enabling Events' that are usually assigned to reduce the Initiating Event likelihood, and 'Conditional Modifiers' that are usually assigned to reduce the likelihood of the consequence occurring. They include:

- time at risk;
- occupancy;
- ignition;
- factors/probabilities with Technical Safety Technical Authority TA-1 approval.

Care shall be taken in the application of modification factors to ensure that they are valid within the overall context of the SIL Assessment process and do not compromise the conservative nature of the analysis.

Enabling Events are conditions that are not as a result of a failure or error, but are conditions that allow an incident sequence to continue beyond the initiating event (i.e. it must be present for the scenario to proceed). It includes equipment being in a particular state of operation (e.g. see time at risk below). When considering use of an Enabling Event the possibility of a common cause failure with another PL shall be considered. Use of Enabling Events in LOPA are rare and their use shall be clearly justified.

Time at risk shall be used with caution and shall:

- Only be applied to systems that are not in continuous use, and are out of service for the time that the system is not in use (i.e. it does not apply to systems that can start and operate at any time even if for a limited duration as the failure needs to be revealed before the system comes back online);
- Only be applied where the associated random failure mode is checked, able to be detected, and fixed before that system comes back on line;
- Be determined based on a conservative estimate of the fraction of a year which the system is operational and thus presents a hazard;
- Not be applied to continuously operating equipment or equipment operating with a redundant sparing (e.g. 3 x 50% pumps); and
- Not be applied for start-up activities.

Conditional Modifiers act to reduce the likelihood of the consequence. Use of Conditional Modifiers shall be justified and used with care. Personnel occupancy and Ignition probability are examples of Conditional Modifiers (see below).

- Personnel occupancy should:
 - Only apply to systems that have low manning levels or are unmanned and where there is clear justification for its application;
 - Be included in the assessment of SIL for health and safety consequence scenarios only;
 - Be determined based on a conservative estimate of the fraction of time personnel are exposed to a hazard in the course of a year. As a default, occupancy should not be applied for permanently manned offshore facilities;
 - Be determined with due consideration of the scenario consequence category (i.e. if consequence category B is selected it refers to occupancy by more than one individual);

- Be limited to the following values unless specific work is done to establish occupancy levels and this is approved by the Technical Safety TA-1:
 - 0.5 (i.e. personnel not in the vicinity of the hazard 50% of the time);
 - 0.25 (i.e. personnel not in the vicinity of the hazard 75% of the time);
 - 0.1 (i.e. personnel not in the vicinity of the hazard 90% of the time); and
 - 0.01 (i.e. personnel not in the vicinity of the hazard 99% of the time). Use of 0.01 implies a very strict degree of control over the exposure and it is only appropriate to use this factor in locations where access is strictly controlled and limited to 1 or 2 days per year.
- Take into account periods of increased occupancy (within an annualised average) to ensure that the SIL Assessment remains robust; and
- Not be applied for scenarios where personnel may be in attendance as a result of initiating cause (e.g. start-up scenarios where personnel are present or where operators may be sent to the location to investigate the initiating cause due to an alarm annunciation etc).
- Ignition Probability:
 - Shall only apply to systems where the release of flammable materials would not result in significant safety consequences unless it ignites (i.e. does not apply to toxic gases or where there is asphyxiation risk); and
 - Shall not be lower than the values stated in Table 5 below.

Table 5 - Generic Ignition Probabilities

Fluid	Situation	Description	Release Rate (kg/s)	Ignition Probability
Gas/Condensate	Confined	Large	>50	0.5
		Medium	1-50	0.15
		Small	<1	0.05
	Semi-confined	Large	>50	0.3
		Medium	1-50	0.05
		Small	<1	0.01
	Open	Large	>50	0.2
		Medium	1-50	0.03
		Small	<1	0.01
Oil	Confined	Large	>50	0.15
		Medium	1-50	0.08
		Small	<1	0.05
	Semi-confined	Large	>50	0.08
		Medium	1-50	0.05
		Small	<1	0.03
	Open	Large	>50	0.05
		Medium	1-50	0.03
		Small	<1	0.01
All	Above auto-ignition temperature	Any	Any	1
	Close to high energy ignition source	Any	Any	1
Pyrophoric	All	Any	Any	1

APPENDIX D: IPL PROBABILIY OF FAILURE ON DEMAND

Where the relevant IPL equipment Probability of Failure on Demand (PFD) is not addressed within Table 6, other data sources may be utilised (e.g. OREDA) with prior approval of the INPEX Technical Safety Technical Authority TA-1.

Table 6 - Equipment Probability of Failure on Demand

Independent Protection Layer	PFD (=1/RRF)
Demand Mode SIF - Refer to APPENDIX E: for range of values. Values listed here reflect the higher value of PFD for a SIL that has not yet been verified - they therefore present a conservative estimate of the likely PFD. The PFD can be modified if the quantification of random failure (i.e. the PFD calculation) has been done. For multiple SIFs being applied in one hazardous scenario, any common sub-systems shall be accounted for and the PFDs adjusted accordingly.	0.1 (for SIL 1 SIF) 0.01 (for SIL 2 SIF) 0.001 (for SIL 3 SIF)
BPCS function, where it is sufficiently independent and is not associated with the initiating event being considered (from AS IEC 61511) - see Note 1 below this table	0.1
CCR Operator response to a BPCS alarm, where alarm is sufficiently independent and is not associated with the initiating event being considered (from AS IEC 61511) - see Notes 1,2 below this table	0.1
Multiple/redundant equipment failure (with auto-start of redundant equipment or initial failure alarmed and Operator can start within PST). Note if BPCS is utilised to start the redundant device then refer to BPCS constraints in Notes 1,2 below this table. (BPCS value applied)	0.1
Relief valve – Single valve, clean service, sized to mitigate scenario, and with no isolation valves (or with locked open isolation valves). (Refer to OREDA 2015 Ed 6 - Upper Calendar time failure rate with 2 yearly testing applied) Note valves shall be designated as SRD.	0.01
Relief valve – Multiple (qty N) partial load valves, clean service, all required to function to mitigate full load (includes staged release PSVs), and with no isolation valves (or with locked open isolation valves). (i.e. any 1 of the N valves failing will cause overpressure) Note valves shall be designated as SRDs.	$N \times 0.01$
Relief valve – Multiple (qty N) full load valves on line, clean service, each is sized to mitigate scenario, and with no isolation valves (or with locked open isolation valves). (i.e. all N valves would need to fail to cause overpressure) (worst case $N=2$; using PFD of 0.01 per valve and a nominal 10% beta factor - i.e. $0.01 \times 0.01 + 0.01 \times 0.1 = 0.0011$, note that beta portion dominates the result) Note valves shall be designated as SRDs.	0.001

Independent Protection Layer	PFD (=1/RRF)
Relief valve – Multiple (qty N) partial load valves, clean service, and sized such that more than one PSV would need to fail for scenario to occur, and with no isolation valves (or with locked open isolation valves). (i.e. M valves would need to fail to cause overpressure where $2 \leq M < N$) Using 10% beta factor: If 2 out of 4 RVs need to fail to cause overpressure – PFD = 0.0015 If 2 out of 5 RVs need to fail to cause overpressure – PFD = 0.0018 If 3 out of 5 RVs need to fail to cause overpressure – PFD = 0.001 So worst case is where any 2 of the RV set would have to fail, and using M=2 and N=5 as a typical qty with 10% Beta , PFD ~ 0.002 Note valves shall be designated as SRDs.	0.002
Relief valve – plugging service with no protection, or flowing / non-flowing pilot operated PSV in non-clean fluids.	1
Relief valve – plugging service with protection. Design is proven based on prior history of suitable operation in the required service conditions. PFD is as per relevant scenario above.	See above
Rupture Disc – sized to mitigate scenario, no isolation valves (or with locked open isolation valves). Note that effectiveness can be very sensitive to service and experience (Refer to American Institute of Chemical Engineers CCPS Concept Book, Layer of Protection Analysis, Simplified Process Risk Assessment, Centre for Chemical Process Safety 2001 - Table 6.4 - range is 0.1 to 0.00001) Note valve shall be designated as an SRD.	0.01
Vacuum breaker Note valves shall be designated as SRDs.	(refer to Relief valves above)
Centrifugal/Reciprocating pumps/compressors – protections vary depending on hazard scenario	(to be advised by Rotating Equipment specialist)
Car-sealed valve (open or closed) – no credit to be taken	1
Locked valve with single non-sequenced lock (open or closed) – key is managed in accordance with site requirements. (typical/estimated value - takes into account potential common cause with other field operations tasks) <i>Note this shall only be applied in combination with human error frequency, per Appendix B.</i> Note valve shall be designated as an SRD.	0.1

Independent Protection Layer	PFD (=1/RRF)
Locked valve with captive key sequenced lock (open or closed) i.e. interlocked valves – key is managed in accordance with site requirements. It is also required that the interlock arrangement is an effective protection against the hazard at both the start and the end of the interlock sequence. (typical/estimated value - takes into account key is not readily available as needs to be released from another device) <i>Note this shall only be applied in combination with human error frequency, per Appendix B.</i> Note valves shall be designated as an SRD.	0.01
Spectacle blind or spacer or spool piece (estimated value – aligned to credit applied for a locked valve with single non-sequenced lock) <i>Note this shall only be applied in combination with human error frequency, per Appendix B.</i>	0.1
Single check valve fail to close – clean service and valve is to be periodically functionally checked or replaced to ensure functionality Note check valves are credited to prevent significant flow, but cannot be credited to prevent small leakage / pressurisation cases. (Refer to CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis - Appendix D based on failure rate 1.92×10^{-2}/yr and PFD extrapolated for 10/20 year intervals). Note check valve shall be designated as an SRD.	0.1 (10 yr test interval) / 0.2 (20 yr test interval)
Multiple dissimilar check valves fail to close – clean service and valves are to be periodically functionally checked or replaced to ensure functionality Note check valves are credited to prevent significant flow only, but cannot be credited to prevent small leakage / pressurisation cases. (Refer to CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis - Appendix D based on failure rate 1.92×10^{-2}/yr and PFD extrapolated for 10/20 year intervals). Note both check valves shall be designated as SRDs.	0.01 (10 yr test interval) / 0.05 (20 yr test interval)
Mechanical Stop - Permanent Stop is set and verified initially with adjustment or slippage not possible thereafter without deliberate verified intervention e.g. stop is welded or securely bolted in place. Device placement is checked as per X060-A1-STR-60094 requirements, to confirm integrity and that it remains in correct location. (Refer to CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis Dec 2014 – Data Table 5.10) Note valve shall be designated as an SRD and the SRD Register shall detail the required mechanical stop.	0.01

Independent Protection Layer	PFD (=1/RRF)
Adjustable Movement Limiting Device Adjustable device which prevents human miss operation. Device is easily adjusted but governed by a specific procedure and it can only be adjusted by trained and authorised individuals. There is clear indication that the device must not be tampered with by unauthorised personnel. Incorrect positioning is easily detectable by a visual check and checks are completed as per X060-A1-STR-60094 requirements to confirm integrity and ongoing effectiveness of the device. (Refer to CCPS Guidelines for Initiating Events and Independent Protection Layers in Layer of Protection Analysis Dec 2014 – Data Table 5.48) Note valve shall be designated as an SRD and the SRD Register shall detail the required mechanical stop.	0.1
Flame / Detonation Arrestors (Refer to American Institute of Chemical Engineers (AIChE) CCPS Concept Book, Layer of Protection Analysis, Simplified Process Risk Assessment, Centre for Chemical Process Safety 2001 - Table 6.3) Note shall be designated as an SRD.	0.01
Open Vent or Tank Overflow Line – line is properly sized, clean/non-fouling service with no valving or potential impediment to flow. (Based on American Institute of Chemical Engineers (AIChE) CCPS Concept Book, Layer of Protection Analysis, Simplified Process Risk Assessment, Centre for Chemical Process Safety 2001 - Table 6.3)	0.001
Open Vent or Tank overflow line – line is properly sized but potential impediment to flow (e.g. fouling). (100x above value)	0.1
Dike (bund) to reduce the frequency of large consequence (widespread spill) of a tank overflow/rupture/spill event. (Refer to American Institute of Chemical Engineers (AIChE) CCPS Concept Book, Layer of Protection Analysis, Simplified Process Risk Assessment, Centre for Chemical Process Safety 2001 - Table 6.3)	0.01
Actuated valve opening or closing time is credited to ensure equipment is protected from hazard and valve stroke time is achieved by mechanical means (refer to requirements in X810-AJ-SPC-70001). Valve shall be designated as an SRD, the SRD Register shall detail the required opening/closing time (or rate) and valve stroke time must be monitored to ensure required time is maintained (refer X060-A1-STR-60094 for maintenance requirements).	0.01

Note 1: During design phase the same BPCS layer may only be applied once in a LOPA scenario, unless Instrument & Technical Safety TA-1 approval is given.

However during operational phases then the same BPCS can be used a maximum of two times (including its use as the initiating event where applicable). Sufficient independence between these two BPCS functions needs to be confirmed otherwise the 2nd BPCS PL PFD shall be set to 1. To be “sufficiently independent” the following shall apply (including approval by Instrument TA-1/2):

- A separate sensor process tapping is used (considers common isolation error).

- A separate sensor, field termination assembly, and input module is used (considers common hardware failures).
- A separate output module and actor is used (considers common hardware failures).
- Separate logic function blocks are used (considers potential for a single software change/error to adversely impact both functions), unless the common 'block' (e.g. a common input processing function block) is subject to change control with peer checking and testing and that is confirmed to be in place.
- The BPCS shall have redundant processors, power supplies and communication modules (and I/O modules are not located in same rack as the CPUs).

(Junction Boxes, Cabinets, Homerun cables, FCSs, FCSs Racks, Buildings, HVAC systems, earthing systems and UPSs may be shared without violating independence rules).

Note 2: For Operator response to an alarm to be applied as an IPL:

- The Operator is to be present to receive the alarm, the alarm is a critical priority and the Operator has a relevant and clear AOA and/or procedural response to prevent the hazard; and
- There shall be sufficient time for the operator to react (a PST of at least 15 mins is required assuming the CCR operator receives the alarm and can act correctly without requiring field operator action); and
- The normal IPL rules for LOPA (see section 6.3) need to be applied for the alarm; and
- The rules regarding the BPCS as per Note 1 above need to be applied for the alarm.
- It is normally expected that the control system PFD will dominate over the human factor considerations in acknowledging and responding to the alarm. Therefore change of shift considerations shall generally be ignored. However, if an alarm can be expected to still be 'active' and visible across shift boundaries, and the next shift operator could be expected to see the alarm then additional credit can be considered against operator/human error.
- Note that as a preference, alarms should not be credited as IPLs due to the reliance on human action and the need for ongoing auditing/testing of the alarm and operator action.

APPENDIX E: SIL DEFINITIONS

The following tables align with AS IEC 61511 Tables 4 & 5 and map SIL to PFD for demand mode, and map SIL to dangerous failure frequency for high demand mode:

Table 7: SIL vs PFD

SIL	Demand Mode	
	Average PFD _{SIF}	Risk Reduction Factor (1/PFD _{SIF})
4 (not permitted)	$10^{-5} \leq \text{PFD} < 10^{-4}$	$10,000 < \text{RRF} \leq 100,000$
3	$10^{-4} \leq \text{PFD} < 10^{-3}$	$1,000 < \text{RRF} \leq 10,000$
2	$10^{-3} \leq \text{PFD} < 10^{-2}$	$100 < \text{RRF} \leq 1,000$
1	$10^{-2} \leq \text{PFD} < 10^{-1}$	$10 < \text{RRF} \leq 100$
SIF has no special integrity requirements.	$10^{-1} \leq \text{PFD}$	$\text{RRF} \leq 10$

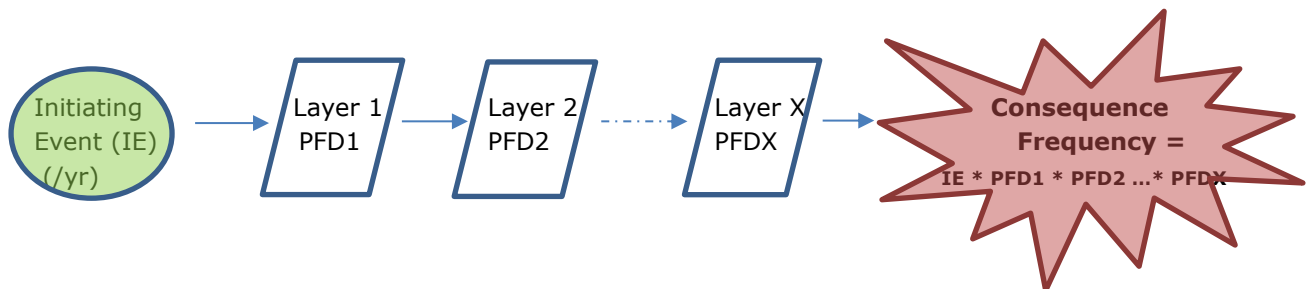
Table 8: SIL vs Frequency of Failure

SIL	High Demand Mode
	Average Frequency of dangerous failures (per hour)
4 (not permitted)	$10^{-9} \leq \text{Freq} < 10^{-8}$
3	$10^{-8} \leq \text{Freq} < 10^{-7}$
2	$10^{-7} \leq \text{Freq} < 10^{-6}$
1	$10^{-6} \leq \text{Freq} < 10^{-5}$
SIF has no special integrity requirements.	$10^{-5} \leq \text{Freq}$

APPENDIX F: HIGH DEMAND MODE

The following is an explanation of high demand mode application – i.e. when to use the frequency of failure of an IPL rather than multiply the IPL's PFD by the frequency of demands on it.

Using the following diagram as a guide, there are 1 or more layers of protection between the 'cause' (the Initiating Event) and the hazardous scenario 'consequence'. When the 'cause' occurs (or is expected to occur) more than once per year this puts the 'first protection layer' in "high demand mode" (as defined in AS IEC 61511) and hence it is the frequency of this first protection layer that is relevant. Therefore it is this first protection layer that becomes the initiating event (it would be incorrect and overly conservative to multiply the high frequency of the initial event by the PFD of the first protection layer).



A BPCS is an example of a high/continuous demand mode system as it is continually 'controlling' the process – and only when it fails at its defined frequency (usually taken as 0.1/yr) does a demand on the next protection layer occur (and in this example, the high frequency of the demands on the BPCS is irrelevant as they occur more than once per year). As an example using a process parameter being controlled by the BPCS ;

- Say the process parameter deviation occurs 100x per year.
- Then if the first protection layer was taken to be the BPCS (with a PFD of 0.1) then it would be incorrect to calculate $100 \times 0.1 = 10$ /year and use this value as the combined resultant frequency, as this frequency is greater than the failure frequency of the BPCS (0.1/yr).
- Recognising the high frequency of the initiating event, this means that the first protection layer (i.e. the BPCS in this example) is in high demand mode and so it is the frequency of failure of the BPCS that is relevant. The BPCS failure frequency is 0.1 /year and it is the failure of the BPCS that becomes the actual initiating frequency. This is why process parameter deviation frequencies are typically 'ignored' and the BPCS is taken as the initiating event with its typical 0.1/yr failure rate applied.

In applications where the demand rate on a SIF is more frequent than once per year, the hazard rate cannot be higher than the dangerous failure rate of the SIF, and so the SIF undetected dangerous failure frequency can be used as the initiating event. As an example, looking at a SIF in high demand mode:

- Say the BPCS loses control 10x per year due to controllability or other issues.
- Then if a SIL 1 SIF is the next layer of protection (with a PFD of 0.04) it will be demanded 10x per year, and it would be incorrect to calculate $10 \times 0.04 = 0.4$ /yr as the combined resultant frequency, as this frequency is greater than the failure frequency of the SIL 1 SIF (say 0.08/yr).
- Recognising the high frequency of the initiating event, this means that the first protection layer (i.e. the SIL 1 SIF in this example) is in high demand mode and so it is the frequency of failure of the SIF that is relevant. The SIF failure frequency used in this example is 0.08 /year and it is this failure frequency of the SIF that becomes the actual initiating frequency.

APPENDIX G: AUDIT CHECKLIST/QUESTIONS

	Suggested Questions	Verification
SIL Assessments shall be planned and conducted at the appropriate time in the project or facility lifecycle	a) Have SIL Assessment studies been included within a project master schedule as key milestones to follow HAZOP studies?	Project Master Schedule
Each SIL Assessment shall have a clearly identified SIL Assessment Sponsor.	a) Does the SIL Assessment study have a clearly identified Sponsor? b) Does the SIL Assessment Sponsor meet all competency criteria?	Project Documentation
Each SIL Assessment shall have a clearly identified SIL Assessment Co-ordinator	a) Does the SIL Assessment study have a clearly identified Co-ordinator? b) Does the SIL Assessment Co-ordinator meet all competency criteria?	Project Documentation
A SIL Assessment Terms of Reference (ToR) shall be developed, approved and distributed for each SIL Assessment	a) Has a Terms of Reference document been prepared and distributed to the SIL Assessment Team a minimum of 2 weeks in advance of the SIL Assessment start date? b) Have the terms of reference been approved by the SIL Assessment Sponsor prior to circulation?	SIL Terms of Reference
The rule sets/assumptions to be used in the completion of the SIL Assessment shall be clearly established and formally agreed with participants prior to commencement of the SIL Assessment	a) Have rule sets been clearly defined and agreed by all SIL Assessment participants prior to the commencement of the SIL Assessment? b) Do rule sets include both estimation of the consequence rating for a hazardous event in each of the impact areas (i.e. Safety, Environmental and Financial) and estimating hazardous event frequencies? (note, these may reside with the HAZOP where HAZOP was the precursor to the SIL Assessment).	SIL Terms of Reference
A SIL assessment shall be facilitated by an independent SIL Assessment Workshop Leader	a) Was the SIL Assessment study facilitated by an independent facilitator? b) Was the facilitator approved by INPEX per 'Register of Approved HAZOP / SIL Study Leaders' (0000-AH-LIS-60001) or Technical Safety TA-1?	SIL Terms of Reference / SIL Assessment Report

	Suggested Questions	Verification
SIL assessments shall be completed by an experienced multidisciplinary team	a) Did the SIL Assessment Team consist of the minimum people representing the required core engineering disciplines? b) If specialist/specific areas of the process system were being investigated, were appropriate specialists involved in the SIL Assessment workshop? c) Does each member of the SIL Assessment team meet all competency criteria?	SIL Terms of Reference / SIL Assessment Report
All hazards associated with operating a process system shall be identified	a) Did the SIL Assessment address all relevant hazards and SIFs?	SIL Assessment Minutes / SIL Assessment Report
SIL Assessment studies shall be documented and records maintained	a) Has the SIL Assessment Scribe satisfactorily recorded the SIL Assessment study in the required worksheet format?	SIL Assessment Minutes
A SIL Assessment Report shall be prepared for each SIL Assessment	a) Has a SIL Assessment Report been developed and reviewed by SIL Assessment Team members prior to formal issue? b) Has a final SIL Assessment close-out report been issued?	SIL Assessment Report
All SIL assessment recommendations shall be actioned and closed-out using a robust and auditable process	a) Have SIL Assessment recommendations been tracked to their completion and closed out? b) Is responsibility for the recommendations clearly defined? c) Are the recommendation responses adequately recorded and monitored? d) Do the recommendations address the primary concern of the SIL Assessment recommendation? e) Has a formal review and approval been instigated for the close-out of SIL Assessment recommendations? f) Has a schedule been set for the close-out of recommendations?	Action tracking system SIL Assessment Documentation SIL Assessment Close-out Report

	Suggested Questions	Verification
SIL assessments shall be subject to review and audit processes to ensure they are fit for purpose	a) Have SIL assessment studies been subject to review and audit?	FSMP Project / Operations internal review mechanisms for SIL Assessments. Independent audit reports for detailed design and Vendor SIL Assessments.
SIL Assessments shall be reviewed at regular intervals to ensure they remain representative of the operating facility	a) Was an Independent FS Assessment conducted prior to initial start-up? b) Was the status of all outstanding SIL assessment recommendations reviewed to confirm that no safety related recommendations remained outstanding prior to initial start-up? c) Was the status of all relevant SIL assessment recommendations reviewed to confirm that no safety related recommendations remained outstanding prior to facility re-start following a process system modification or change? d) Have SIL assessments been completed for process systems after Revalidation HAZOPs	FSMP Independent audit reports for management of change SIL assessments Revalidation HAZOP Reports

APPENDIX H: ICHTHYS OPERATIONAL PHASE RECOMMENDATIONS ADDITIONAL GUIDANCE

H.1 Existing Risk Identified

The following guidance is applicable for recommendations raised from LOPAs completed for Ichthys facilities which are currently in operation, where the recommendation relates to an existing risk.

LOPA recommendations should be prioritised using this rule set, which is aligned to the Inpex Prioritisation Matrix (X060-A0-DAT-60001).

Residual RRF	Priority	Note
$RRF \geq 1000$	P1	Critical HSE risks require immediate mitigation and to be raised to risk owners.
$100 \leq RRF < 1000$	P2	-
$10 \leq RRF < 100$	P3	-
$1 < RRF < 10$	-	Note as per Decision Note (X060-A1-DCN-70010) this level of Residual RRF may be deemed ALARP by the workshop team with no recommendation raised. If deemed ALARP, ensure LOPA record documents the position and refers to X060-A1-DCN-70010. If not deemed ALARP, P4 priority should be used. Noting that P4 recommendations should generally be minimised, as per MOC 400001561.

Facilitators should ensure recommendations raised meet above requirements.

Prior to upload to the Action Management System (eg Cority) recommendation due dates should be confirmed outside of workshop in discussion with actionee and relevant Team Lead, using the following as starting point.

Priority	Due Date	Finding Owner	Approver	Tech Safety Verifier
P1	3 months	Discipline Team Lead	Discipline TA-1	Tech Safety TA-1
P2	6 months	Discipline Team Lead	Discipline TA-1	Tech Safety TA-1
P3	12 months	Discipline Team Lead	Discipline TA-2	Tech Safety TA-2
P4	24 months	Discipline Team Lead	Snr Discipline Engineer	Snr Tech Safety Eng
P5	48 months	Discipline Team Lead	Discipline Engineer	Tech Safety Eng

Actionee is typically as per LOPA record, however, can be reassigned by relevant Team Lead.

For recommendation allocated to Operations personnel (eg procedure updates) the Approver is relevant Process Engineer (level dependant on priority level).

Tech Safety Verifiers are aligned to Action Management Procedure (0000-A0-PRC-70007).

H.2 New Risk Introduced

The following guidance is applicable for recommendations raised from the LOPA of a proposed change to an Ichthys facility currently in operation. For example, a LOPA is completed for an Operations Project or MOC where equipment is to be added and the LOPA recommendation is only applicable if the project is executed (ie there is no existing risk).

LOPA recommendations should be prioritised as P3 to align with TA-2 endorsement.

Note depending on the change, the Operational Phase LOPA gaps Decision Note (X060-A1-DCN-70010) may not be applicable.

Prior to upload to the Action Management System (eg Cority) recommendation due dates should be confirmed outside of workshop with actionee and relevant Team Lead, based on scope completion dates, noting that all recommendations should typically be addressed prior to implementation.

Priority	Due Date	Finding Owner	Approver	Tech Safety Verifier
P3	Various	Discipline Team Lead	Discipline TA-2	Tech Safety TA-2

Actionee is typically as per LOPA record, however, can be reassigned by relevant Team Lead.

For recommendation allocated to Operations personnel (eg procedure updates) the Approver is Process Engineer TA-2.

Tech Safety Verifiers are aligned to Action Management Procedure (0000-A0-PRC-70007).