400 Series:
Process Safety

IPL/SIL Assessment Methodology

Standard Number: IVL EHS-406
Version: 2.0
Issue / Revision Date: 17 March 2025

Global Environmental, Health and Safety
Indorama Ventures

Note: The original of this document was distributed in electronic form. All printed copies are uncontrolled documents and may not be the most current.

Table of Contents

1. Purpose

This standard establishes Indorama Ventures minimum requirements for the process to identify mechanical, administrative, instrumented, and other types of Independent Protection Layers (IPLs), as well as the Process Hazard Analysis (PHA) Typical Initiating Cause Frequencies, the Risk Reduction Factor credits of an IPL, the IPL/SIL (Safety Integrity Level) assessment methodology, and the reliability required of the Safety Instrumented Functions (SIFs) to bring the frequency of identified potential process related incidents into compliance with the Indorama Ventures risk criteria as defined in the IVL EHS-208, Risk Management Standard and Matrix.

2. Scope

This standard applies to all Indorama Ventures owned/operated sites as defined in IVL EHS-417 Process Safety Management Applicability Standard. This standard does not apply to joint ventures (JVs) in which Indorama Ventures is a minority owner, nor to third-party warehouses and tollers, unless specifically requested by the related Segment EHS Leader.

For the purpose of this standard, the term ‘EHS’ includes process safety, transportation, and security, as well as environmental, health and safety.

The standard does not address the design and specification, or integrity management of Safety Instrumented Functions (SIF) and Safety Instrumented Systems (SIS). These will be addressed in the IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips) standard to be released at a future date.

This standard must be implemented by each site. Until implementation of this standard is complete, each site must at a minimum be in compliance with the local applicable regulations.

3. Responsibilities

Following is an overview of key responsibilities for this standard. Additional responsibilities, as applicable, are included in Section 4, Requirements.

3.1. Corporate EHS

3.1.1. Provide ongoing technical assistance related to this standard.

3.1.2. Periodically audit sites to determine compliance with this standard.

3.1.3. Review, update and communicate to all Indorama Ventures sites any updates or changes to this standard and associated documents and tools.

3.1.4. Periodically review this standard to ensure its continuing adequacy and suitability to Indorama Ventures operations.

3.1.5. Ensure this standard is consistently implemented from site-to-site within Indorama Ventures.

3.1.6. Communicate, as applicable, any lessons learned as a result of best practices identified or any non-compliances associated with implementation of this standard.

3.2. Site Head or Designee

3.2.1. Ensure implementation of and compliance with this standard including that it is adhered to and a site-specific program is developed so all personnel receive the proper training, resources, and communications.

3.2.2. Assist with the implementation of the site-specific program; in particular:

- Be thoroughly familiar with the requirements of this standard, the site-specific program, and any associated procedures and work practices.
- Provide support, resources and training needed to carry out the requirements of this standard and the site-specific program.
- Ensure required records are kept current, up to date, and maintained on file.
- Ensure compliance with site-specific program by employees and contractors (as applicable).

3.2.3. Appoint the IPL/SIL Assessment Leader and Responsible Engineer for existing process systems, as needed.

3.2.4. Ensure the Responsible Instrument Engineer or designee performs a post-analysis review of the assumptions of the IPL/SIL Assessment and oversees the assessment through into design. This will be addressed further in the IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips) standard to be released at a future date.

3.3. Segment EHS

3.3.1. Ensure that any site or local standard or procedure related to the same topic follows the corporate requirements at minimum.

3.3.2. Support the sites on any technical point related to the standard, including implementation.

3.3.3. Periodically evaluate sites' level of compliance with this standard

3.4. Project Manager for Capital Projects

3.4.1. Appoint the IPL/SIL Assessment Leader and Responsible Project Engineer(s).

3.4.2. Ensure the Responsible Instrument Engineer or designee performs a post-analysis review of the assumptions of the SIL Assessment and oversees the assessment through into design. This will be addressed further in the IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips) standard to be released at a future date.

3.5. IPL/SIL Assessment Leader

3.5.1. Select the appropriate IPL/SIL Assessment methodology described in Step 3 of Attachment B and ensure that the chosen methodology is applied appropriately.

3.5.2. Ensure the IPL/SIL Assessment is in compliance with applicable legislative and regulatory requirements.

3.5.3. Approve the final IPL/SIL Assessment documentation.

3.5.4. Other responsibilities listed in Attachment B, Section 3.4.

3.6. Program Owner

3.6.1. Be thoroughly familiar with the requirements of this standard and local regulatory requirements.

3.6.2. Develop and implement a site-specific program that meets the requirements of this standard and any local/regional regulatory requirements.

3.6.3. Periodically review and monitor for compliance with the requirements of this standard, and per local regulatory requirements, at least every five (5) years.

3.6.4. Develop an action plan to correct any non-conformance with local regulatory or Indorama Ventures requirements.

3.7. Employees and Contractors

3.7.1. All affected personnel must understand and follow the requirements of the site-specific program including being aware of and trained on, as applicable, the requirements associated with this standard.

3.7.2. Individuals experienced in the process under evaluation (e.g., operations specialist, maintenance associate, process engineer) shall be involved in the IPL/SIL assessment as requested, such as:

- Participating as technical resources when requested.
- Being aware of the IPL/SIL Assessment for the areas where they work, as applicable, and where to locate them (e.g., within PHA documentation).

3.8. In addition to the roles and responsibilities detailed above, the site-specific program must define and document the roles and responsibilities for all personnel who play a role in implementing the site-specific program, at a minimum:

- Supervisors
- Engineering and Maintenance
- EHS Personnel

a. Other applicable functions, as staffed at individual site level

4. Requirements

The site shall establish and maintain a site-specific program for conducting IPL/SIL assessments to determine the required IPLs and SIL targets necessary to be in place as independent protection layers to provide safe operations per the risk reduction requirements in the IVL EHS-208 Risk Management Standard and Matrix.

4.1. The IPL/SIL Assessments shall follow the methodology, or equivalent methodology, defined in Attachment B.

4.2. The Process Hazard Analysis (PHA) process, as described in the IVL EHS-403 Process Hazard Identification and Analysis standard, is established to identify all safeguards required for all process scenarios with the potential for a hazardous event of any consequence.

4.3. The IPL/SIL Assessment process, as described in this standard, is a detailed analysis that shall be completed for all PHA process scenarios identified with the potential for a hazardous event with a Severity Category of A thru F (as defined in the Risk Management Standard and Matrix, IVL EHS-208).

4.4. Clarification and guidance on how to conduct an IPL/SIL Assessment using the LOPA methodology is referenced in Attachment C.

4.5. Clarification and guidance on how to conduct an IPL/SIL Assessment using the Numerical Hazard Analysis methodology is referenced in Attachment D.

4.6. IPL/SIL Assessment Reports shall be maintained for the life of the asset.

4.7. IPL/SIL Assessment Reports shall be maintained as current through the Management of Change process (IVL EHS-204).

4.8. An IPL/SIL Assessment team, consisting of individuals experienced in the process that is under evaluation, and led by a competent IPL/SIL Assessment Leader shall carry out the IPL/SIL Assessment. The team shall consist of at least two individuals.

4.9. An IPL/SIL Assessment Leader, in consultation with competent process representatives, may choose to use either the Layers of Protection Analysis (LOPA) or Numerical Hazard Analysis methodologies. The choice of methodologies shall be at the discretion of the IPL/SIL Assessment Leader based on the process complexity and hazard levels of the process.

4.10. IPL/SIL Assessments shall be performed with reference to the Risk Management Standard and Matrix, IVL EHS-208.

4.11. The IPL/SIL Assessment documentation shall be comprehensive in nature (see section B.16 for documentation guidance), support the numeric values integrated into the analysis, and contain the minimum content identified in Attachment B.

4.12. All mechanical, instrument, alarm, or administrative system credited as an IPL to meet the target risk criteria for Severity of A thru F events shall be considered EHS Critical IPLs per the IVL EHS-405 EHS Criticality standard, and shall meet the additional requirements of the other IVL EHS standards.

4.13. All Enabling Events (EEs) and Conditional Modifiers (CMs) credited with risk reduction, or frequency modification, on Severity A thru F events shall be considered EHS Critical enabling events or conditional modifiers shall be considered EHS Critical per the IVL EHS-405 EHS Criticality standard, and shall meet the additional requirements of the other IVL EHS standards.

4.14. Consequences shall be considered with and without Consequence Mitigation Systems (CMSs) during the IPL/SIL Assessment. If a secondary hazard results from activation of a CMS, it shall be analyzed as a separate hazard event scenario.

4.15. Timing

4.15.1. For capital projects, the IPL/SIL Assessment shall be performed during the design phase. An IPL/SIL Assessment can be initiated from a modification to existing sites as part of a Management of Change, IVL EHS-204.

4.15.2. An IPL/SIL Assessment can also be initiated from an initial or five-year revalidated PHA per the Process Hazard Analysis Standard, IVL EHS-403.

4.15.3. The IPL/SIL Assessment for the process shall be revalidated at least every five (5) years.

4.16. Clarifications

4.16.1. Process hazard event scenarios may be developed in PHAs (see IVL EHS-403), incident investigations (see IVL EHS-106), design reviews, or other hazard identification forums.

4.16.2. During an IPL/SIL Assessment, there is a possibility that a SIF may not be required if adequate risk reduction is met by physical IPLs, CMSs, etc.

4.16.3. The results of an IPL/SIL Assessment are highly dependent on the team's understanding of how a hazard event scenario propagates and the risk ranking typically developed in the PHA. Thus, it is general practice to closely align the scheduled performance or revalidation of an IPL/SIL Assessment with the related PHA.

5. Training

Training requirements must be defined in the site-specific program. At a minimum, all training must be documented with the training date, the names of employees trained, the names of the trainer(s), the content of the training (or reference to content) and other site-specific/business segment requirements, when applicable.

5.1. Initial

Training on the requirements of this standard and the site-specific program must be provided to Indorama Ventures personnel based on their relevant responsibilities and shall be provided in the local language. At a minimum, personnel and/or management with direct responsibilities for this standard and site-specific program must be trained prior to conducting activities associated with the site-specific program.

The IPL/SIL Assessment Leader must be trained in leading IPL/SIL assessments and in the specific methodologies being used.

5.2. Refresher

Refresher training shall be provided periodically according to the requirements of this standard, the site-specific program, and any local legal requirements, at appropriate intervals (e.g., changes to regulatory requirements), or at least once every three (3) years.

6. Recordkeeping

Records associated with the site-specific program and IPL/SIL assessments must be controlled and retained in accordance with regulatory or site business segment record retention requirements, whichever is more stringent. IPL/SIL assessment reports relevant to the site shall be maintained for the life of the asset. Examples of records to be maintained include but may not be limited to completed IPL/SIL assessment reports and any associated information/documentation referenced.

7. References

7.1. IVL EHS-106, Incident Investigation

7.2. IVL EHS-204, Management of Change

7.3. IVL EHS-208, Risk Management Standard and Matrix

7.4. IVL EHS-403, Process Hazard Analysis

7.5. IVL EHS-405, EHS Criticality Assessment

7.6. IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips)

7.7. IVL EHS-417, Process Safety Management Applicability

7.8. IVL EHSF-406-03, Independent Protection Layer Verification and Integrity Assessment

7.9. IEC 61508 Functional safety of electrical / electronic / programmable electronic safety related systems

7.10. IEC 61511 Functional safety - Safety instrumented systems for the process industry sector

7.11. ANSI / ISA 61511-1-2018 Functional Safety: Safety Instrumented Systems for the Process Industry Sector

7.12. ANSI / ISA 84.91.01-2021 Identification and Mechanical Integrity of Process Safety Controls, Alarms, and Interlocks in the Process Industry Sector

7.13. CCPS / AIChE, Layer of Protection Analysis – Simplified Process Risk Assessment

7.14. CCPS / AIChE, Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis

7.15. Guidelines for Quantitative Risk Assessment, CPR-18E, ISBN 90-12-08796-1

7.16. Guidelines for Safe and Reliable Instrumented Protective Systems, Center for Chemical Process Safety, ISBN 9780471-97940-1.

7.17. Process Safety Leadership Group 2009 Report entitled, Safety and Environmental Standards for Fuel Storage Sites, Annex 5, ISBN 978 0 7176 6386 6.

8. Terms and Definitions

See IVL EHS Glossary and Attachment A

9. Revision History

Version	Date	Summary of Update	Owner	Approver	Next Review Date
Original	18 April 2022	Initial Release	Chad Wyble, Global Process Safety Program Director	Todd Hogue, VP, Global Head of EH&S	18 April 2025
1.0	09 August 2024	Updated implementation timeframe (Section 2) and Responsibilities (Section 3); made minor editorial updates.	Chad Wyble, Global Process Safety Program Director	Todd Hogue, VP, Global Head of EH&S	09 August 2029
2.0	17 March 2025	Updated wording about BPCS IPL being in automatic mode. See C.7.3.3.e, Table C-5, Table C-7, and Figure C-3. Added Overpressure Consequences Tables to Attachment C. Modified wording in Sections C.5.7.1 thru C.5.7.3.	Chad Wyble, Global Process Safety Program Director	Todd Hogue, VP, Global Head of EH&S	17 March 2030

Attachment A: Definitions and Glossary

A.1 Availability

The probability that a system will be able to perform its designated function when required for use. Another term frequently used is Probability of Failure on Demand Average (PFDavg). Availability = (1 - PFDavg).

A.2 Basic Process Control System (BPCS)

The control equipment and system is intended to regulate normal production functions, including sensors, logic solvers, final elements, communications, power supply, and human machine interface. The BPCS may be a distributed control system (DCS), programmable logic controller (PLC), or other type system used for normal process control.

A.3 Bypass

A defined action that is taken to defeat an IPL in order to test or perform maintenance on the IPL devices.

A.4 Common Cause Failure

A single source of failure that causes multiple elements to fail. (The single source can be internal or external to the process or system.)

A.5 Common Mode Failure

Failure of two or more channels or items in the same way, causing the same erroneous result.

A.6 Communication Bus

The I/O communication bus is the communication network between the controllers and their respective I/O modules. If safety critical signals of concern are between the controller and the I/O modules, then the I/O bus needs to be validated as independent.

The Control LAN communication bus is the communication network between two or more controllers and between the controllers and the operator stations for process and alarm data and operator input from the human machine interface. If the safety critical signal is related to an alarm with operator action, then the Control LAN needs to be validated as independent.

A.7 Consequence Mitigation System (CMS)

Any independent means that reduces the severity or frequency of the escalation of a process related incident. (Note: it could be a pressure relief device, a gas detection system that prompts an administrative procedure such as an emergency plan or engineered systems such as a storage tank bund / dyke).

A.8 Conditional Modifiers

One of several possible probabilities included in scenario risk calculations, generally when risk criteria endpoints are expressed in impact terms (e.g., fatalities) instead of in primary loss event terms (e.g., release, vessel rupture). Conditional modifiers include but are not limited to probability of a hazardous atmosphere, probability of ignition, probability of explosion, probability of personnel presence, and probability of injury or fatality. See Attachment C, section C.5.4.3 for additional conditional modifier information.

A.9 Dependency (Failure)

There are two different types of dependency:

- Functional dependency:

A single failure or condition which results, in turn, in the coincidental failure of multiple systems (e.g. electrical supply failure, or instrument air failure, failure of an item common to control and protection or to different channels of the protective system (e.g., blockage of a pressure measurement connection common to control and trip systems).

- Classic dependency:

  The failure of multiple items of equipment due to a common cause or in a common mode, e.g., common maintenance error, vibration, high temperature, faulty batch of equipment.

A.10 Decommissioning

The permanent removal of a complete Safety Instrumented System (SIS) from active service.

A.11 Distributed Control System (DCS)

A multiple input-multiple output control system used for basic process control that is normally used as the BPCS.

A.12 Emergency Shutdown System (ESS) or Emergency Shutdown Device (ESD)

A dedicated system either computer controlled or hard-wired that is independent of the BPCS and used to bring a process to a safe state in an emergency situation.

A.13 Enabling Events or Conditions

These are conditions or events that are necessary for the Initiating Cause to start to propagate towards the final undesired consequence of the hazard event scenario. Enabling events may consist of operating mode (start-up, shutdown, maintenance), operating sequence (specific process phase or step), environmental condition (external temperature), or other basic failures (that are not considered by the team to be protection layers).

A.14 External Risk Reduction

Measures to reduce or mitigate the risks, which are separate and distinct from the SIS or IPL. Examples include a drain system, fire wall, or bund.

A.15 Fail-Safe

A concept that defines the failure direction of a component/Safety Function as a result of specific detected failure. The “fail safe” direction is toward a safer or less hazardous condition.

A.16 Final Element

Part of a safety instrumented system which implements the physical action necessary to achieve a safe state.

A.17 Independent Protection Layer (IPL)

Any independent means that reduces the frequency, but not the severity, of a process related incident by control or prevention means. (Note: it could be a process engineering mechanism such as the size of vessels containing hazardous materials, a mechanical engineering mechanism such as a relief valve or a safety instrumented system. These responses may be automated or initiated by human actions).

A.18 Initiating Cause

The Initiating Cause is the primary failure that occurs and starts the propagation of the incident that leads to the hazard event scenario. Initiating Causes can include equipment failures, procedural errors, instrumentation failures, human errors, etc.

A.19 Inherent / Intrinsic Safety

This is the concept that the process is designed to reduce the potential for hazardous incidents. This typically requires chemical, inventory, process design changes or equipment modifications. Inherent/ Intrinsic Safety can minimize or eliminate the need for IPLs. (This is also referred to as “inherently safer or intrinsic safety”.)

A.20 Logic Solver

That portion of the SIS that performs the logic function.

A.21 Mitigation

An action that reduces the consequence(s) of a hazardous event.

A.22 Probability of Failure on Demand (PFD)

A value that indicates the probability of a function failing to respond to a demand at a specific instance in time – the probability will vary from a value of zero just after a successful proof test to a highest value just before the next proof test.

A.23 Probability of Failure on Demand Average (PFDavg)

The average probability of a function failing to respond to a demand.

A.24 Process Hazard Analysis (PHA)

A PHA is an organized systematic effort to identify and analyze the significance of potential hazards associated with the processing or handling of hazardous materials.

A.25 Programmable Logic Controller (PLC)

A computer, designed for an industrial environment, for implementing specific functions such as logic, sequencing, timing, counting and control.

A.26 Risk Reduction Factor (RRF)

A measure of how much the independent protection layer (IPL) reduces the frequency of the hazard event scenario. It is calculated based on the average Probability of Failure on Demand (PFDavg) or located in Indorama Ventures recognized LOPA table data for the IPL. The risk reduction factor is equal to the inverse of the PFDavg. The RRF should be included in the recommendation or in the IPL list when SIL credit is taken in the PHA.

A.27 Safety Function

Function to be implemented by a SIS, other technology safety related system, or external risk reduction sites, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event.

A.28 Safety Instrumented Function (SIF)

A combination of sensors, the logic solver and final elements with a specified safety integrity level that detects an out-of-limit (abnormal) condition and brings the process to a functionally safe state without human intervention, or by initiating a trained operator response to an alarm. The SIF:

- protects against a specific hazard,
- performs a specific safety function,
- has a defined range or probability of failure on demand related to a specific SIL range, and
- is independent from the initiating event and other protection or mitigation systems.

A.29 Safety Instrumented Systems (SIS)

Instrumented system used to implement one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), Logic Solver(s), and final elements(s). This can include either safety instrumented control functions or safety instrumented protection functions and may or may not include software.

A.30 Safety Integrity Level (SIL)

Discrete level (one out of three) for specifying the safety integrity requirements of the Safety Instrumented Functions to be allocated to the safety instrumented systems. Safety integrity level 3 has the highest level of safety integrity; safety integrity level 1 has the lowest. The SIL is the required integrity of a Safety Instrumented Function (SIF) necessary to control and prevent the propagation of a process safety event, and is determined by the range of Probability of Failure on Demand Average (PFDavg) for the SIF:

SIL	PFDavg	RRF	Availability
1	≥ 0.01 to < 0.1	>10 to ≤ 100	>90 to ≤ 99%
2	≥ 0.001 to < 0.01	>100 to ≤ 1000	>99 to ≤ 99.9%
3	≥ 0.0001 to < 0.001	>1000 to ≤ 10000	>99.9 to ≤ 99.99%

A.31 Worst Credible Hazard Event Scenario

The term “worst credible” refers to a hazard event scenario (process related incident) where the quantity and condition (e.g., pressure, temperature, composition) of a hazardous chemical released takes into account the process conditions and passive mitigation measures.

Worst credible hazard event scenarios are often derived from a review of process hazard analyses and related process incident history. Examples of several worst credible hazard event scenarios include: overfill of a tank at the maximum fill rate resulting from a malfunctioned open feed valve; pipe rupture of a compressed gas line as a result of corrosion under insulation; and gasket leak on start-up following a maintenance turnaround.

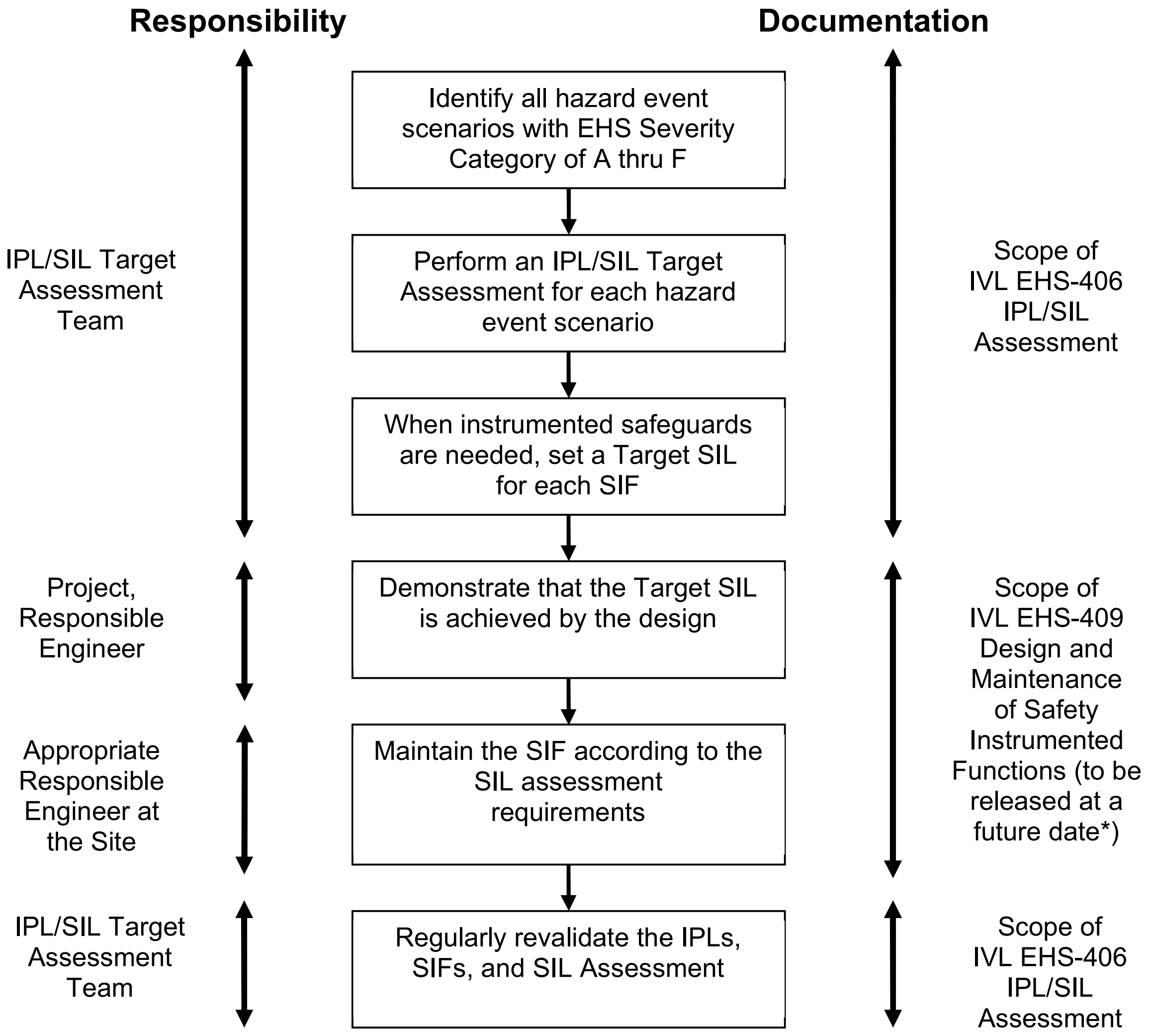
One other aspect to be taken into account is the credibility of a minor event escalating, over time, to a much more significant event when it is very visible and apparent that the event is taking place. For example, if an initiating cause will result in a process upset in upstream and downstream equipment that will be clearly apparent to operators or if smoke associated with a small fire will obviously be observed, then the likelihood of the event propagating may be very low.

Attachment B: IPL/SIL Assessment Methodology

B.1 Overview

B.1.1 This Attachment explains how an IPL/SIL Assessment should be performed. Figure B-1 shows the lifecycle of the process and how the IPL/SIL Assessment interfaces with the later stages of the SIL assessment process, particularly the demonstration of achieved SIL that will be detailed in standard IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips) when it is released at a future date.

FIGURE B-1 IPL/SIL ASSESSMENT LIFECYCLE FLOWCHART


Responsibility
Documentation
Identify all hazard event scenarios with EHS Severity Category of A thru F
Perform an IPL/SIL Target Assessment for each hazard event scenario
When instrumented safeguards are needed, set a Target SIL for each SIF
Demonstrate that the Target SIL is achieved by the design
Maintain the SIF according to the SIL assessment requirements
Regularly revalidate the IPLs, SIFs, and SIL Assessment
IPL/SIL Target Assessment Team
Project, Responsible Engineer
Appropriate Responsible Engineer at the Site
IPL/SIL Target Assessment Team
Scope of IVL EHS-406 IPL/SIL Assessment
Scope of IVL EHS-409 Design and Maintenance of Safety Instrumented Functions (to be released at a future date*)
Scope of IVL EHS-406 IPL/SIL Assessment

* In the interim, follow ANSI / ISA 61511-1-2018 Functional Safety: Safety Instrumented Systems for the Process Industry Sector

B.1.2 A more detailed description of the IPL/SIL Assessment methodology is provided in Figures B-2 and B-3.

B.2 Objectives

B.2.1 The objective of the IPL/SIL Assessment is to ensure all Independent Protection Layers (IPLs), Consequence Mitigation Systems (CMSs) and Safety Instrumented Functions (SIFs) are identified and that they achieve a level of reliability that is appropriate to the risk of the hazard event scenarios for which they provide protection.

B.3 Team Selection

B.3.1 Generally, the IPL/SIL Assessment will be undertaken as part of the Process Hazard Analysis (IVL EHS-403) study, a Process Hazard Analysis (PHA) Revalidation study (IVL EHS-403) or a Management of Change PHA (IVL EHS-204). Ideally the team which performs these studies should also perform the IPL/SIL Assessment.

B.3.2 The composition of an IPL/SIL Assessment Team shall consist of at least two competent individuals consulting with the Leader. Suggested personnel are below:

IPL/SIL Assessment Leader (Required)

Process Engineer

Operations Specialist

Functional Safety Engineer/Specialist

Other possible attendees may be:

a. Process Chemist
b. Maintenance Engineer
c. Project Manager
d. Functional Equipment Specialist
e. EHS/PSM Specialist
f. Vendor Representative

B.3.3 One person may perform more than one role within the team. The members of the team shall be competent individuals knowledgeable in the IPL/SIL Assessment methodology, the process under evaluation and the instrumented protective systems in place. Further details on the roles follow below.

B.3.4 IPL/SIL Assessment Leader

B.3.4.1 The role of the IPL/SIL Assessment Leader shall be to:

a. Control the meeting.
b. Ensure that the team composition is appropriate.
c. Identify the hazard event scenarios through reference to the Process Hazard Analysis (PHA) or additional consideration of the process.
d. Assist the team in estimating initiating event frequencies (demands).
e. Assist the team in determining the consequence categories.
f. Assist the team in agreeing on appropriate failure probabilities.
g. Record the minutes of the meeting or assign this role to another.
h. Direct the team on the appropriateness of assumptions made regarding IPL and CMS credits and Risk Reduction Factors and agree whether they are acceptable.

i. Direct the team in the identification of items in which the SIF is inadequate and generate a formal recommendation for post study verification or redesign.

j. Prepare, plan and generate the IPL/SIL Assessment Report.

k. Approve, in consultation with the team, the final IPL/SIL Assessment Report.

B.3.4.2 To perform this role, the IPL/SIL Assessment Leader shall be a competent in the methodology being used.

a. The IPL/SIL Assessment methodologies described in Attachments C and D range from screening techniques to Numerical Hazard Analysis. It is clear that there is a need for judgement as to the necessary skills required for each level of assessment. It is essential that the person leading an assessment be fully competent in the methodology used, as it is very difficult to check assessments in an effective manner afterwards.

B.3.5 Process Engineer

B.3.5.1 The Process Engineer should provide knowledge of the process design in terms of hardware and reaction chemistry. The Process Engineer should be experienced in all aspects of the process being studied. It may be appropriate to use a number of Process Engineers if the SIL assessment spreads across a number of process areas.

B.3.6 Operations Specialist

B.3.6.1 The Operations Specialist should bring detailed knowledge of the plant operations, in particular experience of site process related incidents, near misses and failures, detailed knowledge of operator competencies, and likelihood of errors and response to alarms and developing situations. The Operations Specialist should also contribute a good understanding of the operating procedures and practices and process under consideration and good judgement of the consequence of any event.

B.3.7 Functional Safety Engineer/Specialist

B.3.7.1 The Functional Safety Engineer/Specialist should have knowledge of the SIFs being considered.

B.3.7.2 For an existing system, details of items such as the sensor and final element and also the testing frequency of the system may be available. However, this information is not essential for the assessment. The Functional Safety Engineer/Specialist should also bring knowledge of all the other Safety Instrumented Systems including all trips and alarms, interlocks, thermal overloads, which may be considered to provide risk reduction in relation to the SIFs being assessed at the meeting.

B.3.7.3 An important aspect of the Functional Safety Engineer/Specialist’s role is their good understanding of the reasons behind a specific SIL assessment such that they can convey and explain it to colleagues who will be calculating the SIL achieved by the installed system. However, the key contribution of the Functional Safety Engineer/Specialist’s role is to provide understanding of the relevant control functions whose failure could cause a demand on the SIF being assessed.

B.3.8 Process Chemist

B.3.8.1 Where the process involves the potential for a reaction exotherm or runaway, the expertise of a process chemist would help clarify what conditions would lead to an exotherm and what conditions would not be significant.

B.3.8.2 The process chemist should provide detailed knowledge where the process chemistry is significant in relation to potential hazard event scenarios.

B.3.9 Maintenance Engineer

B.3.9.1 Should provide knowledge of the performance of equipment on an existing plant including an understanding of the failures, and their frequencies, that have occurred.

B.3.10 Project Manager

B.3.10.1 In the case of a new plant the Project Manager may be able to contribute their wide knowledge of all aspects of the project design, particularly in functional engineering areas not represented in the team.

B.3.11 Functional Equipment Specialist

B.3.11.1 Depending upon the nature of the equipment being studied it may be appropriate to have functional expertise present. For example, a rotating machinery engineer should be considered if large compressors are involved, or a civil engineer should be considered if secondary containment, drains and sumps play an important part in the provision of protection layers.

B.3.12 Vendor Representative

B.3.12.1 The need for the presence of a Vendor Representative depends upon the type and age of the plant being considered.

B.3.12.2 If the equipment has been in operation for a number of years, it is likely that the site team fully understands all aspects of its operation and maintenance and there is no need for a Vendor Representative. If the SIFs under review are associated with a major modification to a plant, for example the installation of a new boiler, then a representative of the boiler vendor should attend.

B.4 Timing

B.4.1 The exact timing of the IPL/SIL Assessment will depend upon the size and complexity of the process under evaluation and the composition of the team. A few options are recommended:

B.4.1.1 If the appropriate complement of team members is represented in the PHA team, time could be set aside at the end of each PHA study day during which the team could undertake the IPL/SIL Assessment for those SIFs identified during the day.

B.4.1.2 If the PHA process is scheduled to last in excess of a week, it may be more appropriate to set aside additional time to perform the IPL/SIL Assessment shortly after the completion of the PHA.

B.4.1.3 If the process is large or complex, it may be beneficial to perform the IPL/SIL Assessment after each hazard event scenario or node is completed in the PHA.

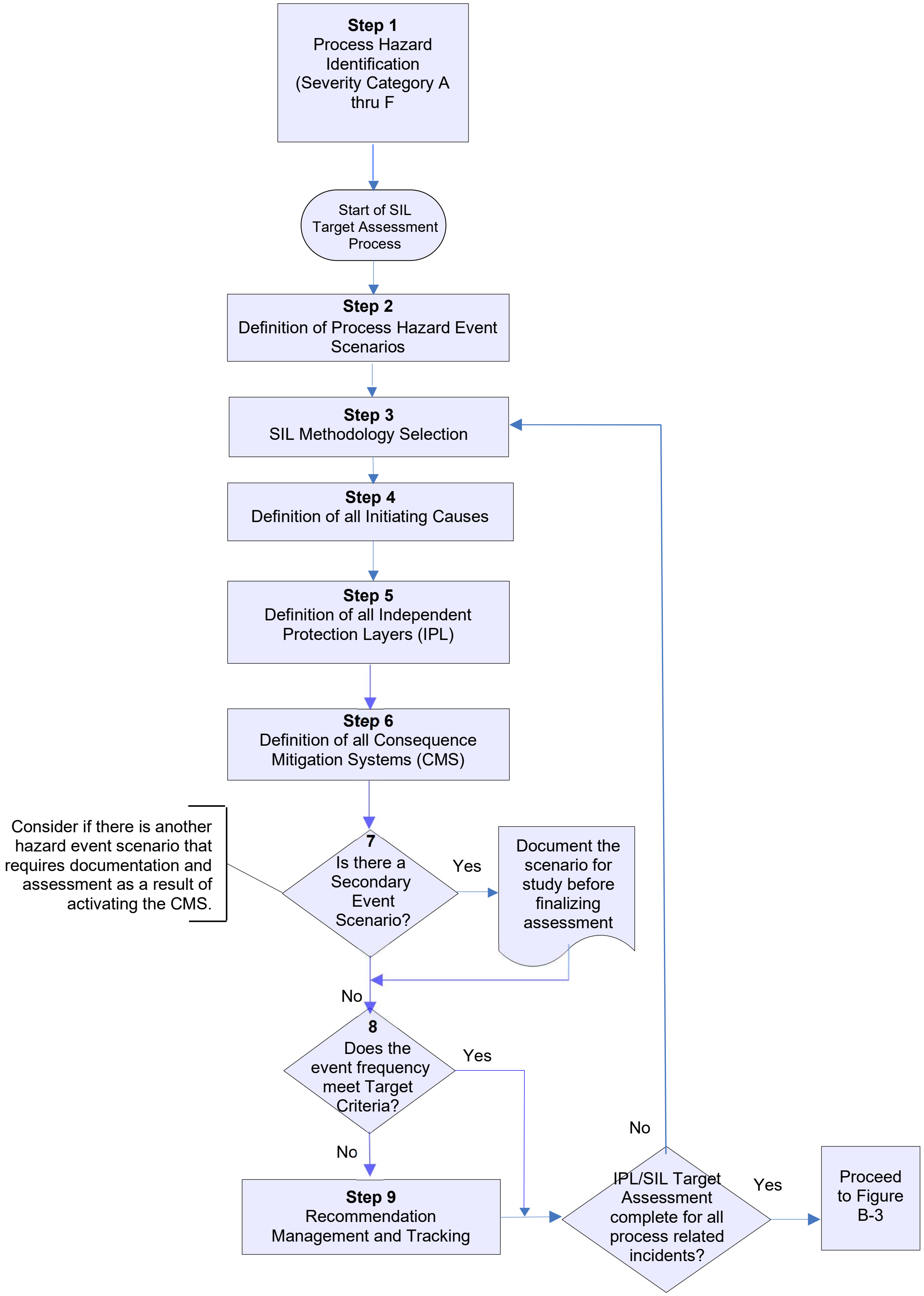
B.5 IPL/SIL Assessment Methodology

B.5.1 The IPL/SIL Assessment is the process of defining the process safety related hazard event scenarios, identifying the protection that mitigates against these events (including any SIFs), and determining what Average Probability of Failure on Demand (PFDavg) or SIL is required to reduce the frequency of the hazard event scenario to an acceptable level.

B.5.2 The basis for any IPL/SIL Assessment is the identification of potential process safety related hazard event scenarios. Once an event scenario has been identified, an assessment of the need for a SIF can be made and the required SIL for that function can be calculated.

B.5.3 The methodology is summarized in Figure B-2.

FIGURE B-2 – IPL/SIL ASSESSMENT FLOWCHART


Step 1
Process Hazard Identification (Severity Category A thru F
Start of SIL Target Assessment Process
Step 2
Definition of Process Hazard Event Scenarios
Step 3
SIL Methodology Selection
Step 4
Definition of all Initiating Causes
Step 5
Definition of all Independent Protection Layers (IPL)
Step 6
Definition of all Consequence Mitigation Systems (CMS)
Consider if there is another hazard event scenario that requires documentation and assessment as a result of activating the CMS.
7
Is there a Secondary Event Scenario?
Yes
Document the scenario for study before finalizing assessment
No
8
Does the event frequency meet Target Criteria?
Yes
No
Step 9
Recommendation Management and Tracking
No
IPL/SIL Target Assessment complete for all process related incidents?
Yes
Proceed to Figure B-3

B.6 Step 1: Process Hazard Identification

B.6.1 Process hazards are most commonly identified during:

B.6.1.1 Preliminary PHA (Hazard Study 2) for the assessment of new plants and major modifications. Process safety related hazard event scenarios identified at this stage are checked during the Detailed PHA (Hazard Study 3) (see IVL EHS-403).

B.6.1.2 PHA Revalidation (see IVL EHS-403).

B.6.1.3 Management of Change (IVL EHS-204) for smaller modifications.

B.6.2 Any of these standards may identify the potential need for a new SIS, SIF, or a new demand on an existing SIS or SIF.

B.6.3 When performing a PHA study, consideration should be given to gathering information that will be valuable in the IPL/SIL Assessment.

B.6.4 Examples of such information are listed below:

a. Comprehensive identification of all demands, i.e., initiating causes and frequency of demand
b. Demand rates.
c. Comprehensive list of all IPLs.
d. Comprehensive list of all CMSs.
e. Equipment failure rates.
f. Assessment of human factors that contribute to either demand or protection.
g. Assessment of common cause failure mechanisms.
h. Assessment of common mode failure mechanisms.

B.7 Step 2: Definition of Process Safety Hazard Event Scenarios

B.7.1 The purpose of this step is to take the information provided by the PHA and determine and document the following:

a. A description of each identified process safety hazard event scenario and the deviations that contribute to it, including human factors and consideration of the possible different modes of operation, such as normal operation, start-up, shutdown, maintenance, process upset, and emergency shutdown.
b. A description of the consequences of each identified hazard event scenario. Document determination of the consequence Severity Category for each hazard event scenario referencing the risk matrix in Risk Management Standard and Matrix, IVL EHS-208.
c. A description of the measures taken to reduce or eliminate hazards or risk.

B.8 Step 3: SIL Methodology Selection

B.8.1 There are two methodologies for determining the IPL/SIL Target. In order of increasing sophistication, they are:

a. Layer of Protection Analysis (LOPA)
b. Numerical Hazard Analysis (NHA)

B.8.2 The choice of methodology will be at the discretion of the IPL/SIL Assessment Leader in consultation with competent process representatives based on the complexity and hazards of the process.

B.8.3 Layer of Protection Analysis (LOPA) is a semi-quantitative assessment tool, which strikes a balance between improved accuracy and documentation detail, and the time required for the analysis. It would typically be the methodology of choice for use in conjunction with PHAs (Hazard Studies), or process changes implemented under Management of Change.

B.8.4 The Layer of Protection Analysis methodology described in Attachment C represents the minimum requirements.

B.8.5 Numerical Hazard Analysis is a well-accepted methodology for quantifying the risk of an event occurring and is referenced in Attachment D.

B.9 Steps 4: Definition of All Initiating Causes

B.9.1 For each hazard event scenario, all initiating causes must be identified with the basis or justification for the initiating cause frequency fully documented.

B.10 Step 5: Definition of all Independent Protection Layers

B.10.1 Each IPL must be identified with the basis or justification for the risk reduction factor fully documented including supporting calculations.

B.11 Step 6: Definition of all Consequence Mitigation Systems

B.11.1 Each CMS must be identified with the basis or justification for the risk reduction factor fully documented including supporting calculations.

B.11.2 The IPL/SIL Assessment Team shall assess if there is a secondary hazard event scenario that requires a separate assessment as a result of a CMS functioning.

B.12 Step 7: Decision – Is there a secondary hazard event scenario that requires an assessment?

B.12.1 Yes – Document for evaluation after completion of the current assessment, and then proceed to Step 8.

B.12.2 No – proceed to Step 8.

B.13 Step 8: Does existing event frequency meet Target Criteria?

B.13.1 The IPL/SIL Assessment Leader shall calculate the existing event frequency with the proposed IPLs and compare it to the Target tolerable risk frequency criteria defined in the Risk Management Standard and Matrix, IVL EHS-208.

B.13.2 If the existing frequency does not meet the target criteria, the IPL/SIL Assessment team shall review the scenario for additional possible IPLs and/or assign the SIL level or average PFDavg necessary to meet the tolerable risk criteria.

B.13.3 If the outcome is a SIL 2 SIF or above, the IPL/SIL Assessment Leader should evaluate if there is a need for a more detailed quantitative analysis to validate the results.

B.13.4 If the existing frequency does meet the target criteria, the IPL/SIL Assessment for the particular hazard event scenario is complete and shall be documented (see Step 10).

B.14 Step 9: Recommendation Management and Tracking

B.14.1 The IPL/SIL Assessment Leader shall complete the following:

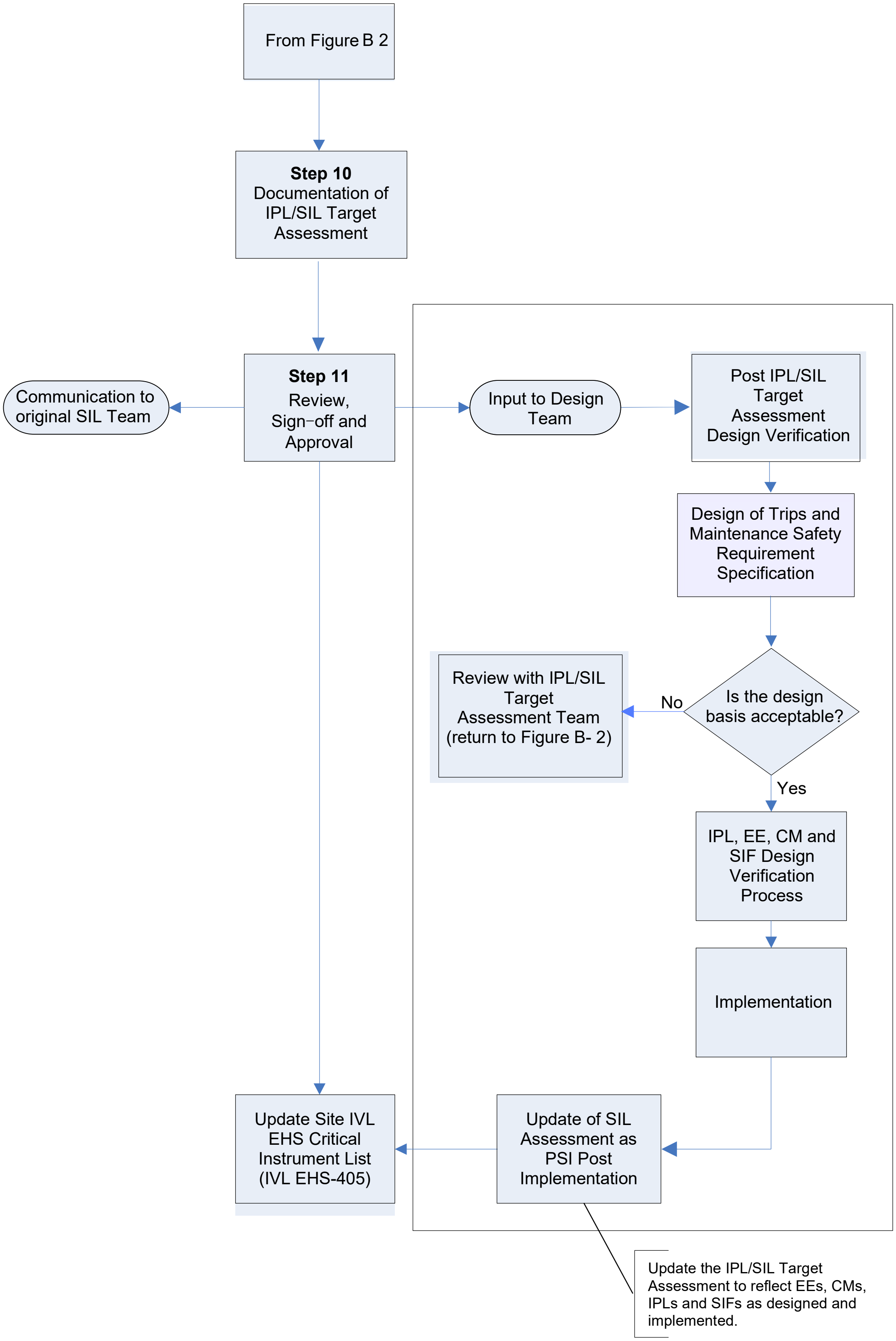
B.14.1.1 Document the gap identified in Step 8 and the action item(s) for the Responsible Instrument Engineer to undertake the post IPL/SIL Assessment design review and to identify the required design for closing the risk gap.

B.14.2 The Site Head / Project Manager is responsible for ensuring a management system is in place for actively addressing the recommendations, developing related action plans, and tracking those plans to completion in accordance with the Management of Recommendations / Actions Standard, IVL EHS-107.

B.15 Post IPL/SIL Assessment Interface

B.15.1 Following completion of the IPL/SIL Assessment, the interface with IPL, EE, CM, and SIF verification, achieved SIL determination and loop design is shown in Figure B-3.

FIGURE B-3 – POST IPL/SIL ASSESSMENT INTERFACE


From Figure B 2
Step 10
Documentation of IPL/SIL Target Assessment
Step 11
Review, Sign-off and Approval
Communication to original SIL Team
Input to Design Team
Post IPL/SIL Target Assessment Design Verification
Design of Trips and Maintenance Safety Requirement Specification
Is the design basis acceptable?
No
Review with IPL/SIL Target Assessment Team (return to Figure B- 2)
Yes
IPL, EE, CM and SIF Design Verification Process
Implementation
Update of SIL Assessment as PSI Post Implementation
Update Site IVL EHS Critical Instrument List (IVL EHS-405)
Update the IPL/SIL Target Assessment to reflect EEs, CMs, IPLs and SIFs as designed and implemented.

B.16 Step 10: Documentation of the IPL/SIL Assessment

B.16.1 The following are the minimum documentation requirements from the IPL/SIL Assessment:

a. Team composition
b. Hazard event scenario description.
c. Environmental and Safety consequences
d. Initiating Causes and associated frequencies
e. List of enabling events credited with frequency reduction
f. List of Independent Protection Layers and Conditional Modifiers
g. List of Consequence Mitigation Systems and associated justification
h. Target SIL
i. Target PFDavg with supporting rationale
j. SIF description
k. Risk-ranked recommendations for management review.

B.16.2 Typically, a ‘comments’ section should be used to record additional information raised during the IPL/SIL Assessment, that may be of use to the Responsible Instrument Engineer during detailed design of the SIS:

a. Proof test interval, e.g., plant shutdown frequency.
b. Effect of spurious trips.
c. Requirement for tight shut-off / fire safe valves.
d. SIF set point.
e. Speed of response.
f. Requirement for overrides.
g. Special maintenance requirements.
h. Non-SIS layers of protection.

B.17 The initial input for the Safety Requirement Specification (SRS), much of which is noted above in B.16.2, is often documented as an output from the IPL/SIL Assessment Team. See IVL EHS-409, which will be issued at a future date, for more details.

B.18 Step 11: Review and Sign-off and Approval

B.17.1 The IPL/SIL Assessment Leader should conduct a technical review to validate the appropriateness of the assumptions and recommendations for the IPL/SIL Assessment prior to seeking management approval.

B.17.2 After the technical review, the IPL/SIL Assessment report shall not be issued as final without a management review and approval. This should be performed by the IPL/SIL Assessment Leader in consultation with individuals competent in engineering and process operations, and with the appropriate manager.

B.17.3 The approval stage initiates the release of the IPL/SIL Assessment to allow a post assessment validation of the assumptions and development of the basis for detailed design as described in standard IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips) to be released at a future date.

B.17.4 Efficient handover of information from the IPL/SIL Assessment to the electrical/instrumentation function is critical to ensure the correct SIF definition is carried through into the final loop design.

B.17.5 Approval should also initiate an update to the EHS Critical List through the initiation of an MOC in accordance with IVL EHS-204. This is also revisited after the design process, reference Figure B-3.

B.17.6 It should be recognized there may be a requirement for the IPL/SIL Assessment to be revisited based on the findings of the post IPL/SIL Assessment design review. The IPL/SIL Assessment team may be asked to review their conclusions with input from the design review.

Attachment C: Layer of Protection Analysis (LOPA) Methodology and Tables

C.1 Introduction

C.1.1 The following outlines the use of the Layer of Protection Analysis (LOPA) methodology to perform an IPL/SIL Assessment which meets the requirements of this standard. Reference Figure C-1, the IPL Flowchart.

C.2 Purpose

C.2.1 LOPA is a semi-quantitative tool for analyzing and assessing risk. LOPA can effectively be used at any point in the life-cycle of a plant/unit, but is most frequently used during:

a. The design stage on new plants/units when the process flow diagram and the Piping and Instrumentation Diagrams (P&IDs) are essentially complete. LOPA is used to examine hazard event scenarios often generated by other process hazard analysis (PHA) tools, such as HAZOP, What-If, etc. (reference Process Hazard Analysis, IVL EHS-403) or as part of Safety Instrumented Function (SIF) design; and

b. Modifications to existing plants/units (i.e., Management of Change (MOC) Standard, IVL EHS-204).

C.3 General Requirements

C.3.1 LOPAs shall always be completed by a competent team. Team composition and competency shall be determined by the IPL/SIL Assessment Leader.

C.3.2 LOPA Study Team

C.3.2.1 Most LOPA Study Teams are similar to PHA Study Teams and consist of:

a. IPL/SIL Assessment Leader.
b. Project representative.
c. Site operations representative.
d. Process engineer
e. Process Control Engineer
f. Functional (design) engineer.
g. Specialists.

C.3.2.2 The ideal composition depends on the stage and project.

C.3.2.3 In cases where operations are to be performed for Indorama Ventures by other parties under contract there may be a substantial involvement of non-Indorama Ventures personnel in the team. However, in all Indorama Ventures projects, there should be an Indorama Ventures representative on the PHA and IPL/SIL Assessment study team.

C.4 Preparation by the IPL/SIL Assessment Leader

C.4.1 Referencing Figure C-1, review the information relating to process related incidents with consequences ranked as Severity Category A thru F. All of these incidents, or hazard event scenarios, shall be evaluated by the IPL/SIL Assessment Team.

C.4.2 Prepare a LOPA worksheet for each identified hazard event scenario consequence severity A thru F. An example worksheet is provided in Table C-1; IPL/SIL Assessment Worksheet. The actual worksheet used shall be at the discretion of the IPL/SIL Assessment Leader.

C.4.3 The remaining methodology references the example worksheet in Table C-1, to provide some clarity to the stepwise approach of performing a LOPA.

C.4.4.1 It is important to document basic information for each specific hazard event scenario. Referencing the top section of the example form in Table C-1, the following information should be documented:

a. Site/plant under evaluation.
b. Date the evaluation is completed by the team.
c. Event description with details based on the information available in the PHA and collected PSI. Documentation should address both the process deviation that could result in an incident, and the propagating events which could lead to loss of containment and/or equipment damage assuming no layers of protection.
d. Event type as it relates to safety or environment. The process may also be used for business related evaluations at the discretion of the business unit.
e. The required form or worksheet for each LOPA assessment.
f. Event consequences, severity category and target frequency (reference guidance below in C.4.4.2 and C.4.4.3).
g. Unique safety function loop number and trip action for each worksheet. Each hazard event scenario leading to an identified consequence should be assigned a unique safety function number.
h. Reference information such as a PHA and/or P&ID.
i. List of team members and the IPL/SIL Assessment Team Leader.

The IPL/SIL Assessment Leader completes this information based on the hazard event scenario information available in the PHA and preliminary discussions with team members. However, the information shall be reviewed and finalized by the team.

C.4.4.2 Consequence Assessment

a. The consequence is assessed according to standardized definitions in Attachment B, Table 1 Consequence Definitions[1], of Standard IVL EHS-208 Risk Management Standard and Matrix.
b. The hazard event scenario is assessed to determine, or validate, its ultimate consequence in terms of health, safety, and environmental impact. To evaluate the consequence and determine appropriate IPLs, the team may consider many factors including but not limited to the following:
    i. Normally trained operators or maintenance staff;
    ii. Normal personnel protection equipment is used;
    iii. Normal testing and inspection;
    iv. Normal cautions, signs, and warnings;
    v. Normal staffing in the unit, including operations, engineering, and maintenance staff;
    vi. The release scenario, including size and location;
    vii. Distance to ignition sources;
    viii. Rate of incident propagation as it applies to detection and egress;
    ix. Early warnings to field personnel, allowing possibility of personnel escape to safe area;
    x. General possibility of personnel escaping the incident due to size of incident;
    xi. Type and degree of equipment damage;
    xii. Sensitivity of the local environment to toxic release; and

[1] This table addresses Safety and Environmental Consequences.

xiii. The need for detailed modelling to support a more quantitative consequence assessment.

c. However, it is important that the team distinguish between the factors that relate to consequence and those that make the occurrence of that consequence less likely. In this step, the evaluation of the consequence severity level is the requirement – not whether it is likely.

d. If factors in paragraph b) above are applied to modify the severity category, the IPL/SIL Assessment Leader shall be careful to not give further risk reduction in the way of enabling events or other frequency reduction due to the limited personnel exposure. (i.e., no “double counting”).

e. There are other factors in paragraph b) above that relate to normal good practice. If any of these normal good practice factors do not apply, then the adverse impact of their absence should be considered. Lack of training may make error more likely or escape to a safe area less likely.

C.4.4.3 The Target Frequency is obtained from Standard IVL EHS-208, Risk Management Standard and Matrix, Attachment D “Target Frequencies for Quantitative Assessments”, Table 7.

C.4.4.4 Obtain a current set of the relevant P&IDs. Make copies of the P&IDs for use by the team during the study.

C.5 IPL/SIL Assessment Table Completion with the Team

C.5.1 The team members sign the sign-in sheet and take a set of P&IDs to establish a record of participation.

C.5.2 Referencing Figure C-2, the team is to review and modify the hazard event scenario description and related information as much as is needed for each scenario.

C.5.3 Inherent / Intrinsic Safety

C.5.3.1 At this point, the team understands the potential incident and how the incident could propagate without considering any IPLs. Inherent / Intrinsic Safety should now be evaluated. Although inherently safer design often requires chemical, inventory, process design changes or equipment modifications, inherently safer design minimizes or eliminates the need for IPLs. For example, if the maximum pump discharge pressure (not positive displacement pump) is less than the process vessel maximum allowable working pressure; the overpressure of the vessel cannot be caused by any failure associated with block-in of the vessel with the pump running. Therefore, Inherent / Intrinsic Safety can eliminate the risk of overpressure through the vessel and pump design.

If Inherent / Intrinsic Safety does not eliminate the risk, the remainder of the IPL/SIL Assessment Worksheet must be completed. Listed below are examples of inherently, or intrinsically, safer concepts for the team to consider but are not limited to:

a. Vessel or piping pressure rating above maximum pressure that can occur from internal and external pressure sources; or
b. Elimination of the use of a process chemical.
c. Location of equipment (proximity to other vessels, personnel or community).
d. Elevation of the pressure relief device for enhanced dispersion.

C.5.4 Initiating Cause Evaluation

C.5.4.1 Initiating Cause

a. Once the hazard event scenario is developed, the initiating cause(s) are documented. The team should list all initiating causes for the process disturbance, including human error, equipment failures, instrumentation failures, procedural errors, etc. For example, the loss of supply of a process chemical due to a valve closure could result in low level in a vessel. An empty vessel could allow process gas to pass to the next vessel potentially rupturing the downstream vessel by overpressure. The initiating cause is loss of supply based on an initiating failure.

C.5.4.2 Enabling Events or Conditions

a. Sometimes, a single initiating cause is insufficient for propagation to a serious incident. When this occurs, the IPL/SIL Assessment Team should examine whether a potential initiating cause could propagate to the hazard event scenario if other events, or conditions, also occurred. These other events are known as enabling events.

b. Enabling events or conditions are events that are necessary for the initiating cause to start to propagate towards the undesired consequence. Enabling events may consist of operating mode (start-up, shutdown, maintenance), operating sequence (specific process phase or step), environmental condition (external temperature), or other basic failures (that are not considered by the team to be protection layers).

c. Enabling events and conditions are expressed as probabilities, i.e., the probability that the event or condition is present or active when the initiating cause occurs. The team should pay particular attention to any possible links between an initiating cause and enabling event. In the conservative extreme, the probability of the enabling event occurring is whenever the initiating cause occurs.

d. The overall initiating cause description should be restricted to the minimum combination of initiating and enabling events that are necessary to result in hazard event scenario. The interaction between the initiating cause and enabling event should be described so that all team members understand the relationship.

e. Enabling conditions are important when considering batch operations, maintenance activities or operator-initiated actions. For example, a flow control valve failure may only propagate to loss of containment during the regeneration cycle. The initiating cause is flow control valve failure and the enabling condition is the regeneration cycle.

f. Enabling events and conditions are typically operational rather than intentional design features and may not be covered by a site’s management of change process. Therefore, caution needs to be taken when the ‘time at risk’ factor includes operational factors that are likely to change. A site shall develop a list of enabling events and conditions to support management of change.

g. If the team cannot determine a credible initiating cause for the scenario, record “No credible cause” in the initiating cause portion of the IPL/SIL Assessment Worksheet. The team will then proceed to the next scenario.

C.5.4.3 Conditional Modifiers

a. In some cases, an additional detailed assessment may be required to quantify the probability that the hazard event scenario will occur.

b. Conditional modifiers are risk reduction factors which are either external to the operation of the site (e.g., weather conditions) or are part of the general design of the site without being specific to a protection layer (e.g., probability of personnel in the area, presence of an ignition source, probability of an injury from exposure to the effects of a fire, explosion or toxic release, etc.). Consequence modelling may be involved in justifying the use of conditional modifiers.

c. The same principles of independence, effectiveness and auditability which apply to IPLs also apply to conditional modifiers. It is important to make sure that the conditional modifier is effective in its own right in preventing the consequence without relying on the performance of another modifier or protection layer.

d. Caution should be exercised if using conditional modifiers in that there must be a documented basis or published reference. Any modifications to standard published values must be justified and documented. The use of conditional modifiers should be limited and only considered when the scenario consequence justifies the additional analysis. Guidance for when to use and when not to use conditional modifiers is provided in the CCPS / AIChE, Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis.

e. Care should be taken when applying conditional modifiers in order to avoid violating rules of independence. For example, if probability of people in the area is considered and influences the consequence severity, the “probability of persons present” cannot be used as a conditional modifier to reduce the frequency of the harmful event.

f. Extreme care should be taken if more than two conditional modifiers are applied to any one hazard scenario to avoid double counting the risk reduction measures.

g. A site shall develop a list of acceptable conditional modifiers to support the requirement to be consistent in their application.

C.5.4.4 Initiating Cause Type

a. The IPL/SIL Assessment Team should consider the types of initiating causes listed below:
   i. Standard Operating Procedures (SOP)
   ii. Basic Process Control System (BPCS)
   iii. Local Control Systems or Shutdowns (LOCAL)
   iv. Miscellaneous items (OTHER)

b. Standard Operating Procedure (SOP) - This type does not require violation of a specific written procedure. It is simply any action or lack of action by operating or maintenance personnel in the plant that could begin the incident propagation leading to the hazard event scenario. Examples are closing a valve in error or at the wrong time, not opening a valve, entering an incorrect set-point for control, or bypassing a process control function.

c. Basic Process Control System (BPCS) - Any failure of a normal regulatory control loop whose inputs and outputs are associated with the unit Distributed Control System (DCS) or Programmable Logic Controller (PLC). The failure could be the sensor, the BPCS hardware or software, or the final element, such as the solenoid, control valve, or block valve.

d. Safety Instrumented System (SIS) – Safety Instrumented Functions (SIFs) are generally designed to bring a process to a safe state. However, the intended or spurious trip of a SIF is considered an initiating cause when it results in a secondary hazard. These would be referred to as SIS initiating cause types.

e. Local Control Systems or Shutdowns (LOCAL) - Any failure of field installed equipment, such as a local controller or local indicator, whose operation is independent of the BPCS. Examples are in-line pressure regulators or indicators.

f. Miscellaneous (OTHER) - Initiating causes that do not fall into one of the other types. Examples are loss of mechanical integrity, major equipment failure, loss of utility, or loss of chemical supply.

g. In the example worksheet, there is a field to record the initiating cause type.

C.5.4.5 Initiating Cause Frequency

a. The frequency of the initiating cause may be estimated by considering how often the initiating cause might be expected to occur during plant operation. The frequency of the initiating cause is evaluated without the consideration of any IPLs.

b. The frequency of the initiating cause should be estimated by considering plant historical performance and/or experience with the initiating cause under similar plant conditions. Frequencies that are outside team experience should be estimated with caution. This is likely to apply to any frequencies less often than once in 10 years.

c. Guidance for estimating the frequency of the initiating cause is provided in Table C-4; Typical Initiating Cause Frequencies. The values shown should be entered into the IPL/SIL Assessment Table accordingly. If the value is taken from Table C-4, it should be documented in the justification section of the worksheet.

d. Any frequencies from the table that the team believes are too low for the specific hazard event scenario being considered may be revised, with documented justification, by the team to better reflect the real situation, as they understand it.

e. Any frequencies from the table that the team believes are too high should only be revised with caution and the justification shall be documented.

f. If the initiating cause is not provided in the table, it must be estimated by the team using published failure rate data, plant historical data, or engineering estimates. The justification for the choice shall be recorded on the IPL/SIL Assessment Worksheet.

g. There may be instances in which the team determines that the initiating cause is not credible due to the process design (inherent/intrinsic safety). When the initiating cause is determined to be not credible, the team shall document “not credible” under the incident frequency and shall also document the justification for that conclusion. This may require listing each obvious candidate for initiating cause with a justification as to why each is not credible.

C.5.4.6 Further Guidance on SOP or Human Factor Initiating Cause Frequency

a. Per Table C-4, and Figure D-17, a typical human error of omission probability on routine task without special procedures, i.e. checklist, etc., is 1 per 100 events.

b. Per Table C-4, and Figure D-17, this may be reduced to 1 per 1000 events if it is an error in a normal routine simple operation where the operator is trained on the required action, it is embedded in a procedure available to examine, and a review of the correctness of the action is performed either by on-line diagnostics or by an independent person. This includes multiple element process procedures such as failure to execute a LO/TO (lock-out tag-out) procedure.

c. Certain, high frequency, events may be treated somewhat differently, but extreme care must be taken. For example, assume that 3 effluent road tankers are loaded each day (assume 1000 operations each year) and overflow is prevented purely by the operator observing the tanker level through the manhole. From Table C-4, we can take an operator failure probability of 1 in 100 times (0.01) and therefore an overflow frequency of 1000 x 0.01 = 10 per year. In some cases, the operating experience may show an overflow event is highly uncommon, and therefore this frequency is not realistic.

   In cases such as this, it is acceptable to use an initiating cause frequency of 0.1/yr if this is supported by site data. However, it must be determined whether other protective systems were utilised in preventing an overflow during the 30 years of experience. For example, the operator may have made an error with a higher frequency, but the road tanker driver spotted the error before an incident arose. If this was the case, it is still possible to use the frequency of 0.1/yr., however further risk reduction cannot be given for the presence of the tanker driver.

d. For frequently performed events, it is acceptable to use an initiating cause frequency of ≤ 0.1/yr if supported by site data. However, it must be determined whether protective systems were utilized in preventing the event and that such systems are not “double counted”.

C.5.5 Independent Protection Layers and Probability of Failure on Demand Rates

C.5.5.1 Identification of Independent Protection Layers

a. Document the IPLs that prevent the hazard event scenario. (Reference the IPL/CMS section in the example IPL/SIL Assessment Worksheet.) The IPLs may include any of the various types listed in Section C.5.5.2. To be considered an IPL, the protection layer must meet the following requirements:

   i. Independent from the initiating event and other protection layers.

   ii. Auditable; capable of being evaluated or validated for performance.

   iii. Effective in preventing the consequence when it functions as designed; the IPL must completely prevent the hazard event scenario without the assistance of any other protection layer.

   iv. IPL security shall be managed by design or by administrative procedure to ensure that unauthorized changes are not made that affect the integrity of the IPL, its availability, or any of its properties.

b. The example IPL/SIL Assessment Worksheet provides a separate PFDavg calculation section for aligning IPLs to those initiating causes that they are fully capable of preventing the potential scenario. The IPL/SIL Assessment Leader is responsible for aligning IPLs to initiating causes appropriately.

c. The IPL should be thoroughly described in the IPL/SIL Assessment Worksheet, including instrument and device tag numbers, SOP number, etc. A functional description of how the IPL works should also be provided to assist the team in allocating the amount of risk reduction provided by the IPL. See Section C.7 for more guidance on IPLs.

d. Where a SIF is proposed but not implemented, or where a SIF currently exists but has not been assessed before, the IPL/SIL Assessment team should not assume a nominal performance or assign a nominal PFDavg to that function. The PFDavg should only be assigned after the SIF is reviewed and confirmed as being implemented.

NOTE: During the normal cyclic Process Hazards Analysis, the PHA team will list all safeguards that are present, including many that do not meet the criteria listed above or the restrictions provided in Table C-5 through Table C-8. IPL/SIL Assessments are detailed assessments of the safeguards to determine the level of risk reduction provided by each safeguard. Many safeguards identified in the PHA will not be considered IPLs during this assessment.

C.5.5.2 Type of Independent Protection Layer

a. An IPL can be categorized into one of the types listed below and described in Section C.7:

   i. Standard Operating Procedure (SOP)

   ii. Basic Process Control System (BPCS)

   iii. Local Control Loop or Shutdown (LOCAL)

   iv. Alarms with Operator Response (ALARM)

   v. Safety Instrumented System (SIS)

   vi. Consequence Mitigation System (CMS)

   vii. Pressure Relief Valves (SRDs)

   viii. Other miscellaneous (OTHER).

b. In the example worksheet, there is a field to record the IPL type.

C.5.5.3 PFDavg Values for Independent Protection Layers

a. The PFDavg for an IPL is the probability that, when demanded, it will not perform the required task. Table C-3 provides a correlation between PFDavg, RRF, and availability. Tables C-5 through C-8 have been developed as internal guidance on the PFDavg for each IPL. In order for the IPL to be credited the listed PFDavg, or related risk reduction, the restrictions provided in the reference tables must be met.

b. As the team assesses each IPL, they must determine whether the IPL meets the restrictions. If the IPL does not meet any one or part of the restrictions, no risk reduction credit should be taken for the IPL (PFDavg = 1 or RRF=1). The IPL should still be listed with an explanation of why credit was not given.

c. The PFDavg, or corresponding risk reduction, that can be credited to any single IPL is limited to those factors provided in Table C-5 through Table C-8. Any other figures should be justified with published references and written documentation.

d. Existing and new safety shutdowns and alarms that are listed on the IPL/SIL Assessment Worksheets having a PFDavg of 0.1 or lower are considered to be part of the existing instrumented safety system and, therefore, are to be in the maintenance, inspection and testing program. Reference Section 3.3.

C.5.6 Consequence Mitigation Systems and Probability of Failure on Demand Rates.

C.5.6.1 CMSs can reduce the severity or the frequency of a scenario. The team must document a description of the CMS in the IPL/SIL Assessment Worksheet. This is entered in the same section of the example worksheet as IPLs.

C.5.6.2 Table C-9 is intended for use in determining the PFDavg, or risk reduction, for each CMS. Typical CMSs that will be considered in the IPL/SIL Assessment are as follows:

a. Tank Bunding (Dikes)

b. Blast Walls.

C.5.6.3 It is important for the team to review the CMS to ensure that they are sized and located such that they completely mitigate the hazard event scenario. If there is no documentation to support the claim that they are sized and located to mitigate the scenario, then no risk reduction credit should be taken.

C.5.6.4 The IPL/SIL Assessment Team shall evaluate if the functioning of the CMS has the potential to result in another hazard event scenario. If that is the case, the IPL/SIL Assessment Leader shall capture the scenario for further analysis as an independent event.

C.5.7 IPL/SIL Assessment (PFDavg Calculation)

C.5.7.1 Referencing the PFDavg Calculation section of the example IPL/SIL Assessment Worksheet, the calculation of intermediate event frequencies is carried out for each of the listed initiating causes. This means that the mitigated risk scenario is based on a single cause-consequence approach. This calculation is the product of the consequence severity level and frequencies associated with the initiating cause and the PFDavg(s) for the associated IPLs and CMSs. This also takes into account any enabling event or conditional modifier frequency credits.

Note: If using the example worksheet, the IPL/SIL Assessment Leader must manually insert a value of 1 into the calculation table where IPLs or CMSs do not fully apply to individual initiating causes.

C.5.7.2 The final risk scenario frequency is the sum of each of the single cause risk scenario Unmitigated Event Frequency (UEF) and the Mitigated Event Frequency (MEF) frequencies.

C.5.7.3 Based on the final risk scenario frequency, it is then possible to decide whether there are any gaps in the integrity level which need to be closed. If the final risk scenario frequency is less than or equal to the target frequency based on the severity category level, then no additional IPLs are required.

C.5.7.4 NOTE: In some instances, IPLs may not be required from a risk standpoint, but may be required by code or regulatory requirement(s). Nothing in the IPL/SIL Assessment Standard negates requirements of codes or regulations. This process simply provides an analysis tool for determining the best strategy for minimizing risk.

C.5.7.5 If the overall achieved frequency is greater than the target frequency, then the team is to review the risk reduction measures for that scenario. The team should: (a) validate the nominal PFDavg assigned to any SIF, and (b) assess whether there are any other risk reduction measures that should be included in the study.

C.5.7.6 The team should then recommend (a) a revised RRF and PFDavg for the SIF and (b) list any other risk reduction measures and associated requirements (procedural etc.) to assure the risk reduction assigned to those measures. When the team makes recommendations, the team should also identify the specific type of IPL to be implemented.

C.5.7.7 The team is typically not expected to design solutions. The expectation is that a recommendation is documented to “close” the gap in integrity level which is identified on the IPL/SIL Assessment Worksheet for the hazard event scenario being discussed. The way that the required integrity level is actually achieved will be determined during the design phase of the implementation process.

C.5.7.8 A gap is considered fully “closed” if the RRF is less than or equal to 1 when compared to the required target. Additional protection layers are to be identified and implemented until gap closure is achieved.

a. For a residual gap of 1 to 5 the site may consider the implementation of a protection layer that may not meet the independence requirement of an IPL, but all other IPL requirements, such as the inspection, testing, and maintenance requirements must be in place.
b. For a gap of greater than 5, the protection layer must meet all IPL requirements.

C.5.8 Comments

C.5.8.1 The comments field, on the example worksheet, is provided to allow the team to document any special considerations that they may have taken into account during the assessment and which type of consequence has been the governing concern.

C.5.9 Recommendations

C.5.9.1 The recommendations field, on the example worksheet, is provided for the team to document actions that need closure to complete the assessment. Such recommendations may include the need for further studies, validation of the assumed SIL of an existing SIF, or modifications of existing IPLs and CMSs to meet the required restrictions.

C.5.9.2 The recommendations should include as much information as necessary to ensure it is clearly understood.

C.5.10 EHS Critical Equipment and Procedures

C.5.10.1 The EHS Critical Equipment and IVL EHS Critical Procedures or Task field, on the example worksheet, is provided for the team to document the specific devices and administrative procedures or tasks given risk reduction credit as an IPL or CMS.

C.5.10.2 Any engineered equipment, or administrative procedure or task which is part of an IPL, and is designed to prevent a Severity Category A thru F hazard event scenario, or to minimize the risk or mitigate the consequence of such events, shall be identified as an EHS Critical IPL per IVL EHS-405.

C.5.10.3 Any failure to perform a procedure or sequence of tasks in a operating procedure that was recorded as an initiating cause for a Severity Category A thru F hazard event scenario shall be identified as an EHS Critical operator task.

C.5.10.4 IPLs, enabling events and conditional modifiers for Severity Category A thru F events shall be assessed to confirm they are designed and maintained to achieve the risk reduction credited. See the IVL EHSF-406-03, Independent Protection Layer Verification and Integrity Assessment form for guidance.

C.5.11 IPL/SIL Assessment Completion

C.5.11.1 When the team has completed the scenario evaluation, associated with each node of the PHA, the team should assess if there are any additional scenarios to complete the assessment. If the team does not find any additional scenarios, the IPL Analysis is complete. Otherwise, the team should execute this assessment for these new scenarios.

C.6 Reporting

C.6.1 Once the study is completed, the IPL/SIL Assessment Leader provides records of the assessment. This includes the IPL/SIL Assessment Worksheets, a description of the process, a reference to the drawings, a list of team members plus their roles, and other pertinent information to be included with the report in accordance with the minimum requirements in B.16.1.

C.6.2 Report records shall be retained for the life of the asset.

C.7 Independent Protection Layer Clarifications

C.7.1 An IPL is an independent protection layer that meets the criteria of specificity, independence, dependability, auditability, and security. IPLs can be active or passive systems, as long as the following criteria are met.

C.7.1.1 Specificity: The IPL is designed to prevent or mitigate the consequences of the identified hazard.

C.7.1.2 Independence: An IPL shall be independent of the initiating cause and all of the other protection layers associated with the identified Hazard Event Scenario. Independence requires the performance must not be affected by the failure of another protection layer or by the conditions that caused another protection layer to fail

C.7.1.3 Dependability: The protection provided by the IPL shall reduce the identified risk by at least ten-fold. In terms of Availability, the IPL must be at least 90% available.

C.7.1.4 Auditability: The IPL must be designed to allow regular validation of the protective function

C.7.1.5 Security: The IPL security shall be managed by design or by administrative procedure to ensure that unauthorized changes are not made that affect the integrity of the IPL, its availability, or any of its properties.

C.7.2 Examples

C.7.2.1 Examples of IPLs include critical control loops in the BPCS, emergency alarms with operator response, safety instrumented systems, and consequence mitigation systems. (See Glossary Attachment A for definitions).

C.7.3 IPL Types

C.7.3.1 IPL Types are categories developed to assist in the assessment of the PFDavg or Risk Reduction Factor (RRF) that can be allocated to each IPL.

C.7.3.2 Standard Operating Procedure (SOP)

a. A Standard Operating Procedure, used as an IPL, is a written and auditable procedure readily available to all operating personnel. The procedure must require a written log of the pertinent process variable that is being used to detect the initiating cause for the hazard event scenario. The SOP lists the action(s) required by the operator if the process variable being monitored goes out-of-range.
b. Standard Operating Procedures used as IPLs shall describe the alarm functionality, the specific actions required when the alarm activates, the alarm priority, means of annunciation and the expected response time for operator action.
c. To determine whether an SOP can be used as an IPL, the IPL/SIL Assessment Team must document that the SOP IPL is independent of the initiating cause. To be independent, the SOP IPL must be performed by a person or persons independent of the initiating cause using devices that are independent of the initiating cause. Care must be taken to ensure the initiating cause, logic solver, and final elements are independent.
d. Only one SOP IPL can be used for a given hazard event scenario due to the potential for common cause failure.
e. Administrative IPL (e.g., SOP or alarm with operator response) risk reduction factors should be limited to two for any single hazard event scenario.
f. Over use of administrative IPLs can give a false impression that more reliable protective layers are not required. From a reliability standpoint, inherent safety should be considered over Safety Instrumented Systems (SIS), SIS over BPCS IPLs, and BPCS IPLs over SOP IPLs.

C.7.3.3 Basic Process Control System (BPCS)

a. A BPCS, used as an IPL (i.e., automatic, non-settable), is a control loop or automated shutdown with software and/or I/O residing in the unit Distributed Control System (DCS) or a Programmable Logic Controller (PLC) used for normal process control. The BPCS IPL must completely mitigate the hazard event scenario without assistance from other systems. The documentation must include a description of how the BPCS IPL mitigates the hazard event scenario.

b. With one BPCS present, only one BPCS function shall be used as an IPL with an RRF of 10, or PFDavg of 0.1 when the initiating cause is a BPCS malfunction. Additional credit may be given if there are two independent BPCS present.

c. To be fully credited as an IPL, the BPCS device or action shall be independent of the initiating cause, enabling event and any other device, system, or action already credited as an IPL for the same hazard event scenario.

d. I/O, sensors, logic, solenoids, and final control elements for a BPCS IPL must be independent from the initiating cause and other IPLs.

e. The BPCS IPL must be in automatic mode when the hazard event scenario exists and be designed to function in truly "stand alone" fashion.

f. Further limitations on using the BPCS as an IPL are listed in Tables C-5 and C-7.

g. Any exception to the above resulting in a RRF of greater than 10 credited to the BPCS shall require a fully documented analysis of independence developed by the IPL/SIL Assessment Leader.

(Note: taking greater than a RRF of 10, or less than a PFDavg of 0.1, is outside the limit established by IEC 61511 unless all of the associated requirements noted in Figure C-3 are met and adequate demonstrations are made.)

h. It is an accepted practice for a supervisory control platform, such as a batch manager or tested, automated and secure logic, to adjust BPCS IPL trip set points based on production campaign. It would not be acceptable for a BPCS IPL trip set point to be written directly from the Operator graphical interface.

C.7.3.4 Alarms with Operator Response (ALARM)

a. ALARM - An alarm with operator response can be considered as an IPL if there: are specific actions that the operator is expected to perform; there is sufficient time for the operator to make the response; the operator is trained on the response; and the operator is independent of the initiating cause. The alarm must be configured with the proper priority to not be lost during an alarm event; not be operator re-settable; the operator cannot inhibit or modify the set point.

Response time requirements are listed in Table C-5 through Table C-8. Only one alarm with operator response can be used as an IPL.

b. Furthermore, if an alarm in the BPCS is designated as an IPL, the criterion for BPCS IPLs applies in Section C.7.3.3.

C.7.3.5 Local Control Loop or Shutdown (LOCAL)

a. LOCAL- Local controls used as IPLs are independent of the BPCS and can fully mitigate the potential incident. Often these devices are local hardwired controls or shutdowns. Because these devices are independent of the BPCS, they can be used when the Initiating Cause of the scenario is a failure of a BPCS function, including sensor, BPCS hardware or software, or valve. However, the risk reduction is limited by the integrity of the individual devices and Logic Solver (e.g. relay, pneumatic loop, PLC).

C.7.3.6 Safety Instrumented Systems (SIS)

a. Safety Instrumented Systems (SIS) - To be considered an IPL, the safety instrumented system must meet the requirements of ANSI/ISA 84.00.01-2004 (IEC

61511 Mod.) and be completely independent of the BPCS. The Risk Reduction Factor for the IPL is dependent on the Safety Integrity Level (SIL) classification of the full functional loop, including sensors, Logic Solver, final elements, and support systems.

C.7.3.7 Consequence Mitigation Systems (CMS) IPLs

a. Consequence Mitigation System (CMS) - IPLs include rupture disks, pressure relief valves, fire and gas systems, etc. To be considered an IPL, the documentation must show that the CMS is designed to mitigate the hazard event scenario. For example, it must be verified that the pressure safety valve or pressure relief valve is sized for the specific relief case generated by the hazard event scenario.

b. To determine whether a CMS can be used as a CMS IPL, the IPL/SIL Assessment Team must verify that the CMS function is independent of the initiating cause and other IPLs. For manually initiated CMS IPL, the initiating cause and other IPLs must be examined to ensure that the same Operator or Operator response that resulted in the other failure cannot also cause the CMS to fail.

c. CMS IPLs reduce the frequency and/or consequence of the hazard event scenario. Depending on the type of CMS IPL, the consequence due to CMS functioning may still be unacceptable. Consequently, the analysis requires the assessment of the consequence due to the CMS IPL functioning.

C.7.3.8 Other Miscellaneous IPL (OTHER)

a. IPLs are classified as “OTHER” if they do not fit into the above categories and typically consist of physical or mechanical devices (i.e., bunds, dykes, mechanical stops on valves) or characteristics of the plant system, such as physical location of the devices that reduce the risk associated with a scenario. If the characteristic is used as an IPL or enabling event, the specifications for the device or system must be recorded and audited so that future changes to the sites will not make the IPL invalid.

b. Also classified as “OTHER” in the example worksheet are enabling events and conditional modifiers, as described in C.5.4.2 and C.5.4.3, respectively. These events or conditions impact the probability of a scenario progressing to the consequence of concern.

C.7.4 IPL Risk Reduction Factor (RRF)

C.7.4.1 This is a measure of how much the independent protection layer (IPL) reduces the frequency of the hazard event scenario. It is calculated based on the Probability of Failure on Demand (PFD) for the IPL. The Risk Reduction Factor is equal to the inverse of the PFD.

FIGURE C-1 IPL FLOWCHART (FACILITATOR PREPARATION)

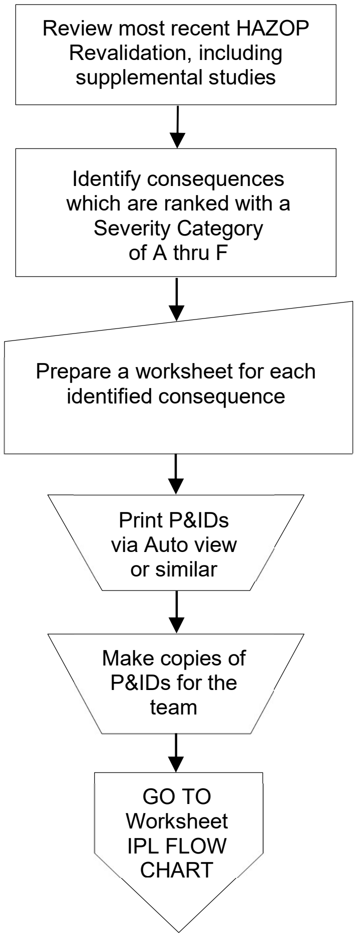

Review most recent HAZOP Revalidation, including supplemental studies
Identify consequences which are ranked with a Severity Category of A thru F
Prepare a worksheet for each identified consequence
Print P&IDs via Auto view or similar
Make copies of P&IDs for the team
GO TO Worksheet IPL FLOW CHART

FIGURE C-2 IPL FLOWCHART (WORKSHEET)

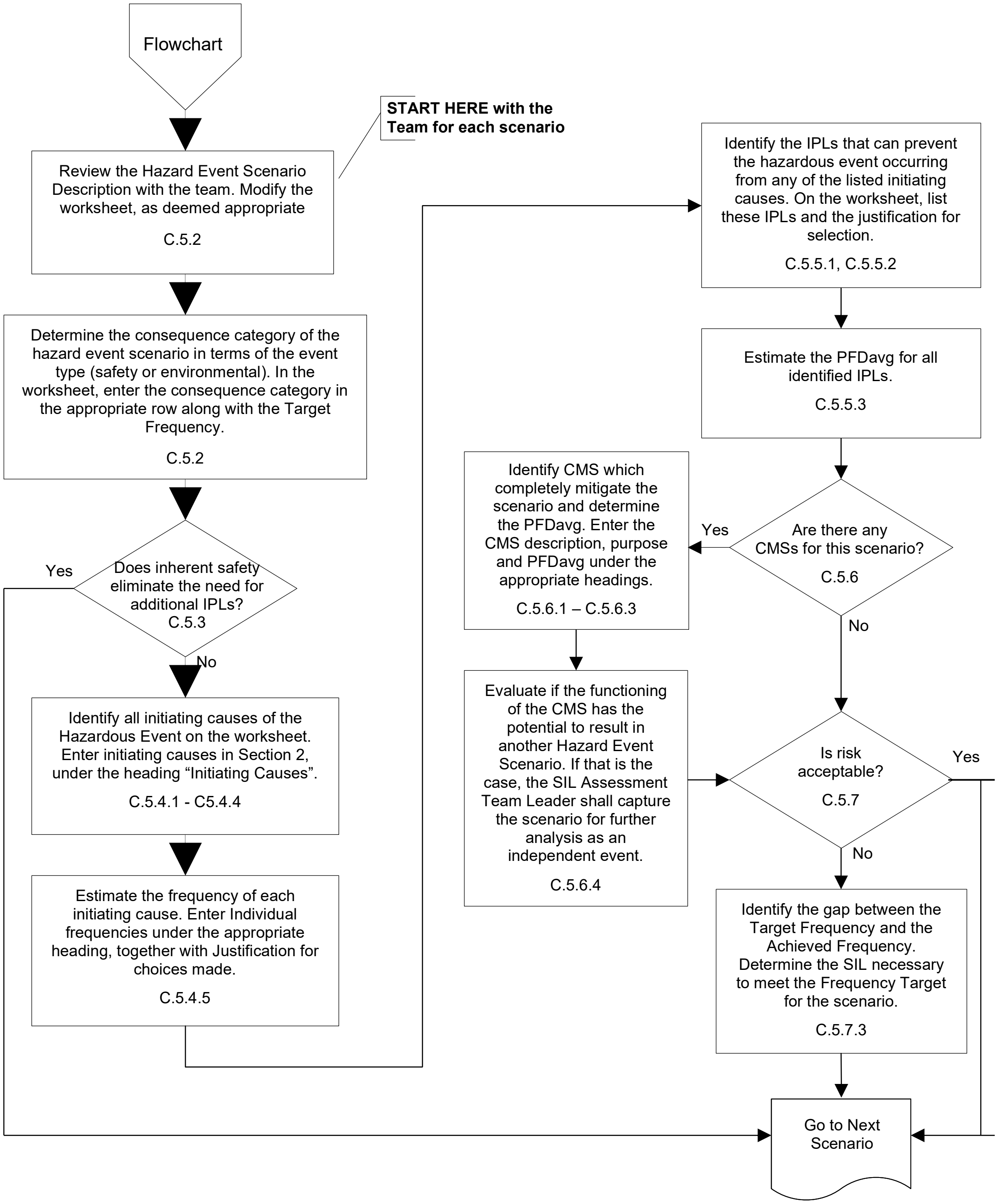

Flowchart
START HERE with the Team for each scenario
Review the Hazard Event Scenario Description with the team. Modify the worksheet, as deemed appropriate
C.5.2
Determine the consequence category of the hazard event scenario in terms of the event type (safety or environmental). In the worksheet, enter the consequence category in the appropriate row along with the Target Frequency.
C.5.2
Does inherent safety eliminate the need for additional IPLs?
C.5.3
Yes
No
Identify all initiating causes of the Hazardous Event on the worksheet. Enter initiating causes in Section 2, under the heading "Initiating Causes".
C.5.4.1 - C5.4.4
Estimate the frequency of each initiating cause. Enter Individual frequencies under the appropriate heading, together with Justification for choices made.
C.5.4.5
Identify the IPLs that can prevent the hazardous event occurring from any of the listed initiating causes. On the worksheet, list these IPLs and the justification for selection.
C.5.5.1, C.5.5.2
Estimate the PFDavg for all identified IPLs.
C.5.5.3
Are there any CMSs for this scenario?
C.5.6
Yes
No
Identify CMS which completely mitigate the scenario and determine the PFDavg. Enter the CMS description, purpose and PFDavg under the appropriate headings.
C.5.6.1 – C.5.6.3
Evaluate if the functioning of the CMS has the potential to result in another Hazard Event Scenario. If that is the case, the SIL Assessment Team Leader shall capture the scenario for further analysis as an independent event.
C.5.6.4
Is risk acceptable?
C.5.7
Yes
No
Identify the gap between the Target Frequency and the Achieved Frequency. Determine the SIL necessary to meet the Frequency Target for the scenario.
C.5.7.3
Go to Next Scenario

TABLE C-1 IPL/SIL ASSESSMENT WORKSHEET (IVL EHSF-406-02)

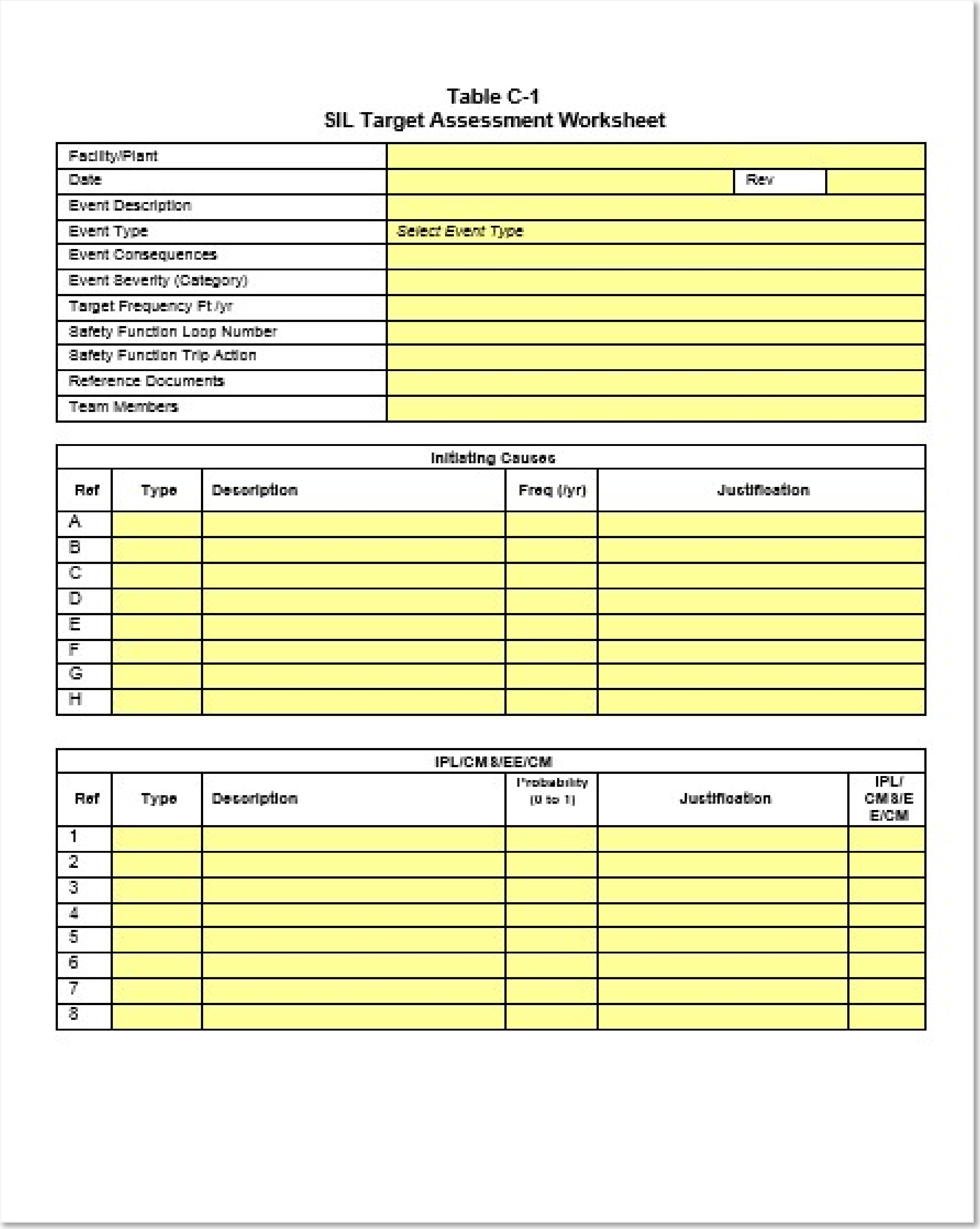


Table C-1
SIL Target Assessment Worksheet

Facility/Plant			
Date		Rev	
Event Description			
Event Type	*Select Event Type*		
Event Consequences			
Event Severity (Category)			
Target Frequency Ft /yr			
Safety Function Loop Number			
Safety Function Trip Action			
Reference Documents			
Team Members			

Initiating Causes

Ref	Type	Description	Freq (/yr)	Justification
A				
B				
C				
D				
E				
F				
G				
H				

IPL/CMS/EE/CM

Ref	Type	Description	Probability (0 to 1)	Justification	IPL/ CMS/E E/CM
1					
2					
3					
4					
5					
6					
7					
8					

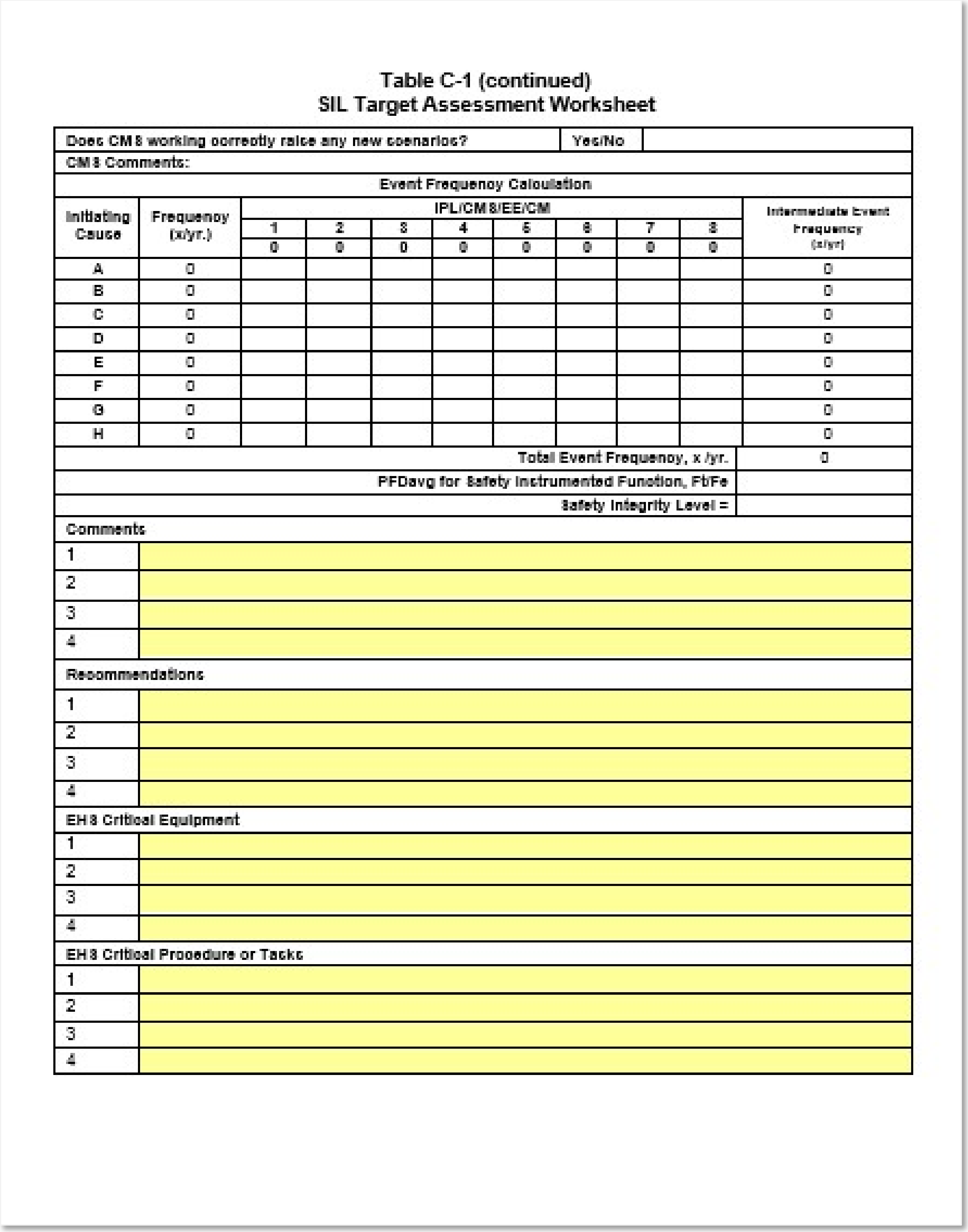


Table C-1 (continued)
SIL Target Assessment Worksheet

Does CMS working correctly raise any new scenarios?								Yes/No		
CMS Comments:										
Event Frequency Calculation										
Initiating Cause	Frequency (x/yr.)	IPL/CMS/EE/CM								Intermediate Event Frequency (x/yr)
		1	2	3	4	5	6	7	8	
		0	0	0	0	0	0	0	0	
A	0									0
B	0									0
C	0									0
D	0									0
E	0									0
F	0									0
G	0									0
H	0									0
									Total Event Frequency, x /yr.	0
									PFDavg for Safety Instrumented Function, Ft/Fe	
									Safety Integrity Level =	
Comments										
1										
2										
3										
4										
Recommendations										
1										
2										
3										
4										
EHS Critical Equipment										
1										
2										
3										
4										
EHS Critical Procedure or Tasks										
1										
2										
3										
4										

Table C-2 I&E Equipment Categorization Abbreviations

Abbreviation	Translation
APL[2]	Asset Protection Level
BPCS	Basic Process Control System
CMS	Consequence Mitigation System
COI	Consequence of Interest
DCS	Distributed Control System
EIL3	Environmental Integrity Level
ESD	Emergency Shutdown System
RRF	Risk Reduction Factor
IL	Integrity Level
IPL	Independent Protection Layer
MOC	Management of Change
PFD4	Probability of Failure on Demand at a specific instant in time
PFDavg	Average Probability of Failure on Demand
PHA	Process Hazard Analysis
P&ID	Piping & Instrument Diagram
PLC	Programmable Logic Controller
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SOP	Standard Operating Procedure
SSS	Safety Shutdown System

[2] This term is not recognized in the related international standards.
[3] This term is not recognized in the related international standards.
[4] The PFD varies with time and is not a constant value.

Table C-3 - The Relationship Between SIL, PFDavg, RRF, and Availability

SIL	PFDavg	RRF	Availability
1	≥ 0.01 to < 0.1	>10 to ≤ 100	>90 to ≤ 99%
2	≥ 0.001 to < 0.01	>100 to ≤ 1000	>99 to ≤ 99.9%
3	≥ 0.0001 to < 0.001	>1000 to ≤ 10000	>99.9 to ≤ 99.99%

Table C-4 Typical Initiating Cause Frequencies

(This table is intended for use as guidance. Actual values used should reflect the conditions at the site and consider enabling events and/or conditions that may modify the frequencies shown in this table.)

Initiating Cause	Conditions	Frequency
Basic Process Control System (BPCS)	The service is relatively clean with no documented history of instrumentation problems due to plugging, polymerization, or deposition. The frequency represents an undetected dangerous failure that can propagate into the incident[5].	0.1/yr
	The service is prone to instrumentation problems due to plugging, polymerization or deposition. The frequency represents an undetected dangerous failure[6] that can propagate into the incident.	1/yr
Loss of Process Supply (OTHER)	Loss of Supply from all causes: e.g., pump failure, accidental block in, or primary supply problem. Includes loss of utilities such as cooling water.	0.1/yr
Relief valve opens early (OTHER)	Opens early propagates to an incident	0.01/yr
Operator or Maintenance Action (SOP)	Action is bounded by normal manual actions. The operator is trained on the required action, has procedures available to examine, and the action is considered normal operational duty.	probability of 1 in 100 times the number of times the action is performed per year
	Action is bounded by normal routine manual actions. The operator is trained on the required action, has procedures available to examine, and the action is considered normal routine operational duty. A review of the correctness of the action is performed either by on-lie diagnostics or by an independent person. Includes multiple element process procedures such as failure to execute a LO/TO (lock-out tag-out) procedure.	probability of 1 in 1000 times the number of times the action is performed per year
	For frequently performed events, it is acceptable to use an initiating cause frequency of ≤ 0.1/yr if supported by site data. However, it must be determined whether protective systems were utilized in preventing the event, and that such systems are not “double counted”.	0.1/yr
Mechanical Failures Metallic (OTHER)	No moving parts – no vibration Low vibration High vibration	0.001/yr 0.01/yr 0.1/yr
Mechanical Failures Non-metallic (OTHER)	No moving parts – no vibration Low vibration High vibration	0.01/yr 0.1/yr 1/y
Mechanical Failures Hoses (OTHER)	No moving parts – no vibration Low vibration High vibration	0.01/yr 0.1/yr 1/y
Pressure Regulator Failures (OTHER)	Local pressure regulator or pressure reducing valve in a clean service under periodic maintenance. If no periodic maintenance use 0.1/yr.	
Pump Failure (OTHER)	Single pump whose failure is sufficiently catastrophic to prevent adequate supply to downstream process, directly resulting in the potential hazard event scenario.	0.1/yr

[5] IEC 61511 states that the dangerous failure rate of a **BPCS** that is not designed in compliance with IEC 61511 cannot be assumed to be higher than 10-5/hr. This is approximately 1 in 10 years

[6] No diagnostic coverage credit is taken for dirty services.

Table C-4 Typical Initiating Cause Frequencies

Pump Failure (OTHER)	Dual pumps with one pump in standby. No auto-start. Pump failure is sufficiently catastrophic to prevent adequate supply to downstream process, directly resulting in the potential hazard event scenario.	0.1/yr
	Dual pumps with one pump in standby. Auto-start is provided. Both pumps must fail catastrophically and prevent adequate supply to downstream process, directly resulting in the potential hazard event scenario.	0.01/yr
	Pump seal failure resulting in a significant leak.	0.1/yr
Other Initiating Causes (OTHER)	Group must consider the components involved in the Initiating Cause.	Use experience of personnel or failure rate data
Pressure Vessel Residual Failure	Breach of pressure vessel resulting in full loss of containment. Use of this data should take actual service and inspection history into account.	0.000001
Piping Residual Failure	Full breach per 100 meters in length. Use of this data should take actual service and inspection history into account.	0.00001
Piping Leak	10% cross section per 100 meters in length. Use of this data should take actual service and inspection history into account.	0.001
Gasket/Packing Blowout	Loss of containment through partial gasket or packing failure.	0.01
Turbine/Diesel engine over-speed	Excessive vibration with potential for casing breach.	0.0001
Third Party Intervention	External impact of containment systems by backhoe, vehicle, etc.	0.01
Crane Load Drop	Overhead hazard with potential for breach of piping or equipment.	0.0001 per Lift

Overpressure Consequence Tables – Guidance

Piping:

Reference Code B31.3 (Allowable Stress = Min of 2/3 SMYS or 1/3 Tensile Strength, TS)

Flange rating at temperature/pressure generally limit MAOP unless there is a weaker point in the line (e.g. site glass, gauge, etc.)

Note: Facilitators should review piping specification sheets for actual flange ratings.

Table 1: Piping – B31.3 (A53B A106B – Carbon Steel)

Percent (%) MAOP Over Pressure	Most Likely Consequence
1.00 to 1.45 x design pressure	None
1.45 to 1.75 x design pressure	Gasket leakage possible
1.75 to 2.40 x design pressure	Gasket leakage, non-resealing
2.40 to 3.00 x design pressure	Line rupture possible

Table 2: Piping – B31.3 (A312 TP304 – 304 Stainless Steel)

Percent (%) MAOP Over Pressure	Most Likely Consequence
1.00 to 1.25 x design pressure	None
1.25 to 1.50 x design pressure	Gasket leakage possible
1.50 to 3.50 x design pressure	Gasket leakage, non-resealing
3.50 to 5.50 x design pressure	Line rupture possible

Pressure Vessels:

Reference Code ASME Section VIII Div.1 and Div. 2

Table 3: Vessels – ASME Section VIII Div. 1 and Div. 2

Percent (%) MAWP Over Pressure	Most Likely Consequence
1.00 to 1.30 x design pressure	None. Typically within PSV accumulation allowance for fire case.
1.30 to 1.50 x design pressure	Potential for gasket leakage, likely no permanent damage to vessel.
1.50 to 2.00 x design pressure	Gasket leakage is likely. There is potential of permanent vessel deformation and potential for cracking or leakage.
2.00 to 2.50 x design pressure	Gasket leakage is very likely and very likely to result in permanent vessel deformation, cracking, and leakage.
2.50 to 3.00 x design pressure	Gasket leakage and vessel deformation leading to significant leakage.
> 3.00 x design pressure	Potential for bursting of the vessel.

Table C-5 Risk Reduction Factors

With BPCS Initiating Causes

Based on Initiating Causes Related to "BPCS Hardware and Software, BPCS Sensor, or BPCS Valve" (Initiating Cause Type Listed: BPCS, ALARM)

<table>
<tr><th>IPL</th><th colspan="4">Further Restrictions on Considering as IPL</th><th>Probability (PFDavg)</th></tr>
<tr><td rowspan="2"><b>BPCS control loop</b></td><td colspan="4"><b>Any control loop residing in the BPCS not meeting the restrictions below.</b></td><td>1</td></tr>
<tr><td colspan="4">Only one BPCS function shall be used as an IPL with an RRF of 10, or PFDavg of 0.1. This applies to scenarios that include the BPCS as an initiating cause provided the BPCS IPL function:
- Shall be independent of the initiating cause and any enabling event.
- Shall be Independent of any other device, system, or action that is already being credited as an IPL for the same hazard event scenario.
- I/O, sensors, final elements, and communication bus for the BPCS IPL shall be independent from the initiating cause.
- The BPCS IPL must be in automatic mode when the hazard event scenario exists and be designed to function in truly "stand alone" fashion.
- Such installations shall be proven in use to be highly available and reliable.
- There shall be appropriate management of change and security procedures and practices in place to ensure the integrity of the IPL and related software.
- Accepted configuration for BPCS system shall include redundancy and fault tolerance of control processors and communications between control processors and I/O modules.
(Reference other requirements in Figure C-3.)</td><td>0.1</td></tr>
<tr><td rowspan="4"><b>Alarm with operator response</b></td><td colspan="4">Operator response is based on alarms generated by the BPCS that uses same sensor or valve as listed in the Initiating Cause</td><td>1</td></tr>
<tr><td>Time (min)</td><td>Where</td><td>How Many</td><td>Restrictions</td><td></td></tr>
<tr><td>&gt;10</td><td>Control Room</td><td>Single Operator</td><td>Independent of Initiating Cause. Alarm is annunciate on separate HMI or local panel, with the instrumentation connected to a separate relay or PLC system. The alarm instrumentation and operator response final element must be independent of the Initiating Cause. The operator is trained on alarm response, has procedures available to examine and practices the action periodically. Alarm must not be operator re-settable.</td><td>0.1</td></tr>
<tr><td>&gt;30</td><td>Field</td><td>Single Operator</td><td>Independent of Initiating Cause. Alarm is annunciate on separate HMI or local panel, with the instrumentation connected to a separate relay or PLC system. The alarm instrumentation and operator response final element must be independent of the Initiating Cause. The operator is trained on alarm response, has procedures available to examine and practices the action periodically. Alarm must not be operator re-settable.</td><td>0.1</td></tr>
<tr><td rowspan="3"><b>Standard Operating Procedures</b></td><td colspan="4">The action must be independent from the initiating cause and any other IPL. If an Operator action is the initiating cause, no RRF or PFDavg can be assigned to any Operator action that solely relies on the same Operator to recognize the problem and quickly correct it. If the initiating cause is the BPCS, no RRF or PFDavg can be assigned to any Operator action that solely relies on BPCS information display (e.g., process conditions, indications).</td><td>1</td></tr>
<tr><td colspan="4">Process Related Rounds and Inspections. Frequency of operator rounds must be sufficient to detect potential incident. If recognition of process variable is required, the operator must log specific values from sensors or valves independent of the Initiating Cause. Operator must log specific values. Log must show unacceptable out-of-range values. SOP must describe response to out-of-range values.</td><td>0.1</td></tr>
<tr><td colspan="4">Observational. Frequency of operator rounds must be sufficient to detect potential incident and prevent ultimate scenario. Impending incident must be obvious to operator through normal visual or hearing range, i.e. loud noise, high vibration, serious leaking, etc.
Review. Independent, supervisory review and sign off that work is complete and correct prior to start up or returning component to service.
Action. An Operator action that uses a different Operator, relying on independent observation.
Corrective Action. An Operator action taken based on a scenario where the event propagation is sufficiently slow that the Operator has enough time to recognize the error and to correct it.</td><td>0.1</td></tr>
</table>

Note: In order to claim a RRF for any IPL, the IPL under consideration must be independent from the listed initiating causes and any other IPLs that the team has already claimed for risk reduction

Table C-6 Risk Reduction Factors

With Human Factor Initiating Causes

Based on Initiating Cause Related to “Operator Action” OR
“Standard Operating Procedure Error” (Initiating Cause Type Listed: SOP)

IPL	Further Restrictions on Considering as IPL	Probability (PFDavg)
Standard Operating Procedures	Any operator action that uses the same operator	1
Alarms with Operator Response	Any operator action that uses the same operator. If the operator action is taken based on a scenario where the event propagation is sufficiently slow that the operator has enough time to recognize the error and to correct it, see below.	1
	An operator action that uses a different operator OR an operator action taken based on a scenario where the event propagation is sufficiently slow that the operator has enough time to recognize the error and to correct it.	See: Table C-5, Table C-7

Note: In order to claim a RRF for any IPL, the IPL under consideration must be independent from the listed initiating causes and any other IPLs that the team has already claimed for risk reduction

Table C-7 Risk Reduction Factors

With Other Initiating Causes

Based on Initiating Cause Related to “System Failures Other Than BPCS Hardware and Software, BPCS Sensor, or BPCS Valve” OR “Operator Action” OR “Standard Operating Procedure Error” (Initiating Cause Type Listed: LOCAL, SOP, OTHER)

<table>
<tr><th>IPL</th><th colspan="4">Further Restrictions on Considering as IPL</th><th>Probability
(PFDavg)</th></tr>
<tr><td rowspan="3"><b>BPCS control loop</b></td><td colspan="4">Any BPCS control loop that is unaffected by the failure listed in the scenario. Control loop’s normal action will prevent the scenario. Risk reduction can only be assumed for one control loop. Additional control loops may be documented but they must be considered one protection layer. The service is relatively clean with no documented history of instrumentation problems due to plugging, polymerization or deposition.</td><td>0.1</td></tr>
<tr><td colspan="4">Any BPCS control loop that is unaffected by the failure listed in the scenario. Control loop’s normal action will prevent the scenario. Risk reduction can only be assumed for one control loop. Additional control loops may be documented but they must be considered one protection layer. The service is prone to instrumentation problems due to plugging, polymerization, or deposition.</td><td>1</td></tr>
<tr><td colspan="4">If the initiating cause and enabling event(s) do not involve the BPCS, then up to two BPCS control loops can be credited as separate IPLs provided that each BPCS IPL function:
- is independent of any other device, system, or action that is already being credited as an IPL for the same hazard event scenario.
- I/O, sensors, logic solvers, final elements, and communication bus for the BPCS IPL shall be independent from the other BPCS IPL.
- The BPCS IPL must be in automatic mode when the hazard event scenario exists and be designed to function in truly "stand alone" fashion.
- Such installations shall be proven in use to be highly available and reliable.
- There shall be appropriate management of change and security procedures and practices in place to ensure the integrity of the IPL and related software.
- Accepted configuration for BPCS system shall include redundancy and fault tolerance of control processors and communications between control processors and I/O modules.
(Reference other requirements in Figure C-3.)</td><td>0.1 x 0.1</td></tr>
<tr><td rowspan="7"><b>Alarms with Operator Response</b></td><td>Time
(min)</td><td>Where</td><td>How Many</td><td>What Else</td><td></td></tr>
<tr><td>&lt;10</td><td>Control Room</td><td>Single Operator</td><td>Operator has less than 10 minutes to respond to the alarm.</td><td>1</td></tr>
<tr><td>&gt;10</td><td>Control Room</td><td>Single Operator</td><td>Operator action is complicated, i.e. large number of alarms generated by Initiating Cause and the response is not clear or documented.</td><td>1</td></tr>
<tr><td>&gt;10</td><td>Control Room</td><td>Single Operator</td><td>The operator is trained on alarm response, has procedures available to examine and practices the action periodically. Alarm must not be operator re-settable.</td><td>0.1</td></tr>
<tr><td>&gt;10</td><td>Control Room</td><td>Two Operators</td><td>All operators listed must receive the same information from two independent BPCS functions. Both operators can make independent responses, which completely prevent the event. The operators are trained on alarm response, have procedures available to examine and practice the action periodically. Alarms must not be operator re-settable.</td><td>0.01</td></tr>
<tr><td>&gt;30</td><td>Field</td><td>Single Operator</td><td>The operator is trained on alarm response, has procedures available to examine and practices the action periodically. Alarm must not be operator re-settable.</td><td>0.1</td></tr>
<tr><td>&gt;30</td><td>Field</td><td>Two Operators</td><td>All operators listed must receive the same information. Both operators have more than 30 minutes to make independent responses, which must completely prevent the event. Alarm must not be operator re-settable. The operator is trained on alarm response, has procedures available to examine and practices the action periodically. Alarm must not be operator re-settable.</td><td>0.01</td></tr>
</table>

Table C-7 Risk Reduction Factors

With Other Initiating Causes

Based on Initiating Cause Related to “System Failures Other Than BPCS Hardware and Software, BPCS Sensor, or BPCS Valve” OR “Operator Action” OR “Standard Operating Procedure Error” (Initiating Cause Type Listed: LOCAL, SOP, OTHER)

IPL	Further Restrictions on Considering as IPL	Probability (PFDavg)
Standard Operating Procedures	The action must be independent from the initiating cause and any other IPL. If an Operator action is the initiating cause, no RRF can be assigned to any Operator action that solely relies on the same Operator to recognize the problem and quickly correct it. If the initiating cause is the BPCS, no RRF can be assigned to any Operator action that solely relies on BPCS information display (e.g., process conditions, indications).	1
	Process Related Rounds and Inspections. Frequency of operator rounds must be sufficient to detect potential incident. If recognition of process variable is required, the operator must log specific values from sensors or valves independent of the Initiating Cause. Operator must log specific values. Log must show unacceptable out-of-range values. SOP must describe response to out-of-range values.	0.1
	Observational. Frequency of operator rounds must be sufficient to detect potential incident and prevent ultimate scenario. Impending incident must be obvious to operator through normal visual or hearing range, i.e. loud noise, high vibration, etc. Review. Independent, supervisory review and sign off that work is complete and correct prior to start up or returning component to service. Action. An Operator action that uses a different Operator, relying on independent observation. Corrective Action. An Operator action taken based on a scenario where the event propagation is sufficiently slow that the Operator has enough time to recognize the error and to correct it.	0.1

Note: In order to claim a RRF for any IPL, the IPL under consideration must be independent from the listed initiating causes and any other IPLs that the team has already claimed for risk reduction

Table C-8 Risk Reduction Factors

Based on Miscellaneous Initiating Cause Types Including Other, Local, SOP, and BPCS

IPL	Further Restrictions on Considering as IPL	Probability (PFDavg)
Check Valve	Single check valve. Must be designed to prevent the scenario	1
	Dual check valves in series. Must be designed to prevent the scenario	0.1
Flame Arrester	Must be designed to prevent the scenario	0.01
Pressure Regulator	Must be designed to mitigate the scenario	0.01
Vacuum Breaker	Must be designed to prevent the scenario.	0.01
Restrictive Orifice	Must be designed to prevent the scenario.	0.01
Special Personnel Protection Equipment	Special personnel protection equipment that is not normally worn by operation or maintenance personnel but is part of an established procedure. This PPE would include wire mesh gloves, fire suits, respirators, self-contained breathing apparatus, etc. The user of the equipment must be trained in the use of the PPE.	0.1
Limited Occupancy	A factor related to individuals present in an area will only be applied when an individual is in the area no more than 10% of the time.	0.1
Safety Instrumented System	Must be independent of BPCS hardware and software. Achieves SIL 1.	0.1 to 0.01
	Must be independent of BPCS hardware and software. Achieves SIL 2.	<0.01 to 0.001
	Must be independent of BPCS hardware and software. Achieves SIL 3.	<0.001 to 0.0001

Note: In order to claim a RRF for any IPL, the IPL under consideration must be independent from the listed initiating causes and any other IPLs that the team has already claimed for risk reduction

Check valves, flame arrestors, restrictive orifices can only be given a RRF if they are regularly tested/checked via a documented maintenance program.

Table C-9 Risk Reduction Factors

Based on Consequence Mitigation Systems (CMS)

CMS	Further Restrictions on Considering as IPL	Probability (PFDavg)
Pressure Relief Valve	Clean Service. PRV must be sized to completely mitigate the scenario.	0.01
	More than one PRV is available to mitigate overpressure scenario. Each PRV listed must be capable of independently relieving the vessel. Each PRV must be sized to completely mitigate the scenario.	0.001
	More than one PRV is available, but more than one is required to mitigate the full load. This includes staged release PRVs. To achieve higher RRF than 10, or lower PFDavg than 0.1, the PRV calculations must be reviewed to determine whether the load can be successfully handled by one PRV, based on the specific scenario under review.	0.1
	Plugging Service, i.e. prone to plugging, polymerization, or chemical deposition. An unprotected PRV used in a plugging service is not considered sufficient for consideration as an IPL.	1
	Plugging Service, i.e. prone to plugging, polymerization, or chemical deposition. Redundant Pressure Relief Valves with separate process connections. Each PRV must be sized to completely mitigate the event.	0.1
	Plugging Service, i.e. prone to plugging, polymerization, or chemical deposition. Pressure Relief Valve with integrated rupture disk. PRV must be sized to completely mitigate the scenario.	0.1
	Plugging Service, i.e. prone to plugging, polymerization, or chemical deposition. Pressure Relief Valve with integrated rupture disk with purging. PRV must be sized to completely mitigate the scenario.	0.01
Vessel Rupture Disk	Must be designed to mitigate scenario. Release must be evaluated for potential risk.	0.01
Blast-wall/Bunker	Process-related blast wall. This is not related to the control room design. The blast wall is typically designed to direct/contain the explosion away from the main the process unit.	0.001
Dike or Bund	Passive secondary containment system or basin with no drain valve or with management practices to ensure the drain valve is in the closed position.	0.01
Fire Detection with Water Deluge System	Operator initiated response. The PFDavg is based on operator alarm and response criteria, as listed in IPL PFDavg Tables (C-5 through C-7). Must be independent of the Initiating Cause and other IPLs.	Tables C-5 through C-7
	Using fire detectors with automatic deluge, e.g. foam, water curtain, water sprays, or emergency evacuation. Must be independent of the Initiating Cause and other IPLs.	0.1
Gas Monitors with Automated Deluge	Operator initiated response. The PFDavg is based on operator alarm and response criteria, as listed in IPL PFDavg Tables (C-5 through C-7). Must be independent of Initiating Cause and other IPLs.	Tables C-5 through C-7
	Using gas monitor with automatic response, e.g. water cannons, water sprays, or emergency evacuation. Must be independent of Initiating Cause and other IPLs.	0.1

Figure C-3 Minimum Requirements for Multiple BPCS Protection Layer Credits

The table below identifies the minimum requirements[7] that shall be met with regard to any programmable electronic system that is part of a BPCS to justify taking credit for more than one control function in the IPL/SIL Assessment.

Determination and documentation of the degree of independence between two functions that share a common logic solver is not a trivial task. Great care should be taken to not underestimate the level of common cause, common mode and dependent failures. Where this level of analysis cannot be performed, the BPCS shall be limited to a credit from a single function as an IPL or initiating cause.

Justification Requirement	Met √
For credit to be taken, the I/O, sensors, final elements, and communication bus for each BPCS function shall be independent of the initiating cause, any enabling event, or any other device, system or action already credited as an IPL for the same hazard event scenario.	□
The BPCS IPL(s) must be in automatic mode when the hazard event scenario exists and be designed to function in truly "stand alone" fashion. Such installations shall be proven in use to be highly available and reliable.	□
There shall be formal management of change, access control and security procedures and practices in place to ensure the integrity of the IPLs and related software.	□
Accepted configuration for BPCS system shall include redundancy and fault tolerance of control processors and communications between control processors and I/O modules.	□
There shall be an operating procedure which clearly defines the action to be taken if the control screen goes blank, a workstation 'freezes', or there are other signs that the programmable device has stopped working correctly.	□
There shall be a back-up power supply available with sufficient capacity to allow emergency actions to be taken in the event of a loss of the main power supply. These actions should be specified in a written procedure. The back-up power supply must be regularly maintained in accordance with a written procedure.	□
Where PFD data for the BPCS is not available and there is no actual failure data to suggest otherwise, and the redundancy, independence, and power supply criteria outlined in this document are verifiable, the BPCS logic solver may be presumed to deliver a PFD of no better than 1x10-2. Examples of distributed control systems which meet this criterion include Emerson Delta V and Provox and Invensys IA.	□
The total IPL PFDavg credit shall be no more than two orders of magnitude or 0.01, i.e. 0.1 for the basic BPCS IPL and 0.1 for the additional IPL justified by data and analysis in accordance with BS EN 61511-1 9.4.2 and 9.5.1. The following options could apply: • If the initiating cause involves a BPCS failure, the BPCS may only then appear once as a protection layer – either as a control function or as an alarm function, and only if there is sufficient independence between the relevant failed BPCS control or protection functions. • If the initiating cause does not involve a BPCS failure, the BPCS may perform up to two functions as protection layers (e.g., a control function and an alarm function) as long as other requirements on independence are met.	□
The basis for the assessment shall be verified during the design process, reference IVL EHS-409, Design and Maintenance of Safety Instrumented Functions (Plant Trips).	□

[7] Annex 5 of Process Safety Leadership Group 2009 Report entitled, Safety and Environmental Standards for Fuel Storage Sites,

Attachment D: Numerical Hazard Analysis (NHA) Methodology

D.1 Preface

The concepts and methodology presented in this attachment are intended for use by those Expert PHA Study Leaders and IPL/SIL Assessment Leaders with relevant competencies in Numerical Hazard Analysis techniques. It may also be useful as a basic guide and reference manual to enable managers, engineers and other technologists to understand the principles behind simple hazard analyses.

Those considering the use of the technique for the first time are strongly advised to discuss their results with a more experienced analyst. The guide uses a number of examples to demonstrate aspects of the technique from fault tree construction and evaluation to assessment of simple protective systems and the use of possible criteria against which to judge a hazardous event. Some summary tables of equations and data are provided.

It is not intended to be an in-depth study of hazard analysis. Those, who are interested in more detailed aspects and requiring tackling more complex analyses, should seek training in the technique.

D.2 Introduction

Hazard analysis is a technique that is used to aid decision making when considering safety and design problems. It is a systematic method for evaluating hazards and for setting appropriate target failure probabilities for instrumented protective measures. As such, it represents an alternative means of setting target Safety integrity levels (SIL) than Layer of Protection Analysis (LOPA).

It usually involves quantifying the frequency of occurrence of hazardous events, estimating the likely consequences and comparing the result with some agreed criteria. A hazardous event is defined as any event that has the potential to cause loss, damage or undesirable effect on plant, equipment, product, people, the environment or profit.

Hazard analysis thus enables the risks associated with a particular hazard to be calculated and hence helps to clarify:

a. Is the level of risk acceptable?
b. Is a particular expenditure justified?
c. Which hazardous events present the greatest risk and therefore which should be dealt with first?
d. Which design is the safest or most reliable?

The necessity for the application of such a technique arises not only from the need to design the safest and most economical plants and to operate them efficiently, but also to ensure that maximum returns are achieved from expenditure on safety.

In the past the question “How safe is safe?" may have been answered only qualitatively. Plant designers and managers have had to rely on judgement based on, perhaps, a limited amount of experience. This question around safety criteria is now addressed in the document” Risk Management Standard and Matrix” [8], which provides guidance on what is required, and should be used for selecting target frequencies for any Numerical Hazard Analysis (NHA).

Although serious incidents arising from errors of judgement have been uncommon, chemical plants have grown in complexity and size, and are operated nearer critical limits and at higher pressures and temperatures than previously. As a result, the decisions on safety and reliability are more difficult to make, because the consequences of error are potentially more serious.

Note:In order to claim a RRF for any IPL, the IPL under consideration must be independent from the listed initiating causes and any other IPLs that the team has already claimed for risk reduction

[8] Document Reference:IVL EHS-208; Title: “Risk Management Standard and Matrix”

Hazard analysis provides a rational method of assessing risks so that decisions can be made with a greater element of certainty.

An attraction of the technique is that it permits a cost-effective analysis to be carried out on safety expenditure, so that in many cases where damage resulting from a hazardous event would be extensive, the expenditure could also be shown to be "good business", as well as giving increased safety.

This document seeks to take the user through the various steps involved in a hazard analysis so that simple problems can be tackled. It must be emphasised that there are many pitfalls that await the unwary and inexperienced analyst.

As a result, it is important that once a preliminary hazard analysis has been carried out it should be discussed with an experienced analyst.

D.3 Hazard Analysis Approach

It is important to appreciate when considering hazards, that there are two main stages: hazard identification and hazard assessment. Hazard analysis is used in the latter stage.

D.3.1 Hazard Identification

There are a number of ways in which a hazard can be identified; reference IVL EHS-403, Process Hazard Analysis. It may be obvious, it may have actually occurred, or it may be identified by the use of a specific technique such as a Hazard and Operability Study (HAZOP), safety audit, use of a checklist etc.

D.3.2 Hazard assessment

There are a number of methods used to decide what to do about a particular hazardous event. The answer may be obvious, may be based on previous experience or may be obtained from a Code of Practice. However, in many cases hazardous events are identified which cannot be handled in this way.

Hazard analysis can be used to assess such hazards and the effectiveness of imposed solutions. However, hazard analysis should not be an excuse for accepting poor designs - if the arrangement is clearly unsatisfactory and can be improved economically, and then this should be done rather than using hazard analysis to justify the status quo. Where inherent EHS solutions can be provided, there will be greater confidence that the system will operate safely.

D.3.3 Basic Stages

There are four main questions that need to be answered by a hazard analysis:

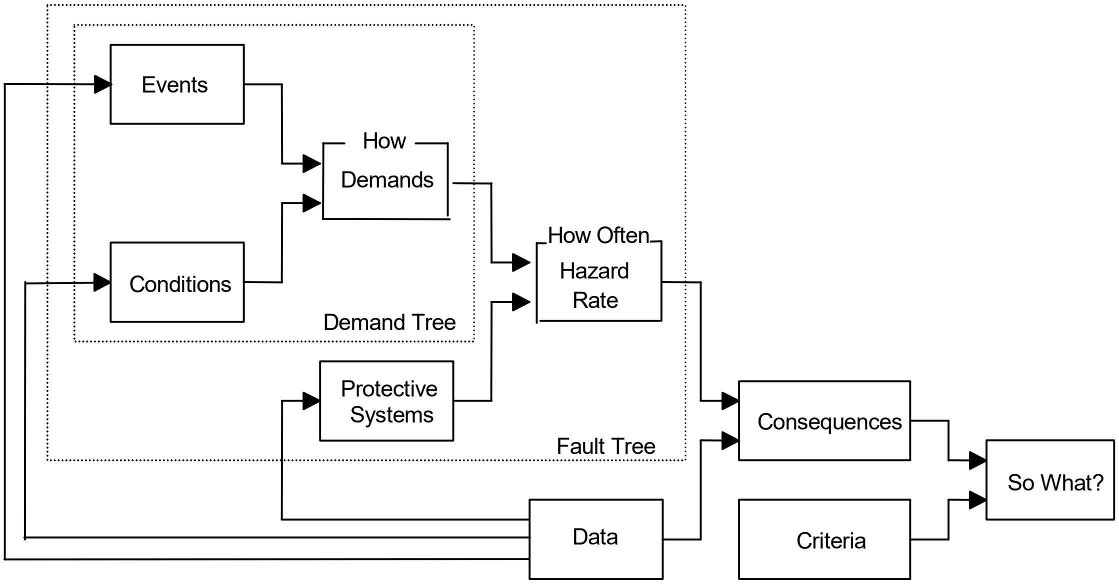
a. HOW can the hazardous event occur?
b. HOW OFTEN will the hazardous event occur?
c. What are the CONSEQUENCES?
d. SO WHAT? Is the situation acceptable or should some action be taken?

Before going on to discuss these questions in more detail, it is necessary to introduce certain other aspects of hazard analysis. Invariably protective systems are encountered. These range from alarms to initiate operator intervention to devices such as relief valves, bursting discs, instrument trip systems which are installed to prevent the hazardous event occurring.

For example, if the hazardous event is "overpressure" then the protective device could be a relief valve. A situation that requires the protective system to operate is said to put a demand on the protective system. The frequency of demands on the protective system is known as the demand rate. If the protective system fails to operate then the hazardous event will occur. The frequency with which the hazardous event occurs is the hazardous event rate. Thus, protective systems act like filters that prevent most of the demands from causing hazardous events.

Figure D-1 shows diagrammatically the stages of hazard analysis. It represents how demands occur on a protective system and how some of the demands result in hazardous events.

FIGURE D-1 BASIC STAGES OF HAZARD ANALYSIS



The most common technique for analysing HOW a hazardous event can occur is fault tree analysis. The first step is usually to draw up a demand tree, which shows all the basic events that could lead to the hazardous event. This excludes all protective systems and operator interventions to correct faults.

The fault tree for the hazardous event is produced by taking the demands identified in the demand tree and including the effects of the protective systems and the operator interventions.

The fault tree may then be quantified by applying failure data to calculate the hazardous event rate i.e., HOW OFTEN. Events and conditions are characterised by “frequencies” and “probabilities”. Protective systems are characterised by “PFDavg” (Average Probability of Failure on Demand), the probability that the system will fail to work when required.

The CONSEQUENCES can then be estimated and finally the appropriate “Criteria” applied in order to assess the situation and determine the necessary action i.e., SO WHAT.

D.3.4 Detailed Stages

For more detailed hazard analyses, the four basic steps already described may be broken down into more detailed activities.

D.3.4.1 Define the Hazardous event

It is important to have a clear and accurate definition of the hazardous event as this simplifies and assists the subsequent stages of the analysis.

D.3.4.2 Establish the Effects (Consequences) of the Hazardous event

This, depending upon the type of hazardous event under scrutiny, may in itself involve a detailed study and may require expert advice.

D.3.4.3 Agree criteria against which the consequences of the event will be judged.

It is sensible to agree the appropriate criteria at this early stage. The criteria will be based on an assessment of the potential consequences and the corresponding target frequency from the table in the document IVL EHS-208.

A rough analysis may show clearly that the hazardous event frequency or consequences are either insignificant, in which case no furthermore detailed analysis is needed, or are completely unacceptable and significant changes are needed to meet the criteria. This is a strong prompt to look for improvements that are inherently better for EHS protection. Where a rough analysis indicates the consequences of the hazardous event are very significant and the frequency is not obviously adequate to meet the criteria, more detailed analysis may be required if inherent EHS improvements cannot cost-effectively allow the criteria to be met.

D.3.4.4 Assemble Information Describing the System

The system to be studied may be a new design or an existing plant. In either case, it is essential to become familiar with the actual or proposed hardware and the actual or proposed operating and maintenance procedures. Line diagrams and operating instructions etc. will generally provide most of the necessary information. If the plant exists, then a plant visit is advisable.

D.3.4.5 Analyse the Causes of the hazardous event

If the systems are complex and interrelated, then the following stages may be helpful:

a. Draw a simplified sketch of the system showing all the instruments but omitting equipment that is not relevant.
b. Draw up a demand tree to show all the possible causes of the hazardous event but excluding protective systems and operator intervention.
c. Develop the fault tree from the demand tree by including the protective systems.

If the system is straight forward then only step (c) or steps (b) and (c) may be necessary.

D.3.4.6 Calculate the hazardous event rate

There are two steps involved here:

a. Collect data for all the initiating events in the fault tree. Wherever possible this data should be obtained from the plant being studied or from similar plants on the same site but where none is available other, less reliable sources should be referred to (see Section D.8).
b. The hazardous event rate can now be calculated using simple probability equations. In certain cases, it may be necessary to carry out a mathematical analysis of equipment failure patterns, but this should be left to experts, as standard procedures are often not applicable.

D.3.4.7 Check the Sensitivity to Uncertain Data and that the Results are Realistic.

In very few cases will good data be available throughout and assumed data will have been used; it is important to determine whether or not variations in such data will have serious effects on the results.

The results of hazard analyses must be realistic. Figures obtained from the fault tree can be compared with those obtained from the plant e.g., frequency of operation of a trip or alarm. Even if an event has not happened on the plant it can still provide useful information, e.g. no events in 5 years means that we could be reasonably confident (about 90%) that the frequency was less than one in 2 to 3 years (assuming that the event is random).

D.3.4.8 Compare the Result with Established Criteria

Having established the effects of the hazardous event and predicted the frequency at which it may be expected to occur, these can be compared with the appropriate criteria.

D.3.4.9 Further steps if the Risks are unacceptable

a. Check through the fault tree for simplifying pessimistic assumptions and repeat any of the above steps as necessary.
b. Suggest possible improvements or modifications. The fault tree helps identify the most significant causes and hence the best areas for achieving an improvement. Inherent EHS improvements should always be considered more favourably than the addition of extra protective systems.

D.3.4.10 Monitor Subsequent Performance

This is particularly important for the more significant hazardous events since the analysis will rely on a number of fundamental assumptions relating to the design, operation and maintenance of the process. If for any reason, changes are made which invalidate these assumptions the results will become meaningless. Monitoring should cover the demands on protective systems, when the protective system was the essential safeguard against a hazardous event, and the failures of the protective systems, found on test or on demand.

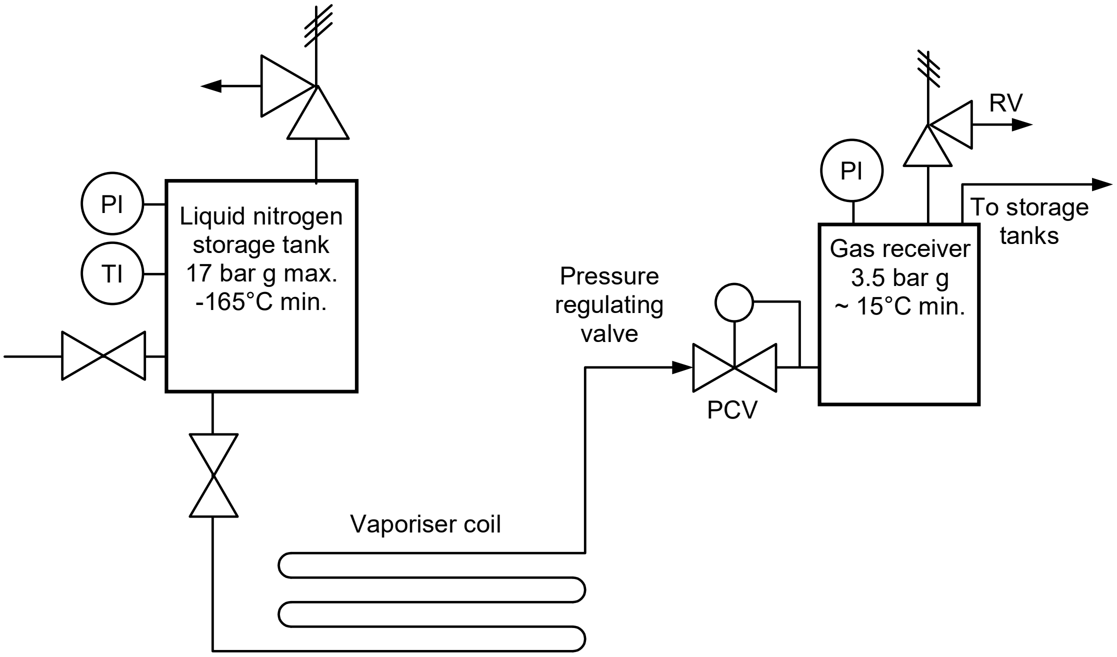
In most studies, certain aspects have to be developed in more detail and with greater accuracy as they are found to contribute significantly to the result of the study. As a result, some of the above steps may have to be repeated a number of times before the hazardous event rate is obtained with sufficient accuracy. In studies that are more complex, there may be a number of different protective systems thus making the calculations more complicated.

D.3.5 Example

In order to demonstrate the hazard analysis technique, a simple example is now introduced and each step in the application of the technique will be carried out on this example.

The example used is a simplified vaporised liquid nitrogen supply system, which is used for blanketing a number of storage vessels. The system consists of a liquid nitrogen tank, a gas receiver, a vaporiser and some valves and instruments as shown below.

Figure D-2 Line Diagram of Simple Nitrogen System



The liquid nitrogen is delivered by a road tanker to the storage tank on a regular basis. The liquid from the tank is fed through a vaporizer coil heated by ambient air. Pressure in the receiver is controlled by the let down valve. The receiver and the line after the vaporizer are not designed to withstand cold liquid nitrogen and the hazardous event to be analyzed is rupture of the line or vessel due to brittle fracture caused by low temperature. No protection against low temperature was fitted; note that the relief valve (RV) on the receiver only protects against vessel rupture due to overpressure, not due to low temperature or to defects in the vessel.

D.4 Analysis of Causes of a Hazardous Event

This is the most important part of hazard analysis and can be the most difficult since it requires the logical synthesis of all possible (significant) causes of the hazardous event. This is usually done by drawing a fault tree. Methods of fault tree construction are described in the technical literature. Mostly these are techniques more suited to complex problems and for expert use, sometimes involving computers.

The two-stage method of fault tree construction described here is much simpler and lends itself to manual calculation.

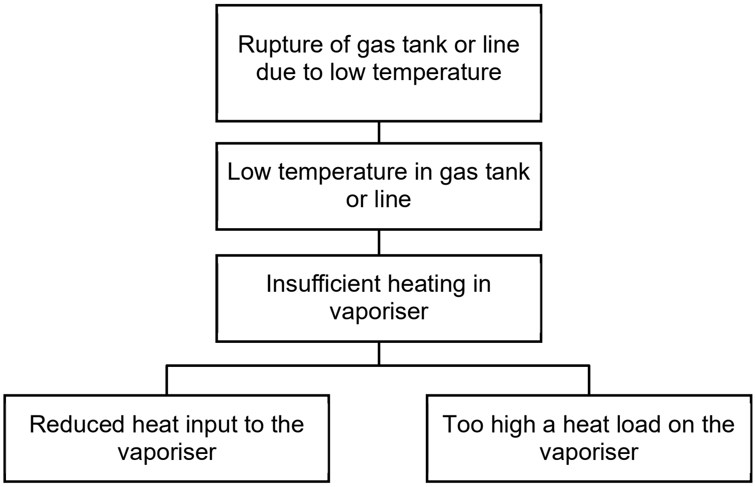
D.4.1 Demand Tree

First, the top event of the demand tree is selected. In a simple analysis, this would usually be the hazardous event itself. In a more complex analysis, several demand trees might be drawn with top events that were each contributing causes of the hazardous event. The demand tree is started by writing down the top event at the top of the page and working down. Once the top event has been fully defined and written down, then the question “how can it happen?” is asked. In deciding what events can potentially cause the top event, it is essential to think in small steps so that each branch of the demand tree is expanded to end in a discrete event that is amenable to quantification, for example, an equipment failure or a human error.

The method of constructing the demand tree will be demonstrated using the example already described. Here the hazardous event is “rupture of the line/vessel due to low temperature” and this would be the top event (see Figure D-3).

The next step is to identify the various causes of this top event by developing the demand tree in small steps. The steps might be “rupture of the line” is caused “by low temperature in the line” which, in turn, is caused by “insufficient heating in the vaporiser”. This might be caused either by “reduced heat input to the vaporiser” or “too high a heat load on the vaporisers”.

FIGURE D-3 NITROGEN SYSTEM - START OF DEMAND TREE FOR RUPTURE OF LINE DUE TO LOW TEMPERATURE


Rupture of gas tank or line due to low temperature
Low temperature in gas tank or line
Insufficient heating in vaporiser
Reduced heat input to the vaporiser
Too high a heat load on the vaporiser

These two events are the main ways in which the top event can occur.

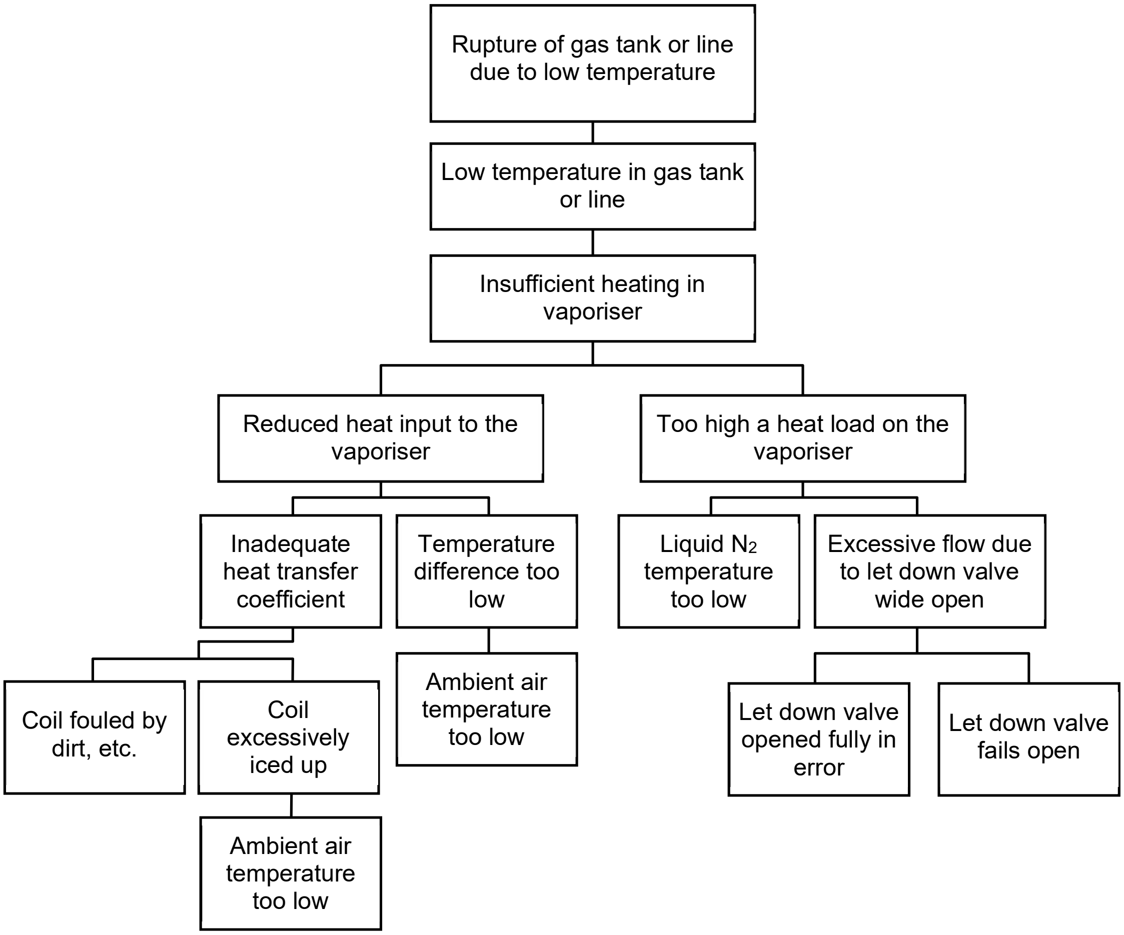
Possible reasons for “reduced heat input” are “low air temperature” or “inadequate heat transfer”. Possible reasons for the “high heat load” are “excess flow” or “reduced liquid temperature”. The developed demand tree is shown in Figure D-4.

Throughout the development of the demand tree a constant watch must be kept for dependent failures. These are faults, events or conditions that can cause the top event via two or more pathways. An instance occurs in the example because “ambient air temperature too low” can cause a “reduced heat input” both by reducing the temperature difference over the vaporiser and by causing excessive icing, which reduces the heat transfer coefficient. To avoid double counting, the dependent failures must only occur once in the tree, and to ensure this, it is usually sensible to segregate dependent failures as entirely separate branches as the tree is developed. Some dependent failures are caused by functional dependency, typically due to instrument air failure, power failure, cooling water failure, etc.

For the purpose of this example, it will be assumed that the events at the end of each branch on Figure D-4 can be quantified.

These can therefore be called the primary causes and it is not necessary to develop the demand tree further.

FIGURE D-4 NITROGEN SYSTEM - DEMAND TREE FOR 'LOW TEMPERATURE IN GAS TANK OR LINE'


Rupture of gas tank or line due to low temperature
Low temperature in gas tank or line
Insufficient heating in vaporiser
Reduced heat input to the vaporiser
Too high a heat load on the vaporiser
Inadequate heat transfer coefficient
Temperature difference too low
Liquid N2 temperature too low
Excessive flow due to let down valve wide open
Coil fouled by dirt, etc.
Coil excessively iced up
Ambient air temperature too low
Let down valve opened fully in error
Let down valve fails open
Ambient air temperature too low

D.4.2 Fault tree

The next step is to construct the fault tree from the demand tree by incorporating the operator interventions and the protective systems.

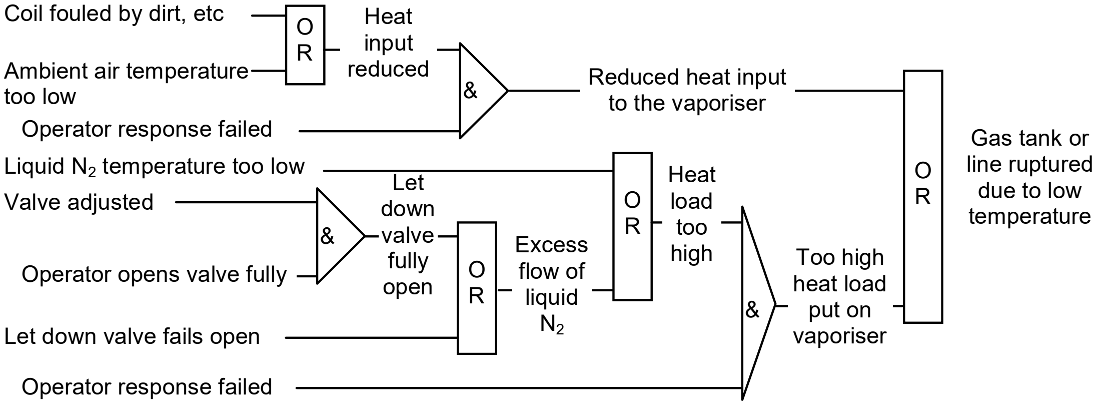
Firstly, the possibility of operator intervention must be considered for each primary cause. If an operator should be aware of the developing hazardous event, (and the need to take action) as a result of alarms, other instrument indications and/or observation of the state of the equipment then the event 'operator response failed' can be combined with the primary cause through an AND gate. That is, the primary event must occur AND the operator fails to respond for the hazardous event to continue to develop.

Secondly, any automatic protection systems (e.g., relief valves, instrumented trip systems) must be considered for each branch of the tree. Where automatic protection is provided and would have time to act then the event "automatic protection (RV, trip) failed" can be combined with the initiating event through an AND gate.

Throughout both these procedures, a careful watch must again be kept for dependent failure effects. For instance, if a primary cause would put an alarm out of action then there might be no possibility of operator intervention. Similarly, if a primary cause would cause a trip system to fail then that trip cannot protect against that particular primary cause.

In the case of the example, there is no automatic protection so that only the possibility of operator intervention has to be considered. The operator is likely to be aware that the ambient air temperature is excessively low, causing excessive icing of the vaporiser coils, or that the coils are fouled. He is very unlikely, however, to notice that the let down valve is wide open. “Operator response failed” is therefore included through an AND gate in each branch of the demand tree. Although it is the same operator who fails to act in each situation, this event is incorporated separately into each branch of the fault tree because the probability of failure to act may be different in the two cases.

FIGURE D-5 THE COMPLETED BUT UNQUANTIFIED FAULT TREE FOR THE EXAMPLE


Coil fouled by dirt, etc
Ambient air temperature too low
OR
Heat input reduced
Operator response failed
&
Reduced heat input to the vaporiser
Liquid N_2 temperature too low
Valve adjusted
Operator opens valve fully
&
Let down valve fully open
Let down valve fails open
OR
Excess flow of liquid N_2
OR
Heat load too high
Operator response failed
&
Too high heat load put on vaporiser
OR
Gas tank or line ruptured due to low temperature

There is not necessarily only one correct fault tree for a particular hazardous event because different people are likely to arrange the branches of the tree in slightly different fashions. In practice this does not matter as long as all the significant primary causes are included and the correct combinations of events through AND and OR gates is achieved. The fault tree must be carefully checked before proceeding to any qualitative or quantitative assessment.

D.4.3 Checking a fault tree

The logic of the branches of the tree can be checked by working along each in turn but the overall validity of the tree may still be invalidated by dependent failure effects. The importance of recognising these at all stages of fault tree construction has already been stressed. A “warning bell” should sound whenever a fault tree is constructed in which the same event appears more than once. If the fault tree cannot be modified to avoid this, an experienced analyst should be consulted to check the validity of the fault tree and to advise on the correct procedure for quantification. A summary of the rules for the construction of fault trees is given in D.13.

D.5 Evaluation of the Fault Tree

The next stage in the analysis is to evaluate the fault tree. This may be either a qualitative or a quantitative procedure. Even with fairly complex problems, visual inspection of the fault tree can often give a good appreciation of the most significant events. For example, any primary cause that leads directly to the “hazardous event” with no other conditions to be satisfied would be immediately apparent. Similarly, the number of AND gates in each branch can give an indication of the relative significance of different routes to the “hazardous event”; the greater the number of AND gates the greater the number of circumstances that have to be satisfied simultaneously for the “hazardous event” to occur. The extent to which reliance is placed upon the operator to safeguard against the hazardous event arising can be judged, particularly if there are branches in the tree containing operator intervention as the only protection.

However the analysis of the hazardous event becomes more complete if the fault tree is quantitatively assessed so that more confident, measured judgements can be made with respect to the significance of different events and the acceptability or otherwise of the hazardous event under review.

D.5.1 Quantitative assessment

In constructing the fault tree the objective is to develop each branch to arrive at primary events that are amenable to quantification. Three basic parameters may be used to quantify events. These are frequency, duration and probability.

a. The frequency is the average number of times/year that the event (failure, demand, operator action, etc.) occurs.

b. The duration is the length of time for which the event state exists.

c. The probability is a measure of uncertainty expressed numerically between 0 = impossibility and 1 = absolute certainty. It either refers to the probability of an event occurring or the probability of a state existing. Probability is dimensionless.

These three parameters are simply related:

Probability (of a state existing) = frequency x duration (D.5.1)

In order to quantify a fault tree it is necessary to have some appreciation of probability theory and to know how to combine the various event parameters through AND and OR gates.

D.5.2 Probability

D.5.2.1 Simple Probability of Events occurring

The calculation of a single event probability is a relatively simple matter.

For example, the probability of throwing a 6 in a single cast of a die is simply one chance in six or 1/6. Each of the possible outcomes, 1 to 6, is equally likely.

However, when considering the probabilities of a number of events the calculation of probabilities is not always so simple.

This can be demonstrated by asking the question, 'what is the probability of throwing a 6 if the die is thrown twice?" An obvious answer to this question is to say that the required probability is simply the sum of the probabilities of throwing 6 in the first throw and a 6 in the second throw. This leads to the answer 1/6 + 1/6 = 1/3. If however another question is asked: "What is the probability of throwing a 6 in seven casts of the die?" it is immediately apparent that the above argument leads to a probability greater than unity which is clearly in error.

A simple method of clearly illustrating this problem is to construct a "truth table", which details all possible outcomes from throwing a die twice. The table is constructed in terms of the probabilities of the event of interest. In this case, the event of interest is the throwing of 6, which is a success (S), and no 6, which is a failure (F).

The probability of throwing a 6 in one throw is 1/6 and not throwing a 6 is 5/6.

Truth Table

	1st throw	2nd throw	Probability		
All Possible Outcomes	S	S	1/6 x 1/6 = 1 /36	2 sixes	Events of interest
	S	F	1/6 x 5/6 = 5 / 36	1 six	
	F	S	5/6 x 1/6 = 5 / 36	1 six	
	F	F	5/6 x 5/6 = 25 / 36	No sixes	
			1		

Hence the probability of throwing a 6 at least once is 1/36 + 2 x (5/36) = 11/36

This can also be worked out using the fact that the sum of all the probabilities is unity and so

Probability of success = 1 - probability of failure
= 1 - 5/6 x 5/6
= 11/36

Or, Probability of success = 1 - (l -1/6) (1- 1/6)
= 1/6 + 1/6 - 1/6 .1/6
= 11/36

Therefore, it can be seen that probability of throwing a 6 in the first throw OR the second throw is the sum of the individual probabilities, but the product must be subtracted.

D.5.2.2 Simple probability of a state existing

To estimate the probability of a state existing, use is made of the Equation D.5.1. If, for instance, we need the probability of a piece of equipment being in a failed state, i.e., its "Unavailability".

"Unavailability" = F Tr (D.5.2)

Where, F is the failure frequency of the equipment per year, and Tr is the average repair time in years.

D.5.2.3 Combination of Probabilities

Simple equations for the combination of probabilities can be written down. If PA is the probability of event A occurring and PB is the probability of B occurring then:

$P_{(A \text{ and } B)} = P_A.P_B$ (D.5.3)
$P_{(A \text{ or } B)} = P_A + P_B - (P_A P_B)$ (D.5.4)

If the probabilities P_A and P_B are small (P_A, P_B<< 1) then the product can be neglected and so

$P_{(A \text{ or } B)} = P_A + P_B$ (D.5.5)

Example

The following simple example illustrates the use of these equations.

Consider two pumps A and B both working together in parallel on a plant. If each pump fails on average twice per year and the repair maintenance work takes two days each time, what are the probabilities of

(a) Only one pump being available (b) no pumps being available?

Probability of either pump being in a failed condition = $P_A = P_B$ = 2 x 2/365 = 0.011

Probability of only one pump being available is given by:

$P_{(A \text{ or } B \text{ failed})} = P_A + P_B - P_A P_B$
= 0.011 + 0.011 - 0.0001
= 0.022

The probability of neither pump being available is given by

$P_{\text{(A and B failed)}} \quad = \quad P_A \, P_B$

$= \quad 0.011 \times 0.011$

$= \quad 0.0001$

N.B. It is assumed that the failures are independent and that pump failure rate is a constant.

D.5.2.4 PFDavg

A significant part of hazard analysis is concerned with protective systems such as relief valves and instrument trip and alarm systems. When a protective system fails in such a manner that the failure is not immediately revealed and the fault will cause the system to be inoperative (i.e. a fail to danger fault) then the system will remain in a failed state until a hazardous event occurs and places a demand on it, or until it is tested and repaired.

For protective systems a special term, PFDavg is used to describe the average probability that the system is failed and unable to provide the required protection.

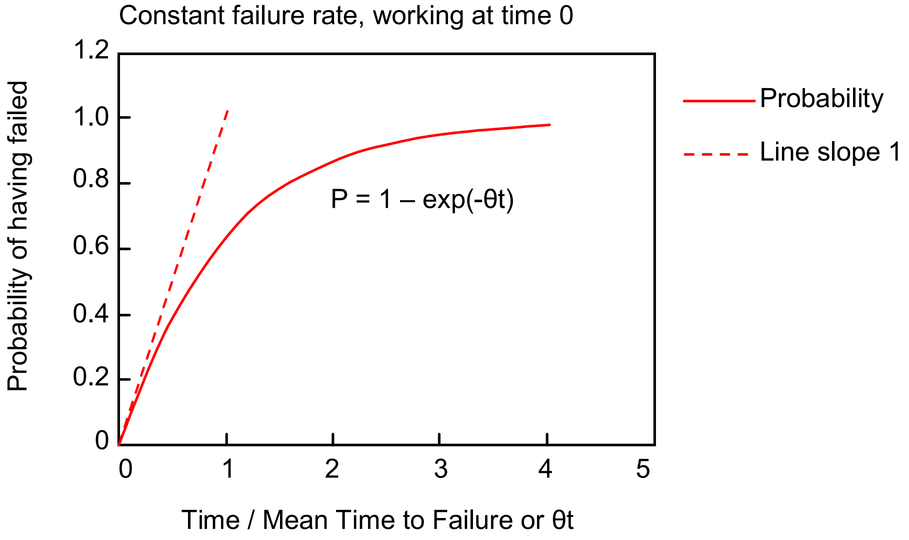
Fractional Dead Time (FDT) has been used previously for this purpose, but it has now been superseded in international standards by PFDavg.

A protective system may be unable to provide protection because of an unrevealed fail-danger fault, but also because, for instance, it is being tested or it has been left off line after a test.

Proof testing discloses unrevealed fail-to-danger failures so that they can be repaired, thus limiting the time for which a protective system is failed.

If we have an item of equipment or a system that is known to be working at time 0, then the probability that it will have failed will increase with time, until ultimately the probability of having failed approaches 1. The simplest model for failures, and the one most commonly used is the constant failure rate.

FIGURE D-6 PROBABILITY OF HAVING FAILED VERSUS TIME



For constant failure rate of θ per year, the probability of having failed PFD is given by:

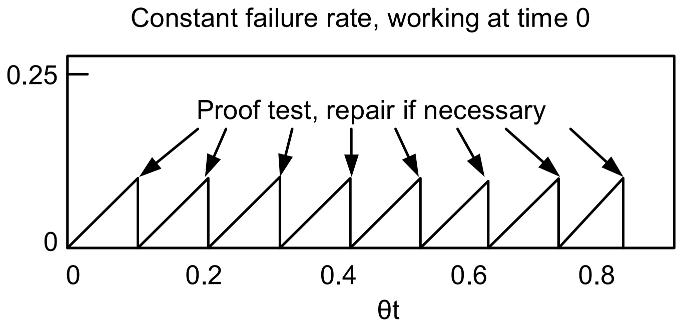
PFD = 1 - exp (- θt)

Where t is the time in years and θ is the failure rate per year.

Where θt is small, say less than about 0.2, the numerical difference between θt and the exact expression 1 - exp (- θt) is small and can be considered negligible for practical purposes.

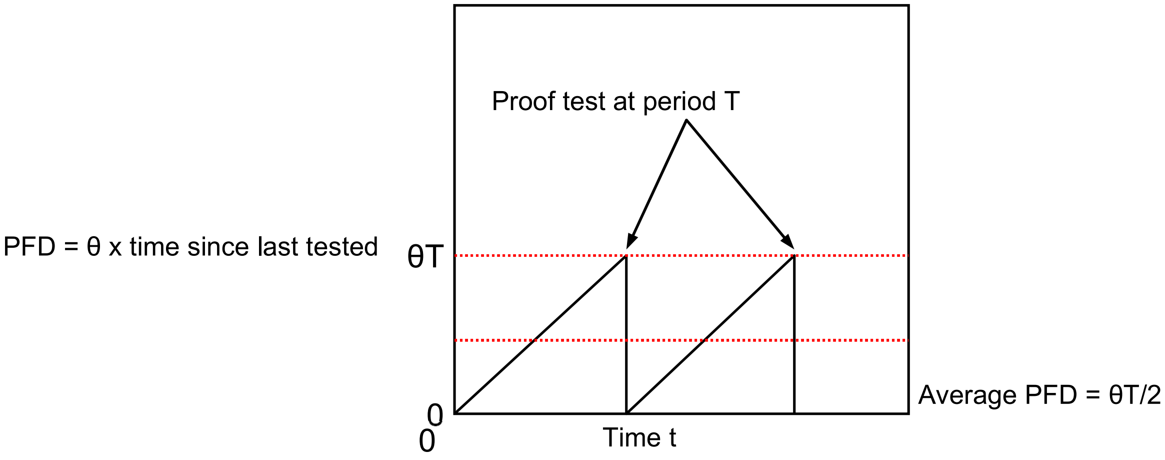
Hence, the assumption can be made that PFD is near enough equal to θt.

Figure D-7 Effect of Proof Testing



The probability of having failed varies from 0 immediately after a proof test to θT immediately before a proof test, where T is the proof test period.

Figure D-8 Average Probability of Failure on Demand (PFDavg)



Hence on average the probability of being failed (PFDavg) is:

PFDavg = θT / 2 (D.5.6)

This simple expression for PFDavg assumes that θT is small, typically less than 0.2.

A useful rule of thumb for checking the validity of the condition θT << 1 is that the average time between failures (1/θ) should be much greater than the test interval.

Example

An example of the calculation of the PFDavg is as follows. A particular protective system has a fail-to-danger failure rate of 0.2/year and is tested every three months. i.e., θ = 0.2 /year and T = 0.25 years

Hence PFDavg = 0.2 x 0.25 /2
= 0.025

This means the system will be “dead" for 2.5% of the time, which on average is equivalent to about 9 days per year. This information is useful, particularly if two or more alternative protective systems are being compared, but it is insufficient for deciding how good the protective system needs to be. This needs the demand rate on the system to be evaluated also. Checking the validity of the condition $\theta T << 1$, in the above example with θ = 0.5/year the time between failures is 2 years which is much greater than the proof test period of 3 months. If the time between tests is not small compared with the mean time to failure, the trip system will be only slightly more reliable than one not tested at all.

D.5.3 Frequency

D.5.3.1 Frequency and rate

The terms frequency and rate both have the units $(\text{time})^{-1}$ but only under some circumstances are they one and the same parameter. Often they are interchanged loosely, which can cause some confusion.

Strictly, for hazard assessment, they can be defined as follows:

a. Frequency is the number of times an event occurs in unit elapsed time.
b. Rate is the number of times an event occurs in unit working (on-line running) time.

Frequency equals rate if elapsed time equals running time.

This can be illustrated if we take two pumps A and B again.

Each pump fails twice per year and runs all year hence for each pump:

Failure frequency = failure rate
= 2 /year

Now consider two other pumps C and D: one working and one spare.

Assume each pump on average fails twice per year and runs for 50% of the time, in this case:

Failure frequency of each pump = 2 /year

Failure rate of each pump = 2 / 0.5 /year
= 4/year

The failure rate is the number of times each of the pumps would fail if it ran for a full year.

Proper definition of frequency and rate can be important for correct evaluation of a fault tree. Some failure data is given as rate and some as frequency, but as can be seen above, wrong use of these can have a significant effect on the calculated results.

D.5.3.2 Combination of event frequencies

If the frequencies with which two independent events occur are F_A and F_B then the frequency which either A or B occurs is:

$F_{(A \text{ or } B)} = F_A + F_B$ (D.5.7)

The frequency of an event, A, occurring at the same time as a state, B, exists is given by

$F_{AB} = F_A P_B$ (D.5.8)

This rule can then be used to calculate the frequency of two events A and B occurring together given that the duration of the two events is t_A and t_B:

$F_{(A \text{ and } B)} = F_A$ x (proportion of time B lasts)
+ F_B x (proportion of time A lasts)
$= F_A P_B + F_B P_A$
$= F_A F_B t_B + F_A F_B t_A$
$= F_A F_B (t_A + t_B)$ (D.5.9)

i.e, the product of the two event frequencies and the sum of the durations.

The average duration of the combined event, t, is given by:

$t = t_A t_B / (t_A + t_B)$ (D.5.10)

It must be noted that, unlike probability, both frequency and duration have dimensions; therefore, it is vital to express them in consistent units when using these equations.

Application of these equations is mostly straightforward especially when considering events that are randomly spread over the same time scale. This is the case when considering coincidence of faults, say, in different items of continuously running equipment. However there are pitfalls when the time scales of events are not concurrent as for example when considering coincidence of faults in items of equipment not all continuously running. It is then often better to work through the quantification by logical deduction. This can be illustrated by further consideration of the pump example.

Pumps C and D, one running, one spare. Each pump fails suddenly twice per year. Repair takes 2 days per failure. On average, each pump runs for 50% of time. How often will there be no spare pump available when the running pump fails?

The running pump (either C or D) fails a total of 4 times/year.

There is no spare pump (either C or D) available for a total of 4 x 2 = 8 days/yr.

Hence, assuming the failures are independent and the failure rates are constant the frequency of no spare pump available when the running pump fails is given by equation D.5.8:

= (frequency of running pump failing) x (probability of no spare available)
= 4 x 8 / 365
= 0.088 /year

D.5.3.3 Hazardous event rate

The "hazardous event rate" is the number of times per year that the "top event" (i.e. the hazardous event) occurs. This is the ultimate objective of quantification of the fault tree. It may be calculated by combining event frequencies and probabilities as described above but when protective systems are involved, some different procedures are required to handle the special probability, PFDavg.

The event that requires a protective system to operate is defined as a "demand" and the frequency with which a demand occurs is known as the "demand rate" commonly denoted by D. If the hazardous event rate arises as a result of the protective system failing to operate when a demand is placed on it then the hazardous event rate, H may be simply calculated as follows:

$$H = D \times PFDavg \qquad (D.5.11)$$

However this simple equation is not always applicable and is only valid if $DT<<1$ and also $\theta T<<1$ to make the computation of PFDavg by equation D.5.6 valid. (θ and T are as defined in Section D.5.2.4)

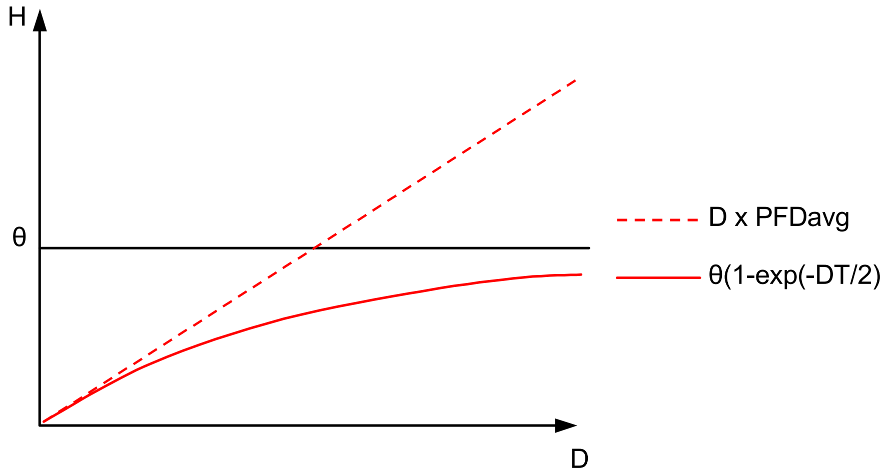
If $DT<<1$ is not satisfied, because the demand rate is high, then the following equation can be used for simple single channel systems only (see Section D.7).

$$H = \theta\,(1 - \exp(- D\,.T\,/2)) \qquad (D.5.12)$$

This expression is valid for any value of D but requires the condition $\theta T<<1$; in most practical situations the latter condition will almost inevitably be satisfied.

The applicability of equations D.5.11 and D.5.12 can be best understood by looking at Figure D-9, which shows the relationship between H and D.

FIGURE D-9 COMPARISON OF HAZARD RATE EQUATIONS



This illustrates clearly how the simple equation D.5.11 will over-estimate (perhaps grossly) the hazardous event rate at high demand rates. At high demand rates, the hazardous event rate tends towards the failure rate of the protective system.

If no proof testing of the protective system is carried out but repairs are made if a hazardous event occurs i.e. if a demand demonstrates that the protective system is faulty, then the hazardous event rate is given by:

$$H = \theta.D / (\theta + D) \qquad (D.5.13)$$

This simple equation however, is a "long time" average and in many cases will seriously overestimate the hazardous event rate. If, in an analysis, an unacceptable hazardous event rate results from using equation D.5.13 then the quantification should best be checked by an expert.

An important point to remember is that, regardless of the conditions, the hazardous event rate can never exceed either the demand rate or the failure rate of the protective system.

The following example illustrates a calculation of hazardous event rate.

Example

A relief valve is tested every two years. If the demand rate, D, is 0.1/year and the fail-to-danger failure rate of the relief valve is 0.01/year, what is the hazardous event rate for the relief valve failing to prevent overpressure of the equipment?

PFDavg = 0.01 x 2 / 2
= 0.01

Before evaluating the hazardous event rate, check the limiting condition:

D T = 0.1 x 2
= 0.2 (which is much less than 1)

Hence H = D x PFDavg
= 0.1 x 0.01
= 0.001 /year

In other words, the hazardous event will occur every 1000 years on average.

It is useful to see how equations D.5.11 and D.5.12 differ depending on the value of D x T. The following table shows the values for the above example:

D	H = D x PFDavg	H= θ (1 - exp(- D.T /2))	D x T
0.1	0.001	0.00095	0.2
0.2	0.002	0.0018	0.4
0.4	0.004	0.0033	0.8
0.5	0.005	0.0039	1.0
1.0	0.01	0.0063	2.0
5.0	0.05	0.0099	10.0
10.0	0.1	0.01	20.0

When DT = 1 the difference between the equations is only about 25% but for higher values it very quickly increases.

D.5.4 Quantification of the fault tree

The preceding sections have described the basic tools necessary to be able to evaluate a fault tree and quantify the top event. Mostly it is required to finish with the hazardous event rate. It may help to have the following guidelines in mind:

D.5.4.1 Units for different types of events

a. Demands (or causes) are usually quantified as FREQUENCIES

e.g., equipment fails, operator does

b. States of equipment/environment, operator response failed, protective system failed, are usually quantified as PROBABILITIES

D.5.4.2 Units for the different types of gate

a. OR gates must have the same units applied to all the events

i.e. the basic events are either all probabilities or all frequencies (Equations D.5.4, D.5.5 and D.5.7)

b. AND gates are more varied. There are three possible combinations:

i. Frequency & Probability

(e.g. demand on a protective system, Equations D.5.8, D.5.11, D.5.12)

ii. Probability & Probability

(e.g. duplicated protective system Equation D.5.3 and see Section D.7)

iii. Frequency & Frequency

This only has meaning where the events being combined have durations; otherwise, the result may be dimensionally meaningless (events per square year, for example).

Where events have a duration, e.g. coincidental events like an electric motor sparking coinciding with a flammable release to cause an explosion, then to combine the frequencies through an AND gate the duration of the events must also be known, Equation D.5.9.

The various guidelines and tools will now be used to quantify the example fault tree developed in Section D.4.

Looking at Figure D-5 the following primary events are causes and so need to be quantified as frequencies. An estimate for each from a typical source is suggested for purpose of illustration:

- 'Ambient air temperature too low' 10 times/year from weather data and plant records
- 'Coil fouled' judged to be negligible
- 'Liquid temperature too low' plant experience shows this to be a negligible effect
- 'Let down valve fails open' 0.02/y from equipment reliability data bank

The last basic cause is 'let down valve opened fully in error' which is synthesised by two primary events through an AND gate. The primary event 'valve adjusted' primary event is an operator action and requires a frequency. The 'operator fully opens valve' is an operator error and requires a probability.

- 'Let down valve adjusted' 365/y plant operation requires an adjustment every day
- 'Operator fully opens valve' P = 10-4 (i.e., 1 error in 10,000 operations) routine operation, no stress, chance of error low ‘(see Section D.8)

It will be assumed that the chances of the operator opening the valve when it is not required to be opened are negligible compared with the other causes.

The protective system is the operator but there is no instrumentation to help him. He therefore has to note visual signs, like icing on the vaporiser coils, if he is to take effective action. The events 'operator response failed' require probabilities, which are estimated as follows:

- 'Operator response failed' against reduced heat input: P = 10-2 (i.e., 1 in 100 chance of failure) from achieved performance (see also Section D.8)
- 'Operator response failed' against excessive heat load: P= 1 (i.e., no chance of taking action a) because valve would fail too quickly for the operator to be able to intervene, and b) if the operator has already opened the let down valve wide in error he is very unlikely to correct his own error quickly enough).

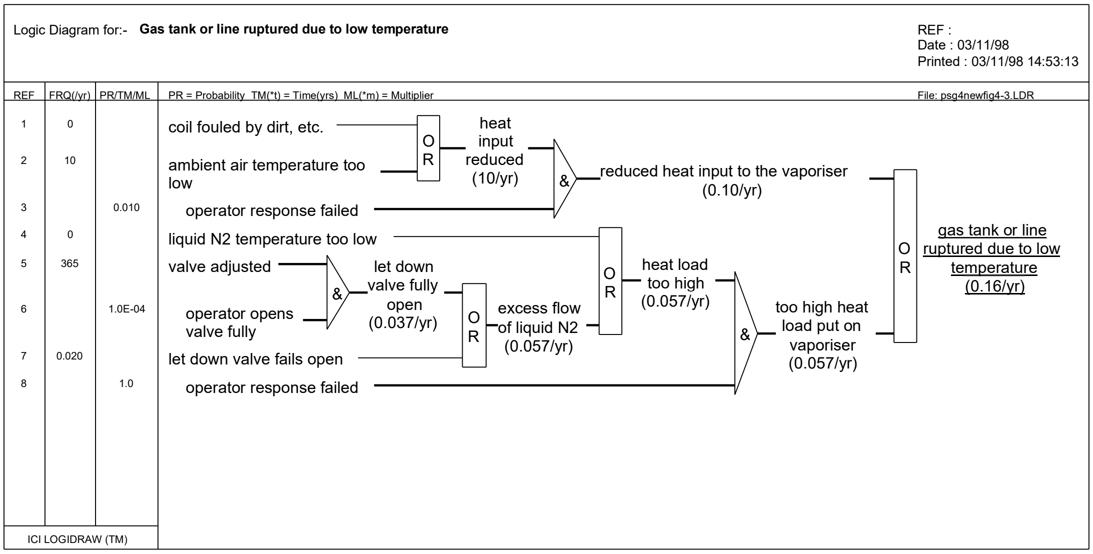
These figures are added to the fault tree in Figure D-10 and evaluation of the various AND and OR gates results in a hazardous event rate of 0.16 times/ year. This may be expressed in a number of ways that may be more or less helpful when assessing the significance of the hazardous event. For instance, we night say that 'rupture of the line' is likely to occur:

0.16 times per year

about 1 in 6 years

or about 1 in 7 chance in any one year.

FIGURE D-10 NITROGEN SYSTEM - QUANTIFIED FAULT TREE FOR HAZARD OF 'GAS TANK OR LINE RUPTURED DUE TO LOW TEMPERATURE'


Logic Diagram for:- Gas tank or line ruptured due to low temperature
REF :
Date : 03/11/98
Printed : 03/11/98 14:53:13
REF
FRQ(/yr)
PR/TM/ML
PR = Probability TM(*t) = Time(yrs) ML(*m) = Multiplier
File: psg4newfig4-3.LDR
1 0
2 10
3 0.010
4 0
5 365
6 1.0E-04
7 0.020
8 1.0
coil fouled by dirt, etc.
ambient air temperature too low
operator response failed
liquid N2 temperature too low
valve adjusted
operator opens valve fully
let down valve fails open
operator response failed
OR
&
heat input reduced (10/yr)
reduced heat input to the vaporiser (0.10/yr)
let down valve fully open (0.037/yr)
excess flow of liquid N2 (0.057/yr)
heat load too high (0.057/yr)
too high heat load put on vaporiser (0.057/yr)
gas tank or line ruptured due to low temperature (0.16/yr)
ICI LOGIDRAW (TM)

Confidence in the result of any fault tree quantification will depend largely on the confidence in the basic data used. Generally when an analysis contains a preponderance of human factors (as with this example) it is more difficult to quantify with confidence than when mostly hardware failures 'have to be considered. The result must always be examined critically. Its sensitivity to variations in the basic data, which may be of dubious accuracy, must be tested. Above all the results must be credible in the light of experience and it is useful to test a prediction against the judgement of people with experience of the system being analyzed. However having said that, it must be remembered that experience can sometimes cloud judgement because of familiarity with a problem: in these circumstances, the rational logical approach of hazard analysis will maybe query the experienced judgement.

Rules for evaluating fault trees are summarized in D.14.

D.6 Criteria for Hazard and Risk Evaluation

D.6.1 Introduction

Whenever some analysis is to be carried out it necessary to establish at the outset what criteria will be used to evaluate the outcome. Hazard analysis is usually focused on a specific hazardous event. The nature of that event will normally be known and understood by those on the site asking for the analysis. Any aspects that are initially unclear will require the analyst to ask questions for clarification.

Hazardous events will generally fall into one of two categories: (a) those where the concern is protection of people and (b) those where the concern is protection of the environment. It is important to establish which is the principal concern and then to use appropriate criteria.

D.6.2 Risk Matrix

Many companies express their approach to risk criteria in the form of a grid or matrix. Figure D-11 has an example matrix.

Figure D-11 Example Risk Matrix
(Refer to IVL EHS-208 for the official risk matrix.)

	Frequency Category							
	$>10^{-7}$ to 10^{-6}/yr	$>10^{-6}$ to 10^{-5}/yr	$>10^{-5}$ to 10^{-4}/yr	$>10^{-4}$ to 10^{-3}/yr	$>10^{-3}$ to 10^{-2}/yr	$>10^{-2}$ to 10^{-1}/yr	$>10^{-1}$ to 1/yr	>1/yr
Severity Category	1	2	3	4	5	6	7	8
A	EHS-2	EHS-3	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4	EHS-4
B	EHS-2	EHS-3	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4	EHS-4
C	EHS-2	EHS-2	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4	EHS-4
D	EHS-1	EHS-2	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4	EHS-4
E	EHS-1	EHS-2	EHS-2	EHS-3	EHS-3	EHS-3	EHS-4	EHS-4
F	EHS-1	EHS-1	EHS-2	EHS-2	EHS-3	EHS-3	EHS-3	EHS-4
G	EHS-1	EHS-1	EHS-1	EHS-2	EHS-2	EHS-2	EHS-3	EHS-3
H	EHS-1	EHS-1	EHS-1	EHS-1	EHS-1	EHS-2	EHS-2	EHS-3

It has a number of categories from which to select to describe the severity of an event and a scale along the other axis to indicate the associated frequency or likelihood to the event. There is usually a numeric scale for frequency on the grid - where shown. Alternatively, the Frequency Categories may be each defined as a specific range.

This grid is by way of illustration - the analyst must refer to the latest version of IVL EHS-208 for the official company matrix.

Essentially, the analyst needs to know Severity Category is appropriate for the specific hazardous event in question and the corresponding Target Frequency below which the risk is regarded by the site/plant as tolerable.

D.6.3 Risk to People

D.6.3.1 On-site risk to people

Risk to people on site is usually expressed in terms of risk to the most exposed person. This is usually risk of fatality.

Consider an event with the potential for an on-site fatality. If the hazardous event frequency is F per year, then the risk to the individual most at risk from the event may be expressed as follows:

Individual Risk = F x P1 x P2 x P3 (D.6.1)

Where

P1 is the probability of person being "at work" at the time of the hazardous event.

P2 is the probability of the person being within range of the hazardous event whilst at work.

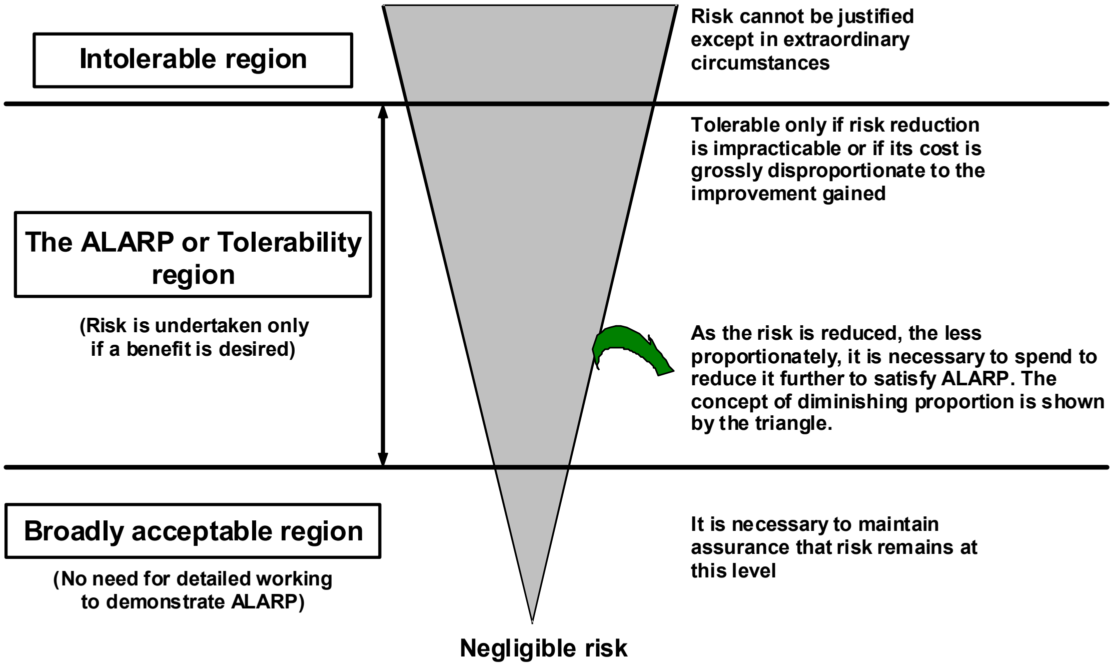
P3 is the probability of person being fatally injured.

A typical value used for P1 is 0.2 - this implies a working year of 8760 x 0.2 hours. This is a good choice if no other information is available. P2 will vary considerably from one situation to another. For a major hazardous event, it is possible for P2 to be as high as 100%, if the person is always in the hazard area when at work. At the other end of the spectrum, it could be as low as 1%. Low figures should be questioned as to whether the person is likely to enter the hazardous area specifically to investigate circumstances leading up to the hazardous event. In other words, the probability of being in the vicinity of the hazardous event is high, even though the person would not normally be there at all. For example, a compressor starts to show signs of vibration and an operator goes to investigate. This could put the operator close to the compressor just when there is a failure. We therefore need to look at the probability that the operator is close to the compressor when a failure occurs rather than use a more general (lower) figure for the operator being close to the compressor. P3 is a more difficult parameter to estimate. For a major hazardous event, P3 is likely to be in the range of 0.1 - 1.0. Figures lower than 0.1 are difficult to support with evidence and should be avoided.

D.6.3.2 ALARP Principle

The diagram in Figure D-12 shows three regions: at the bottom is the broadly acceptable region, at the top there is a region where the risk is so high as to be unacceptable, between these is a region where the level of risk may be tolerated depending on the level of risk and the cost of reducing it. The level of risk in this region must be demonstrated to be As Low As Reasonably Practicable (ALARP). For some regulatory regimes, the use of the ALARP principle is considered essential.

FIGURE D-12 THE 'ALARP' TRIANGLE


Intolerable region
Risk cannot be justified except in extraordinary circumstances
The ALARP or Tolerability region
(Risk is undertaken only if a benefit is desired)
Tolerable only if risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained
As the risk is reduced, the less proportionately, it is necessary to spend to reduce it further to satisfy ALARP. The concept of diminishing proportion is shown by the triangle.
Broadly acceptable region
(No need for detailed working to demonstrate ALARP)
It is necessary to maintain assurance that risk remains at this level
Negligible risk

The risk levels are based on risk from all sources of harm. This includes risk from slips, trips and falls as well as process risk. Another factor to be taken into account is that the person most at risk from the hazardous event being assessed may also be at risk from other hazardous events on site. It is therefore necessary to apportion the level of risk that would be tolerable across all sources of harm. For example, where a person may be at risk from a hazardous event on five different sections of a process, we may divide the risk criteria by 5 when looking at a specific hazardous event on one section. This has been taken into consideration in the setting of target frequencies in the document IVL EHS-208.

D.6.3.3 Off-site risk to people

Off-site risk to the public is assessed in two ways: (a) in terms of individual risk and (b) societal risk.

Individual risk at a location will be based on all the sources of risk across the site. This can usually be illustrated by drawing risk contours around the site and considering where habitation exists around the site. In some instances, there will be areas of population right up to the site boundary; in other cases, the nearest populated areas may be some distance from the boundary.

Societal risk assessment involves consideration of each possible hazardous event and the numbers of potential fatalities. The results are combined to form an F-N curve. This represents the frequency (F) for which there could be N or more fatalities.

Assessment of societal risk is beyond the scope of this document.

D.6.4 Risk to the Environment

Hazard analysis criteria for risk to the environment should be based on the target frequencies for the site.

These are again to be found in IVL EHS-208.

However, if the regulatory regime for the site requires more stringent criteria than those target frequencies in IVL EHS-208 then the more stringent criteria should be used.

D.7 Protective Systems

Protective systems are installed on chemical plants to reduce the chances of hazardous events occurring. They protect the plant, personnel and the environment from damage when failures occur.

This document cannot deal in detail with every aspect of instrumented protective systems and detailed further guidance should be obtained from references given later.

Broadly speaking protective systems are either automatic, mechanical devices such as relief valves and bursting discs or instrumented protective systems that will render the plant safe in the event of some specified condition arising.

It is not always possible to have fully automatic instrumented protection so that an instrumented protective system may consist of

a. Automatic action and alarm, or
b. Alarm + operator action

For a type (b) system, the operator's reliability has to be taken into account when assessing the adequacy of the system. It should be noted that (a) can be degraded to (b) on occasions when the automatic system is being maintained or has been partly defeated for test purposes and thus reduce the reliability of a type (a) system.

An instrumented trip system broadly comprises three parts:

a. The initiator monitors the process variable of concern and provides a signal when a set point is reached, then
b. The logic transfers the signal from the initiator, mostly via electronic devices, relays and wires, to
c. The actuator carries out the appropriate action e.g. a trip valve that shuts to stop a process flow.

A system comprising one initiator, logic and actuator is called a "single channel" system.

The assessment of the adequacy of a protective system requires the consideration of two main factors, capability and reliability.

Firstly, the system must be capable of performing its required function. For instance, it must be able to respond quickly and precisely enough to a developing hazardous event so that effective action can be taken in time to prevent the full hazardous event occurring. In an analysis of an existing system, its capability should always be queried and checked. When an analysis is done for the design of a new system, it may be necessary to make some assumptions concerning the system capability. Those assumptions e.g. a particular speed of response must then become part of the design specification for the system.

Secondly, the effect of possible system conditions and faults on the reliability of the system must be evaluated. There are two aspects to consider:

1. "Reliability for safety"' - will the system perform its function when required to do so?

2. “Reliability for production" - to what extent will faults in the system cause undesirable interruptions to production?

The two aspects may be inter-related.

There are two principal modes of failure that can affect the reliability of a protective system.

“Fail danger" (i.e. a fault that would prevent a protective system operating when required to do so)

“Fail safe” (i.e. a fault that would cause a protective system to operate without a demand being made on it - a ‘spurious trip'

The fault might be “revealed" or “unrevealed".

D.7.4.1 Reliability for safety

Unrevealed fail-to-danger failures are those relevant to this aspect of reliability. In order to identify and correct fail-to-danger failures it is necessary to regularly proof test the protective system in order to find and remove those faults before a demand occurs. To be effective the proof testing frequency must generally be much higher than the frequency of demands on the protective system.

The reliability of a protective system is normally expressed by its PFDavg. This is the proportion of time that the system is in a failed state and unable to provide the protection for which it was designed.

There are three main causes of “dead" time in protective systems in general and instrument trip systems in particular. For a simple, single channel protective system these are:

D.7.1.1 Failure of the trip system itself

This part of the PFDavg was introduced in section 5.2.4 and is given by:

PFDavg1 = $\theta T/2$ if $\theta T<<1$ (D.7.1)

Where θ is the fail to danger failure rate, per year and T is the proof test period in years

D.7.1.2 Due to testing

The trip system may be out of action while it is being proof tested and so:

PFDavg2 = $t / (8760 . T)$ (D.7.2)

where t is the time in hours that the trip system is disarmed (defeated) for testing.

D.7.1.3 Due to errors in testing

There is the possibility that errors made in the testing procedure could leave the system disarmed until the next test. To allow for this:

PFDavg3 = ne (D.7.3)

Where n is the number of operations in the testing procedures where an error could leave the system disarmed, and e is the probability of human error per operation

Alternatively, ne can be rolled up as p the overall probability of the system being left in a disarmed state after each test.

Thus, the total PFDavg is given by the sum of the three parts:

PFDavg = □ T /2 + t/ (8760 . T) + ne (or p) (D.7.4)

For a simple instrument trip, system, for example, the various parameters might have the following values:

θ = 0.3 /year

t = 1 hour

n = 5 operations per test

e = 10^{-3} errors /operation

Hence from equation D.7.4

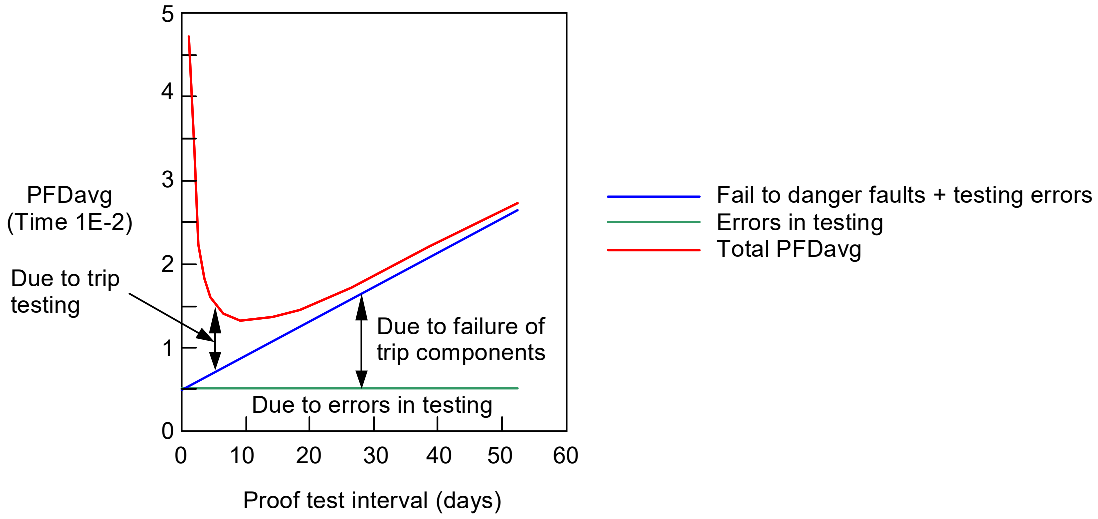
PFDavg = 0.15T + 1/(8760 T) +0.005

This equation is plotted in Figure D-13 and shows that the minimum PFDavg is 0.012 and that it occurs for a proof test period of 10 days. In practice, it is both undesirable and mostly unnecessary to test simple trip systems so frequently. Test intervals of 1 to 3 months are typical. At these test frequencies the dead time due to testing (both down-time and errors) can be neglected and for most situations equation D.7.1 will be adequate and the practical minimum PFDavg for a simple trip is usually assumed to be of the order of 0.01 to 0.03. Operating experience on many plants has shown that this level of reliability is acceptable for the majority of instrumented protective systems.

A number of important assumptions are implicit in equation D.7.1 and must be remembered:

a. Failures are random - a situation where the exponential distribution can be applied
b. The items of equipment are in their useful life phase
c. Failures are independent - no propagation from component to component
d. Repair of equipment is perfect
e. Testing is perfect i.e. failures will always be detected
f. The product of failure rate and test interval
(□ x T)<<1
g. The process is operating continuously (8760 hours per year)

FIGURE 2 FIGURE D-13 PFDAVG OF A SIMPLE TRIP SYSTEM



It is apparent that each trip system has its limitations. The PFDavg may be reduced by increasing the frequency of testing but this could be expensive in terms of maintenance time and, in the limit, can in fact increase the PFDavg. One way to improve the "reliability for safety" is to duplicate part or all of the system. This is known as providing some redundancy in the system. For instance if two similar trips are installed to stop flow into a vessel in the event of rising pressure, then both have to fail to leave the vessel unprotected. Conversely, only one of the two needs to function to give protection and the system would be described as a "one out of two" channel protective system. The PFDavg due to system faults would be greatly improved and given by the following expression:

PFDavg (1oo2) = $(\theta^2 T^2) / 3$
= 4/3 x (PFDavg (1oo1) $)^2$ (D.7.5)

assuming both channels are identical, are tested at the same time and no faults affect both channels simultaneously. Table D-1 summarises the expressions for calculating the PFDavg due to component failure for systems with redundancy.

Taking the simple trip system considered above, duplicating it and testing monthly (i.e. T = 1/12 years) then the PFDavg due to fail to danger faults is as follows:

PFDavg (1oo1) = FT / 2
= 0.3 x 1/12 /2
= 0.013

PFDavg (1oo2) = $1/3\ (0.3 \times 1/12)^2$
= 0.0002

Now the latter figure is considerably less than the PFDavg due to error in testing and so is obviously not the major contribution to the overall PFDavg.

D.7.1.4 Dependent failures

Simple dependent failures to watch for are the simultaneous blocking of impulse lines by impurities, loss of air or power supply but more obscure dependent failures can occur for particular systems.

Also potential dependent failures can be created when the system is installed, for instance if all the cables for each channel of a multi-channel system were installed along the same route then they might all be easily damaged at the same time by some incident.

D.7.1.5 Beta Factor Method for Assessing Dependent (Common Mode) Failure

The Beta Factor Method is the simplest method for assessing the effect of dependent failures. The total fail danger failure rate is made up of independent failures and dependent failures.

The beta-factor is the ratio of the dependent dangerous failures to the total of all dangerous failures.

$\beta = \theta_{cm} / \theta$ (D.7.6)

where θ_{cm} = Frequency of dependent dangerous failures and θ = Frequency of all dangerous failures.

The frequency of dependent dangerous failures is usually much lower than that of other failures.

Typical estimates of beta:

Instrument configuration.	Beta
Identical channels	0.15
Diverse hardware, but similar function.	0.04
Diverse hardware and function.	0.01

Whenever complex protective systems are used to achieve higher reliability then it is vital to check very carefully for dependent failures and expert advice should be sought.

Continuing with the same example with two identical trip channels:

Assuming:

0.27 random faults per year per channel
β = 0.15
1 month proof test period
1 hour total testing time
1 in 1000 probability of leaving the system disarmed following a test

PFDavg (due to dependent failures) = ½ x 0.27 x 0.15 x1 /12
= 0.002

PFDavg (due to coincidence of random faults) = 1/3 x (0.27 x 1/12) 2
= 0.00017

PFDavg (due to testing time) = 1 x 12 / 8760
= 0.0014

PFDavg (due to testing errors) = 0.001

Total PFDavg = 0.002 + 0.00017 + 0.001
= 0.0047

This assumes that both channels are tested at the same time. If it can be arranged that each channel can be tested, all or in part, leaving the other live then the PFDavg due to testing time can be reduced. "Staggered" testing can also reduce the system PFDavg, but the calculation of this effect is beyond the scope of this document.

It is often helpful, especially with more complex protective systems, to construct a block diagram. Examples are shown in Figure D-14 and Figure D-15.

Redundancy built into the system shows as alternative parallel routes in the block diagram. The extent of cross linking between two channels also affects the overall PFDavg and can be easily shown.

The way to improve a trip system further is to introduce diversity. This may involve using different methods of measuring a process using more than one process variable to initiate the trip, using different types of device to actuate the trip and providing more than one route for essential services such as air and electricity.

The aim is to reduce the possibility of dependent failures. Simple diversity such as using both torque tube and a DP cell to detect level or temperature change and direct measurement to detect level is frequently used. However, using diversity to get very high reliability results in complex systems are beyond the scope of this document.

D.7.4.2 Reliability for production

It is important to remember the other reliability condition which is spurious operation of the trip. This is given by the fail safe failure rate. The plant is made safe but production is interrupted so "reliability for production" has to be considered. A simple trip system could have around one fail safe fault per year. Depending on circumstances, that may or may not be acceptable. A problem with building redundancy into a protective system is that although it improves "reliability for safety" it reduces "reliability for production". A, one out of two system would cause twice as many spurious trips as the corresponding single channel system.

FIGURE 3 TABLE D-1 COMPARISON OF PROTECTIVE SYSTEMS (ASSUMES THAT THE SUBSYSTEMS ARE IDENTICAL)

System Voting	Fail safe failure rate - Faults/Year	Fail to danger failure rate - Faults/Year	PFDavg
1 out of 1	S	θ	$\theta T / 2$ = PFDavg
1 out of 2	2S	$\theta^2 T$	$\theta^2 T^2 /3 = 4/3$ $(\text{PFDavg})^2$
2 out of 2	S^2T or 2 S^2T' *	2θ	θT = 2 PFDavg
1 out of 3	3S	$\theta^3 T^2$	θ^3 $T^3 /4$ = 2 $(\text{PFDavg})^3$
2 out of 3	$3S^2T$ or $6S^2T'$ *	$3\theta^2 T$	$\theta^2 T^2$ = 4 $(\text{PFDavg})^2$

T = test interval in years, T' = repair time in years

Note: (*) the second expressions apply if the fail-safe faults are revealed and can be repaired in time T'

The above expressions for PFDavg do not include the effects of dependent failures, testing time and errors which, for systems with redundancy, are likely to limit the PFDavg that can in practice be achieved.

The way to improve reliability for production whilst maintaining reliability for safety is to use a voting system - a two out of three system is commonly used. Three identical channels are provided and the trip condition has to be registered by any two out of the three before the trip action is initiated. Although this system has more fail-to-danger failures than a 1 out of 2 system it has far fewer fail safe faults and is popular when good all-round reliability is required. It can be easily tested on line without reducing the integrity of the trip system because with the channel under test put into trip condition the system becomes 1 out of 2 for the duration of the test. The failure rates and PFDavg for various combinations of protective devices are listed in Table D-1.

D.7.4.3 Hardware Fault Tolerance

Hardware fault tolerance (HFT) is a requirement for compliance with the international standards on Functional Safety: IEC 61508 and IEC 61511. It is important for the hazard analyst to be aware of the requirements and to check whether any trip system being assessed complies with the requirements.

D.7.3.1 Definition

Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware.

For example, hardware fault tolerance of 1 means that a failure of one of two parallel components or subsystems does not prevent the safety action from occurring. A voting arrangement of 2oo3 will normally have a HFT of 1. A voting arrangement of 1oo3 will normally have a HFT of 2.

D.7.3.2 HFT Requirements - IEC 61511

The following tables show the hardware fault tolerance requirements for safety related systems according to IEC 61511. These tables are taken from IEC 61511 Part 1, Clause 11. They are a simplification for the process industry sector of the requirements in IEC 61508.

TABLE D-2 MINIMUM HARDWARE FAULT TOLERANCE FOR SENSORS, FINAL ELEMENTS AND NON-PROGRAMMABLE ELECTRONIC LOGIC SOLVERS

SIL	Minimum hardware fault tolerance
1	0
2	1
3	2
4	Not acceptable within Indorama Ventures (Special requirements apply - see IEC 61508)

Note: This table based on the requirements in IEC 61511 Part 1 - Table 6.

TABLE D-3 MINIMUM HARDWARE FAULT TOLERANCE FOR PROGRAMMABLE LOGIC SOLVERS

<table>
<tr><th rowspan="2">SIL</th><th colspan="3">Minimum hardware fault tolerance</th></tr>
<tr><th>SFF < 60%</th><th>SFF 60% to 90%</th><th>SFF > 90%</th></tr>
<tr><td>1</td><td>1</td><td>0</td><td>0</td></tr>
<tr><td>2</td><td>2</td><td>1</td><td>0</td></tr>
<tr><td>3</td><td>3</td><td>2</td><td>1</td></tr>
<tr><td>4</td><td colspan="3">Not acceptable within Indorama Ventures
(Special requirements apply - see IEC 61508)</td></tr>
</table>

Note: This table based on the requirements in IEC 61511 Part 1 - Table 5.

The abbreviation SFF in the above table stands for Safe Failure Fraction. The meaning of this term is explained below.

D.7.3.3 Safe Failure Fraction (SFF)

Definition: fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure.

Failure Mode

From IEC 61508 - 2 Annex C, safe and dangerous failures are categorised as follows

- A safe failure: a failure leading to the safety integrity of an Electrical, Electronic or Programmable Electronic (E/E/PE) safety-related system not being compromised, for example, a failure leading to a safe shut-down or having no impact on the safety integrity of the E/E/PE safety-related system; or

- A dangerous failure: a failure leading to an E/E/PE safety-related system, or part thereof, failing to function, or leading to the safety integrity of the E/E/PE safety-related system being otherwise compromised.

Assessing Safe Failure Fraction

a. From an estimate of the failure probability of each component or group of components, λ, and the results of the failure mode and effect analysis (FMEA), for each component or group of components, calculate the probability of safe failure, λ□$_{S}$, and the probability of dangerous failure, λ_{D}.
b. For each component or group of components, estimate the fraction of dangerous failures which will be detected by the diagnostic tests and therefore the probability of a dangerous failure which is detected by the diagnostic tests, λ□$_{DD}$.
c. For the subsystem, calculate the total probability of dangerous failure, $\Sigma\lambda_{D}$, the total probability of dangerous failures that are detected by the diagnostic tests, $\Sigma\lambda$□$_{DD}$, and the total probability of safe failures $\Sigma\lambda_{S}$,
d. Calculate the diagnostic coverage of the subsystem as $\Sigma\lambda_{DD}$ /$\Sigma\lambda_{D}$.
e. Calculate safe failure fraction of the subsystem as ($\Sigma\lambda$□$_{S}$ + $\Sigma\lambda$□$_{DD}$)/($\Sigma\lambda$□$_{S}$ + $\Sigma\lambda$□$_{D}$).

It is to be noted that SFF for logic solvers will normally be provided by the supplier. The hazard analyst will not be expected to calculate the SFF and the formulas above are provided only for reference.

D.7.4.4 Examples

The following examples further illustrate the applications of the various principles introduced above.

D.7.4.1 Example 1 - Relief Valves

Consider a relief valve that is overhauled and tested every two years. What is its PFDavg assuming it fails to lift 0.005 times/year? What would the PFDavg be if the relief valve were duplicated? Assume that 10% of the relief valve failures would be caused by dependent failures.

For the single relief valve,

PFDavg = ½ θT
= ½ x 0.005 x 2
= 0.005

For the duplicated system both relief valves must fail to lift and so:

PFDavg = PFDavg (due to common faults)
+ PFDavg (due to coincidental faults)

= ½ x (0.1 x 0.005) x 2 + 1/3 $(0.0045^2 \times 2^2)$

= 0.0005 + 0.000027

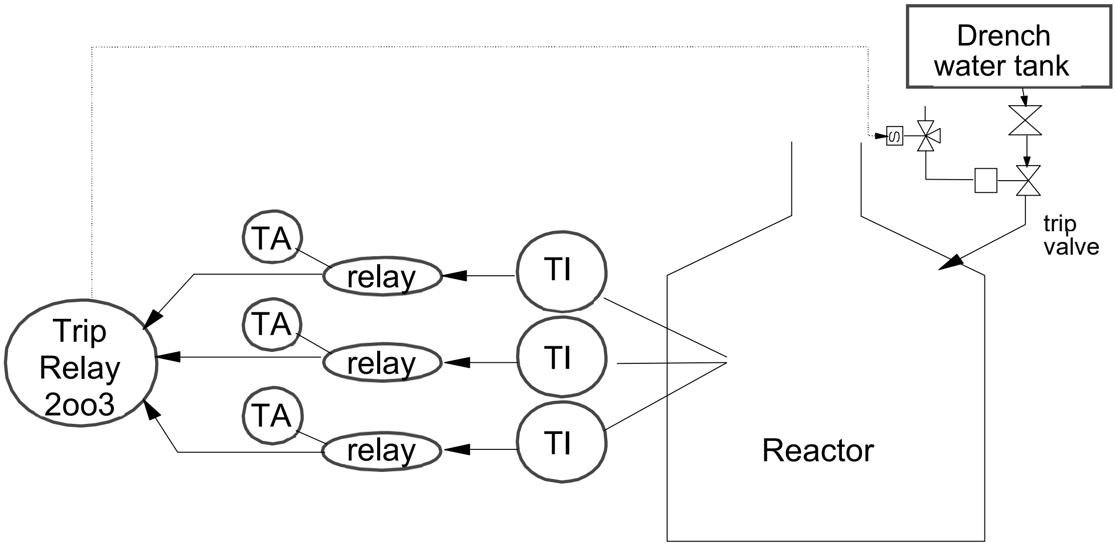
= 0.00053

D.7.4.2 Example 2 - Reactor Trip

Figure D-14 shows a high temperature trip on a reactor. Three temperature indicators are provided each of which has an alarm but two out of three need to register a high temperature in order to actuate the essential trip action, which is for the trip valve to open and let the drench water into the reactor.

Assume the following failure rates and estimate the PFDavg and spurious trip frequency for a test period of 3 months.

FIGURE D-14 HIGH TEMPERATURE TRIP ON REACTOR



Initiating channels	Failure rate / yr.[9]	
	Fail-safe	Fail-danger
TI	2.0 *	0.25
Loss of power (common)	0.05	0
Broken wire, terminal in individual circuits	0.01	0
Relay coil	0.05	0
Relay contacts	0.01	0.002
Total:	2.12	0.252

*Assume fail-safe faults in the initiating channels would be revealed and can be repaired within 1 day.

[9] Note these figures are given for illustrating the calculation only. They should not be taken as generic failure rates.

Trip logic and actuator	**Failure rate / yr.** [10]	
	Fail-safe	Fail-danger
Loss of air	0.05	0
2oo3 logic card	0.002	0.001
Solenoid valve	0.04	0.02
Trip valve	0.1	0.04
	0.192	0.061

The relays and solenoid valve de-energize to trip and the trip valve opens on air failure.

PFDavg for 2oo3 initiators = θ^2T^2 (from Table D-1)
= $(0.252 \times ¼)^2$
= 0.004

PFDavg for actuator = ½ x 0.061 x ¼
= 0.008

Total PFDavg = 0.012

The spurious trip frequency would be as follows:

Due to common power loss = 0.05/y

Due to revealed faults in 2oo3 Initiator channels:

$6S^2T$ = $6 \times 2.12^2 \times 1/365$
= 0.07/y

Due to faults in trip actuator system = 0.19/y

Total frequency of spurious trips = 0.31/y

Note: that a similar PFDavg could be obtained by a single channel system if the initiators were tested monthly.

PFDavg for 1oo1 initiators = ½ x 0.252 x 1/12
= 0.0105

Total PFDavg then could be = 0.0185

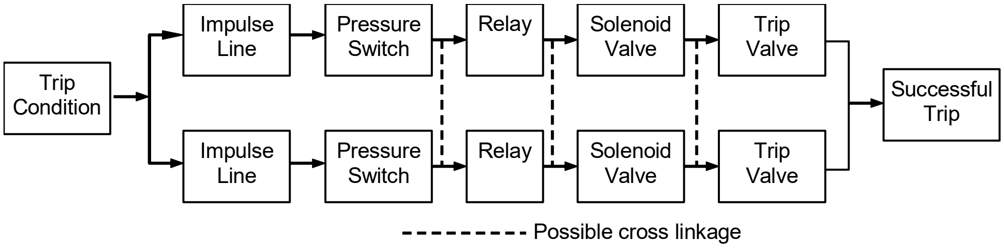
However with a 1 out of 1 system all the revealed fail safe faults would also cause spurious trips and so the spurious trip frequency could be very much greater at 2.3 per year.

D.7.4.3 Example 3 - High Pressure Trip

Figure D-15 shows a block diagram for a 1oo2 high pressure trip.

[10] Note these figures are given for illustrating the calculation only. They should not be taken as generic failure rates.

FIGURE D-15 BLOCK DIAGRAM FOR 1OO2 HIGH PRESSURE TRIP



This could be arranged with (a) each channel separate or (b) cross-connected as shown by the dotted lines. The calculation of PFDavg must take account of the extent of cross connection and would be as follows assuming a test interval of 2 months.

Item	Fail-danger [11] failure rate / yr.	PFDavg
Impulse line leakage/blockage	0.01	0.013
Pressure switch	0.15	
Relay	0.002	0.00017
Solenoid valve	0.02	0.0025
Solenoid valve	0.01	
Trip valve	0.04	0.0033
TOTAL	0.232	0.019

a. 1oo2 separate channels

Independent failures PFDavg = 4/3 $(0.019)^2$
= 4.8×10^{-4}

Assuming a Beta factor of 0.15 for identical hardware in the 2 channels, the dependent failure PFDavg would be:

= 0.15 x 0.019
= 0.0028

Giving a total PFDavg = 0.0028 + 0.00048
= 0.0033

b. 1oo2 interconnected channels

Independent failures PFDavg = 4/3 {(0.013)2 + (1.7 x 10-4) 2 + (2.5 x 10-3)2 + (3.3 x 10-3)2}
= 1.9 x 10-4

and with the same dependent failures PFDavg as above,

Total PFDavg = 0.0028 + 0.00019
= 0.0030

[11] Note these figures are given for illustrating the calculation only. They should not be taken as generic failure rates.

Note that cross connection seems to give marginally higher reliability but the full assessment must take account of testing as well. The apparent advantage of the cross connected system could be lost because of the need to defeat the whole system for testing whereas with independent channels, each could perhaps be tested separately so that at least 1oo1 protection was available whilst testing. Note also that some faults not accounted for could degrade the system by affecting both channels simultaneously, e.g.:

i. Blockage of both pressure switch impulse lines by a common cause

ii. If both solenoid vents are joined to a common vent pipe then a single blockage could prevent both solenoid valves working

iii. Scale or other deposits might prevent both trip valves closing completely.

As far as possible, functional dependency failures of this nature must be designed out of the system but the effect of such failures needs to be included in the assessment. For advice on this, a person skilled in hazard assessment should be consulted.

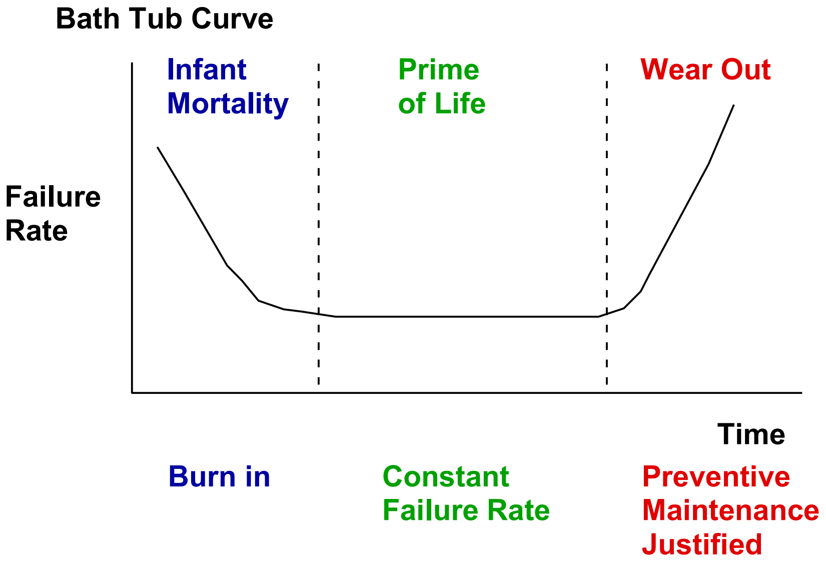
D.8 Failure Data

In order to evaluate the demand rate on or the reliability of the protective system, it is necessary to have information about the failures which could be expected from the equipment and its mode of operation. Basically, two categories of failure are important - equipment (i.e., hardware) failures and operator failures (i.e., human error). The interface between these two categories is often not clearly defined and many human error faults, such as wrong assembly of a machine after maintenance, will probably be identified as a machine failure. This interface is also affected by software e.g., plant operating instructions, standing instructions etc. Data to a greater or lesser extent exists on both equipment failure rates and human error rates. The following sections will discuss these two categories of failure.

D.8.1 Equipment failure

Figure D-16 shows a "bath tub" curve which describes the failure rate variation with age of an item. The curve shows a high initial failure rate (burn in or infant mortality) which later levels to a constant failure rate and then increases near the end when wear out occurs. Equipment included in hazard analyses may exhibit any of these failure modes, but it is normal and usually justifiable to assume that equipment is in the constant failure rate phase. This allows the use of simple mathematical equations.

FIGURE D-16 GENERALIZED PATTERN OF FAILURE RATE VARIATION WITH EQUIPMENT LIFE - THE "BATH TUB" CURVE



Most early failures, caused by manufacturing flaws or poor inspection, are corrected during the commissioning period. Wear out failures resulting from old age are anticipated by routine maintenance.

D.8.1.1 Data collection and sources

There are basically three ways in which reliability data can be obtained: sampling, prediction and field experience; the last is the most important.

1. Sampling

   Sampling may be an accurate tool when dealing with large numbers of mass-produced items, which will be installed in fairly similar environments e.g., electronic components. However, when considered in the context of the chemical and allied industries it is not feasible.

2. Prediction

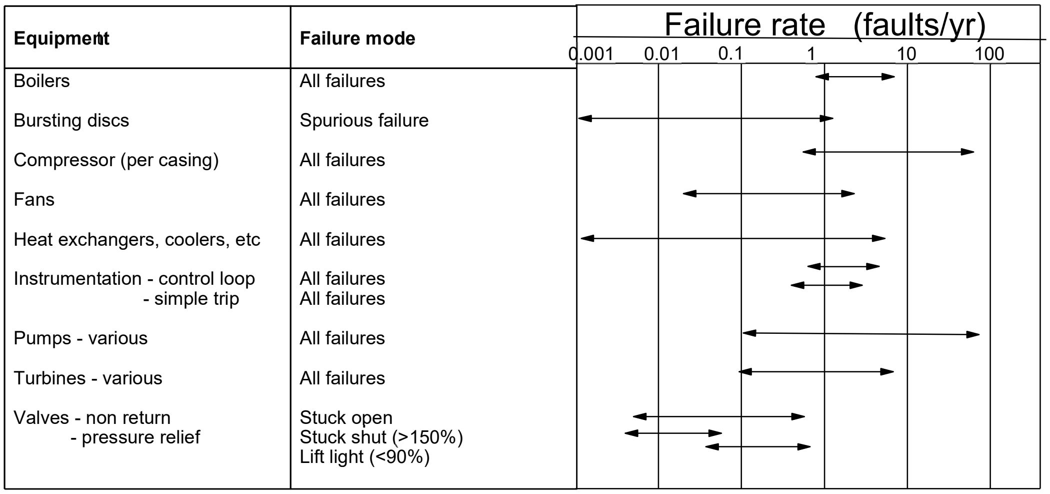
   There are considerable data available on failure rates of commonly used small components like resistors, connections, diaphragms, etc. The prediction technique breaks down an item of equipment into its components. Each component failure is analysed to predict its effect on the overall performance of the equipment. The overall failure rate of the equipment is predicted by summing the component failures for each equipment failure mode. This technique has limited application in hazard analysis but in some instances, it can be useful for assessing the split of failures between the fail-safe and fail-to-danger modes. It is used widely by manufacturers of electronic equipment to estimate values for their published data.

   Watch out for predictions of failure rates for items that contact the process fluid. Often these predictions, carried out for manufacturers, have only considered the failure of the electronic components and create predicted failure rates for the overall item (such as a sensor or a valve) that are significantly lower than experience might suggest as realistic. Such predictions are available from manufacturer’s websites.

3. Field data

   The most suitable data for use in hazard analysis of chemical process problems derive usually from that collected in the "field". Ideally, data collected from the plant being studied are best but obviously, this is impossible for a design study and impractical if the plant has not been operating long. In those cases, wherever possible, the data should be obtained from a comparable plant or duty because in the chemical industry there are so many possible variations in the environmental conditions which affect the failure rate e.g., temperature, vibration, cleanliness, type of duty, load, frequency of start up, size etc.

Table D-4 Spread of Failure Rates



Equipment	Failure mode
Boilers	All failures
Bursting discs	Spurious failure
Compressor (per casing)	All failures
Fans	All failures
Heat exchangers, coolers, etc	All failures
Instrumentation - control loop - simple trip	All failures All failures
Pumps - various	All failures
Turbines - various	All failures
Valves - non return - pressure relief	Stuck open Stuck shut (>150%) Lift light (<90%)

The above table shows the sort of spread in failure rates that can be caused by factors such as pressure, temperature, environment, maintenance policies, design standards, etc.

When local data are not available, more general sources have to be used. It is suggested that HPSHEG 14 - Reliability Data is consulted for failure data if it is necessary to use generic data.

There are also some generic data to be found in the technical literature.

D.8.1.2 Problems with data

a. Classification of failure data

   There are many ways in which an item of equipment can fail. International Standards give the terminology necessary to define completely the reliability of equipment, but the possible combinations of all failure classes is nearly 300 and so complete definition of failure for any item is impractical. In practice, the many failure modes can be reduced to a few important ones.

   - Fail danger (i.e. a fault that would prevent a protective system operating or cause a control loop to put a demand on a trip or alarm system).
   - Fail safe (i.e. a fault that would cause a trip system to operate without a demand being made on it - "a spurious trip").
   - Fail-neutral (a fault that neither causes the trip or control system to fail nor causes a spurious trip e.g. a leaking spindle on a valve).

The fault might be “revealed” or “unrevealed”. It could occur ‘slowly' or 'suddenly’.

A sudden fault can be described as one that occurs too quickly for the plant operator to be able to take corrective action.

b. Instrument failure data for hazard analyses

- "Unrevealed fail-to-danger failures” are those most relevant to the reliability of an instrumented protective system because they will cause the system to fail and can only be detected by proof testing.
- "Sudden fail-to-danger failures” of a control loop are those most relevant to assessing the demands on a trip and alarm systems as those give the least time for operator corrective action.

Much failure rate data quoted in the literature are overall values embracing all failure modes. It is difficult from that sort of data to make a realistic assessment of the ability of an alarm or trip system to give protection.

c. Environmental effects

Modifying factors can be used to allow for failure rates being higher in adverse conditions of environment. These factors range from unity for instruments in control rooms, or those subjected only to clean, harmless fluids or atmospheres, to a factor of 4 for extremely aggressive conditions such as acid attack, erosion and blockages. Other factors, which may be taken into account particularly for items such as valves etc., are the operating pressure and temperatures and the maintenance policies. For example, if there is no regular maintenance then some items will begin to exhibit wear out failures.

Little really reliable data on environmental factors exists and so it is advisable where environmental factors could be deemed important to use data from a similar environment.

The following examples illustrate that the effect of environmental factors can be very significant. The solenoid valves on a particular plant had a fail-to-danger failure rate of 0.18 faults/ year which reduced to 0.04 faults/year after some plant modifications were carried out. The reason for the reduced failure rate was an improvement in the quality of the instrument air. Another example concerns level float switches. On one vessel, there were no failures in 31 item years while in a similar vessel there were 19 failures, mostly fail danger, in 31 item years. They were caused by solids blocking the impulse lines. Thus, significant differences in the failure rate can be found for identical items on similar duties on the same plant, in these instances caused by different conditions within the equipment.

Environmental factors can also affect the failure rates of other equipment as well as instrumentation.

d. Sensitivity Analysis

There are two very good reasons for looking at each item of data from the point of sensitivity. Firstly, if a certain value of the data were selected, is it consistent or likely to be consistent with established performance? There is no point, for instance, in using a total power failure rate of once in 20 years if there have been three reported failures in the last 10 years. One should always check as far as possible for a sense of reality.

Secondly, when choosing a figure to use in an assessment, one should in every case consciously ask oneself whether it should be say, 10 times greater, or 10 times smaller. The estimate may be of doubtful accuracy but what is more important is whether it is going to have a significant effect on the predicted 'hazardous event rate because if it matters little whether it is 10 times greater or 10 times smaller, then the value selected is probably acceptable. If however, it has a significant effect, then the value selected requires further thought, and before the final analysis, rough calculations should be made showing the effects of the two extremes.

It is best to remember that rarely will the accuracy of data be greater than about half an order of magnitude and it is always sensible to test the accuracy of data against people's experience and intuition.

D.8.2 Human Error

It is perhaps true to say that almost all faults/hazardous events/accidents are due to a human error in some form or other. Certainly many of the faults that will contribute to equipment failure rates will have their origins in a human error whether it is at the design, construction or maintenance state. However in the context of hazard analysis "human error" mostly refers to the probability of operator error occurring during a process operation. Broadly speaking these errors fall into two classes.

a. "Errors of commission" i.e. The operator does the wrong thing. This will appear in fault trees as say "operator takes wrong action"

b. "Errors of omission", i.e. The operator fails to do the right thing; this will appear in fault trees as say, "operator response failed"

D.8.2.1 Human error data

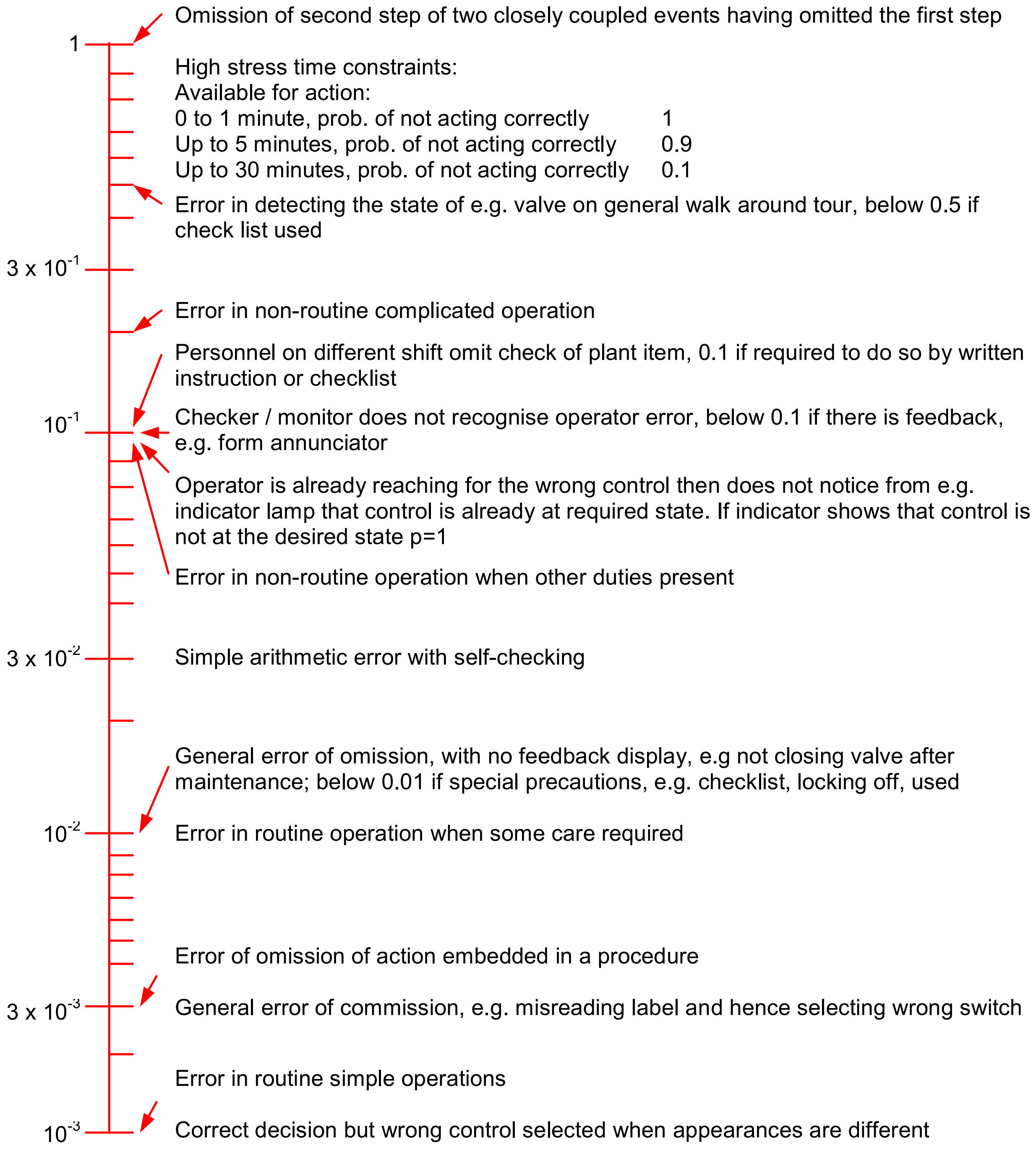
There have been a number of studies of the performance of plant operating staff as a result of which some estimates of error probability have been made. There is a broad spectrum of performance based on a number of factors related to the nature of the task

- Type of operation
- Degree of complexity of the operation
- Degree of familiarity with the operation

The range of error probability is very wide. At best the human operator can be substantially more reliable than, for example, a simple instrument trip system. The low frequency, for instance of overfilling cylinders and tankers can show that in the right circumstances an error probability as low as 1 in 1000 can be achieved for some regularly repeated operations that the operator can do in his own time. However in other circumstances there may be an error in every operation. Any quoted figure should be questioned before use. The fact that it may have been used in one analysis does not necessarily justify its use in another without question. If the analysis is of an existing plant then the site and "work situation" should be examined before judging what error probabilities to use. Wherever possible any assumed figures should be tested against experience. All this requires some appreciation of the factors that affect human performance.

Figure D-17 shows a guide to the range of error probability.

FIGURE D-17 GUIDE TO HUMAN ERROR PROBABILITY



Omission of second step of two closely coupled events having omitted the first step

High stress time constraints:
Available for action:

0 to 1 minute, prob. of not acting correctly	1
Up to 5 minutes, prob. of not acting correctly	0.9
Up to 30 minutes, prob. of not acting correctly	0.1

Error in detecting the state of e.g. valve on general walk around tour, below 0.5 if check list used

Error in non-routine complicated operation

Personnel on different shift omit check of plant item, 0.1 if required to do so by written instruction or checklist

Checker / monitor does not recognise operator error, below 0.1 if there is feedback, e.g. form annunciator

Operator is already reaching for the wrong control then does not notice from e.g. indicator lamp that control is already at required state. If indicator shows that control is not at the desired state p=1

Error in non-routine operation when other duties present

Simple arithmetic error with self-checking

General error of omission, with no feedback display, e.g not closing valve after maintenance; below 0.01 if special precautions, e.g. checklist, locking off, used

Error in routine operation when some care required

Error of omission of action embedded in a procedure

General error of commission, e.g. misreading label and hence selecting wrong switch

Error in routine simple operations

Correct decision but wrong control selected when appearances are different

Sources: Human Reliability Analysis - A D Swain, 27.03.74
Fault Tree Synthesis for Chemical Processes - G J Powers, F C Tomkins, AIChE Journal Vol 20 No.2 March 1974

D.8.2.2 Factors affecting operator performance

An operator may fail to act correctly because:

a. The operator may not know what to do (lack of training)
b. May not want to do it (lack of motivation)
c. The task the operator is asked to do may be beyond his/her physical and mental capability.

Hopefully these factors will be substantially eliminated by suitable recruitment, training, instructions design and so on. Even so, an operator will make occasional mistakes and factors that will affect his performance are:

a. The operator’s characteristics
b. Characteristics of the job
c. The stress level

D.8.2.2.1 Some characteristics of operators

Firstly, no two operators are the same and may react differently to different circumstances, but, in general, they all have both strengths and weaknesses that will affect their performance.

a. **Strengths**

   i. They can acquire meaningful information from a variety of sources around them, even in high "noise" situations.
   ii. They are versatile; they can make judgements; consider and combine information received; they can detect errors; they can recognise patterns and trends for example in instrument readings and recordings; they are good at "feed forward" control.
   iii. They can think, reason, and react to new situations. They can learn from experience.

b. **Weaknesses**

   i. They may be inconsistent.
   ii. They may be slow to respond, particularly in situations which are new or have not been experienced for a long time or which are complex.
   iii. They get tired.
   iv. They have an unreliable "precise memory” and can "revert to habit" particularly at times of stress.
   v. They may become disorganised on overload and panic.
   vi. They have emotions and so may be affected by problems/anxieties both inside and outside the "work situation".

D.8.2.2.2 Characteristics of the job

These include not only "ergonomics", that is the relationship between the operator and his work, but also the situation in which the operator performs his work:

a. Physical arrangements
b. Environment (noise, temperature, lighting)
c. Job methods
d. Job organisation (either as individuals or within working group)

An important factor is the situation the operator is in immediately before and immediately after he is required to act quickly. Immediately before the event, he ought to have sufficient information presented in the right way and at the right rate so that he can recognise what is happening. Layout of alarms, control panels, information displays are therefore important. One aspect, which should not be forgotten, is that people grow to expect certain things to happen: for example, turning a knob clockwise is expected to increase something.

A number of key questions can be asked when considering the possibility of error in a specific job situation:

a. How will the operator know of the upset condition or emergency?
b. How will he know what action to take?
c. What action can he take?
d. How much time has he got to take effective action?

Characteristics of the job are important factors to consider at the design stage and improving the work situation is regarded by some as the most fruitful way of reducing the chance of error - perhaps by a factor of ten.

D.8.2.2.3 Effect of stress

Particularly in an emergency or upset condition to which the operator has to react and take action, stress can arise as a result of:

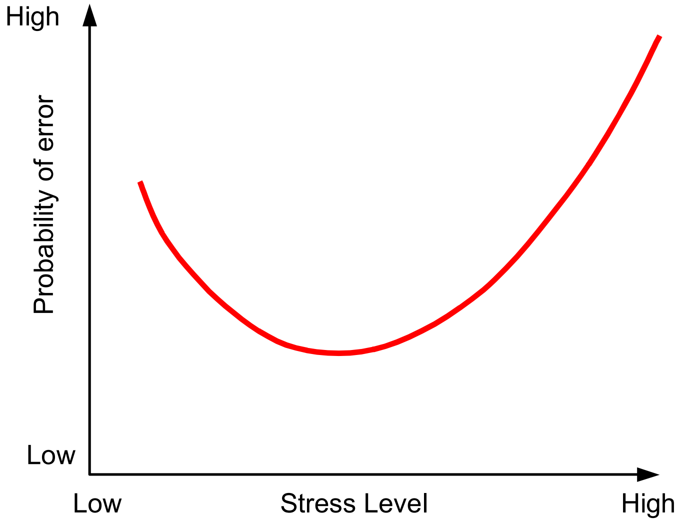
a. Anxiety - physical danger or management reprimand
b. Time - the knowledge that action has to be quick (the pressure of speed will slow down human decision making)
c. Information overload - amount of information: rate at which it is presented
d. Distraction - a number of events may be occurring simultaneously

Under high stress conditions, operators cannot be relied on to act correctly. The US Atomic Energy Commission quotes the following figures for an emergency on a nuclear power station:

Time since incident occurred	Probability of operator error
Within one minute	About 1
After five minutes	0.9
After thirty minutes	0.1
After several hours	0.01

In contrast, at low stress levels, a task may be so dull and unchallenging that most operators do not perform as well as they might, they are bored and their attention wanders. An inspection activity - a walk around to see if everything is in order - is often of this type; error probabilities for this activity have been reported to be as high as 50%. Men are most reliable when the stress level is just sufficient to keep them alert. Figure D-18 qualitatively illustrates the effect of stress level on error probability.

FIGURE D-18 INDICATION OF THE GENERAL EFFECT OF STRESS ON PROBABILITY OF ERROR



D.8.2.3 Some pitfalls in using human error data

D.8.2.3.1 The effect of checking (not to be confused with supervising)

If a person knows he is being checked, he works less reliably. If the error rate of a single operator is 1 in 100, that of an operator plus checker could be greater than 1 in 100.

On the other hand, if the two operators work as a team, error rates come down. Reference 44[12] describes the calibration of an instrument in which one person writes down the figures on a checklist whilst the other person calls them out. They then change over and repeat the calibration, the probability of error is quoted as 10^{-5}.

In contrast to instrument systems, engaging two people on a task does not necessarily increase reliability. Hierarchy or rank seems to be important. This may have contributed to the Stansted air disaster. A junior crew member detected that the plane was becoming uncontrollable but hesitated to warn the pilot (who was not responding) who was much more senior.

D.8.2.3.2 If an operator ignores a reading he may ignore an alarm

Suppose an operator fails to notice a high reading on 1 occasion in 100 (p = 10^{-2}); it is an important reading and he has been trained to pay attention to it. Suppose that he ignores the alarm on 1 occasion in 100 (p = 10^{-2}). We cannot assume that he will ignore the reading and the alarm on 1 occasion in 10,000 (p = 10^{-4}). On the occasion that he ignores the reading the chance that he will also ignore the alarm is greater than average.

[12] See D.11.

D.8.2.3.3 Increasing the number of alarms does not increase reliability

Assume an operator ignores an alarm on 1 in 100 occasions on which it sounds, installing another alarm (say at a slightly different setting) will not reduce the failure rate to 1 in 10,000. If the operator's state of mind is such that he ignores the first alarm, there is a more than average chance that he will ignore the second.

D.8.2.4 Example of the effect of human error

Assume that the plant operator is required to commission a spare pump when an on-line pump fails. The operations in the task would be:

a. Operator goes to correct pump
b. Operator closes the delivery valve on the failed pump
c. Operator closes the inlet valve on the failed pump
d. Operator opens the inlet valve on the standby pump
e. Operator presses the start button on the standby pump
f. Operator opens the delivery valve on the standby pump

On average, the on-line pump fails twice per year. The total number of operations to be done per year is therefore twelve. Assume eight of these (i.e. 4 out of 6 per task) are potentially subject to error such that the process flow would not be restarted.

With normal stress and motivation the probability that the operator will make an error is 1 in l000 or 10-3, therefore, the average frequency of error = 8 x 10-3/year.

With high stress and motivation, for example, if the operator has limited time to make the changeover, the probability of error could be 1 in 10 or 10-1, therefore the average frequency of error = 8 x 10-1/year.

In that situation, it might be beneficial to install an automatic changeover system. If the failure rate of the automatic system is 0.25/year and it is tested monthly, the PFDavg = 0.01, therefore the hazardous event rate = 2 x 0.01 = 0.02/year or forty times better than the manual changeover in a 'high stress situation. But note that this hazardous event rate is greater than that (0.008/y) for manual changeover in a low stress situation.

This is a simplified example. A more rigorous treatment would need to recognise that some of the errors might be revealed by lack of flow in time for the operator to correct his error. However not all situations give opportunity for self-correction. For instance, once the wrong button has been pressed on a coffee machine it is too late to correct the mistake.

D.9 Use of Hazard Analysis: Further Examples

The technique of hazard analysis can be applied to both new and existing plants and processes. In the design of major capital projects there are several stages at which hazard analysis is useful, for instance:

a. Early, coarse scale, analyses can be helpful to give an appreciation of the main potential hazardous events and guidance for site selection.
b. As design proceeds hazard analysis can help with the choice between different designs, can define requirements that the design must meet e.g. protective systems.

c. Simple quantification during the hazard and operability study can help in deciding whether further protection is required. A common example is where an undesirable situation depends on the occurrence of a number of coincident failures. Sometimes this situation will be dismissed as three coincident failures are considered to be very unlikely - but are they? It may depend on whether the failures are related or whether the inspection and maintenance policies are adequate. Sometimes failures can occur and not immediately cause a hazardous event but remain hidden (or uncorrected) until a further failure occurs to complete the combination required for a hazardous event. It is worth remembering that most major incidents occur as a result of a number of coincident failures. Hence some effort to quantify the hazardous event rate may be worth while if it brings out some relevant and unconsidered information.

d. When the design is substantially complete hazard analysis can be used to give a complete quantification of the important hazards.

Hazard analysis is often used on existing plants when concern for a hazard has been aroused by an incident, a “near miss", a change in operating methods, up-rating of the plant etc. Many existing plants were designed when standards were lower and this may need to be taken into account when setting the criterion for the analysis.

Three further examples are given below to show how the technique can be used for different types of problems.

D.9.1 Vent stack sizing - a design problem

It is often convenient to have a common vent system and stack for a number of relief valves. The problem arises of how big to make the vent system. The easiest approach is to size the stack to take the maximum rate i.e. all the relief valves discharging simultaneously at their maximum rates. In practice, this condition may never arise and so the vent stack is oversized. A more realistic approach is to quantify the frequency with which various discharge rates may be achieved and then to use one of the criteria already described to assess the minimum acceptable vent stack size. The following example shows how this type of problem might be quantified.

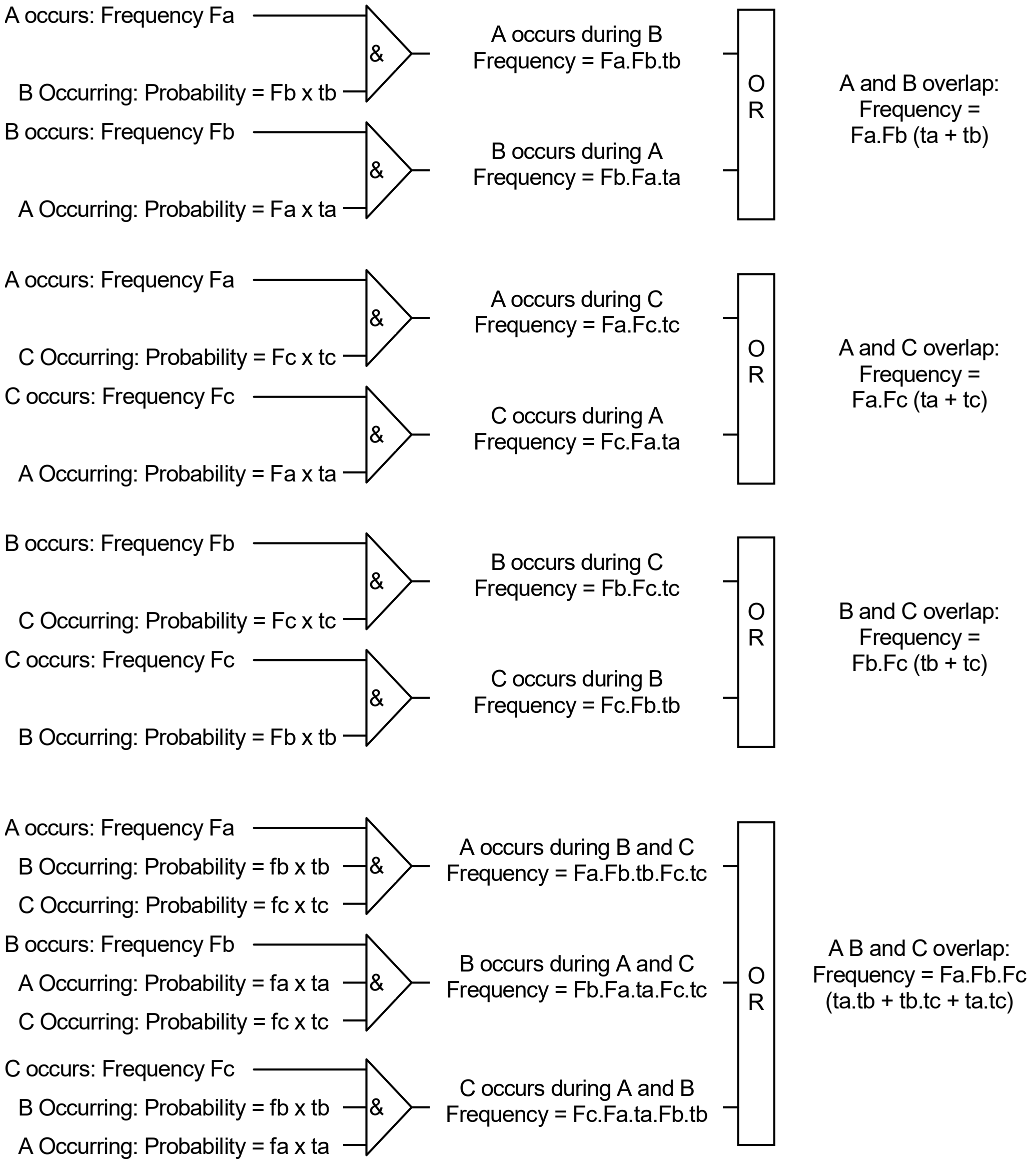
Assume that there are three relief valves A, B and C that pass the following rates at the frequencies shown in the table.

Relief Valve	Discharge Rate te/hour	Frequency of Discharge times/year
A	100	0.01
B	50	1
C	20	0.5

The frequencies would be estimated by analysis of each of the systems protected by the relief valves. If these relief valves are on completely independent systems, then the frequency with which any pair of valves or all 3 valves will be open together can be analysed. If F is the frequency of discharge and t is of the duration of discharge hours (for the purposes in this example it is assumed the same for all the relief valves) then the probability (proportion of time) that relief valve A is discharging is:

F_A t / 8760

The logic for the situations of interest is:



If t = 4 hours, using the data in the fault tree the following discharge rates and frequencies are obtained:

Relief Valves discharging	**Discharge Rate te/hour**	**Frequency times/year**
B & C	70	5×10^{-4}
A & C	120	5×10^{-6}
A & B	150	9×10^{-6}
A & B & C	170	3.1×10^{-9}

All these frequencies of combinations are very low and so the vent stack should be sized to take the largest single relief valve rate i.e. 100 te/ hour. This rate will only be exceeded once in about 70,000 years. This conclusion can be confirmed by evaluating the FAR[13] for certain vent sizes. If the probability that someone is killed i.e., P_{exp} x PF is taken as 0.01 then the following table results:

Vent Size te/hour	FAR Fatalities/10^8 Exposed hours
50	1.2
70	1.1
100	0.0016
120	0.001

Again, it is clear that the vent stack need not be sized to take more than a rate of 100 te/hour.

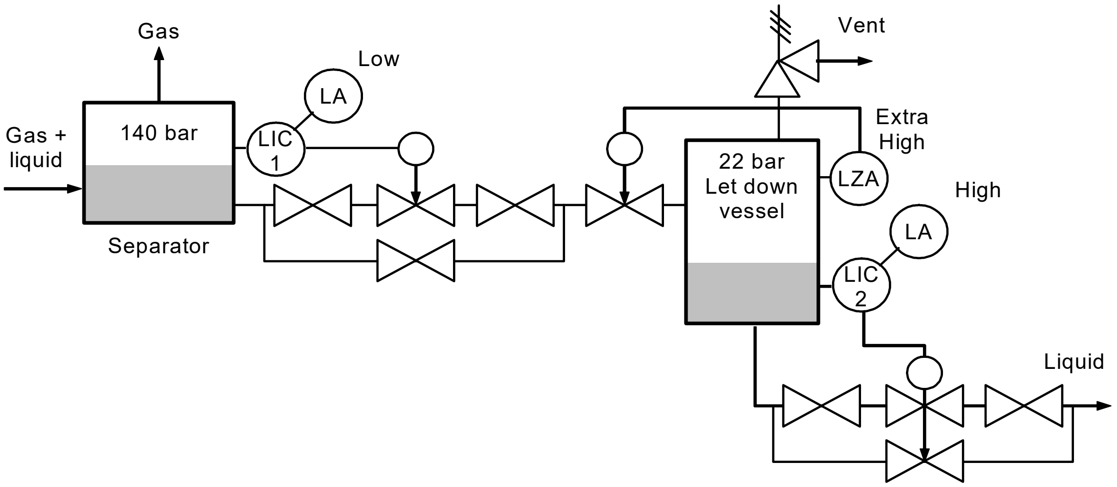
NB When considering problems like this it is vital to check very carefully that there are no common causes that could lead to simultaneous lifting of two or more of the relief valves.

D.9.2 Pressure let down system - assessment of a design

This example is a simplified hazard analysis of a pressure let down system in which a vessel is at risk from overpressure. Figure D-19 shows details of the let-down system.

The first step is to identify the hazardous event and to decide on the criterion for acceptability. In this case, the hazardous event is overpressure possibly leading to rupture of the let down vessel. Overpressure could be caused by gas breakthrough due to loss of liquid level in the separator or as a result of the let down vessel over-filling with liquid. The latter situation is undesirable so a high level trip is installed to stop the liquid flow in that event.

FIGURE D-19 EXAMPLE D.9.2 SEPARATION AND LET-DOWN OF LIQUID FROM A HIGH PRESSURE GAS-LIQUID SYSTEM



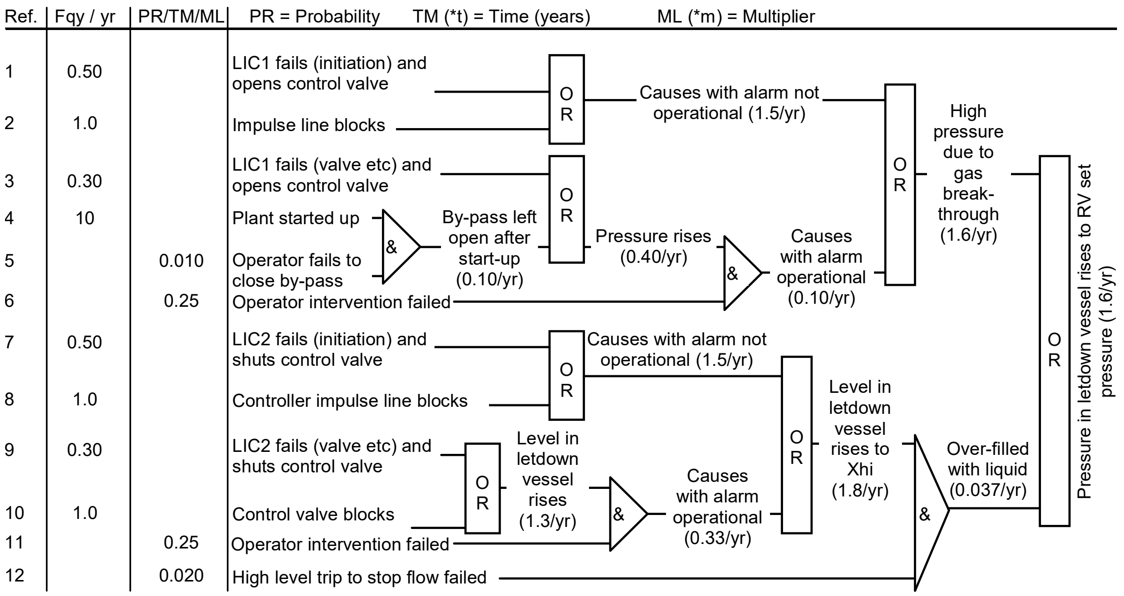
If rupture occurred the material released would probably ignite and cause a fire. Clearly there would be a hazard to any operators in the vicinity and also considerable plant damage causing a shut down with subsequent loss of profit. It would seem reasonable therefore to accept either FAR[14] or cost as a criterion.

The demand rate on the relief valve on the let down vessel has been evaluated using the fault tree shown in Figure D-20.

[13] Fatal Accident Rate
[14] Fatal Accident Rate

FIGURE D-20 FAULT TREE FOR DEMANDS ON RELIEF VALVE

Logic Diagram



Ref.	Fqy / yr	PR/TM/ML	PR = Probability TM (*t) = Time (years) ML (*m) = Multiplier
1	0.50		LIC1 fails (initiation) and opens control valve
2	1.0		Impulse line blocks
3	0.30		LIC1 fails (valve etc) and opens control valve
4	10		Plant started up
5		0.010	Operator fails to close by-pass
6		0.25	Operator intervention failed
7	0.50		LIC2 fails (initiation) and shuts control valve
8	1.0		Controller impulse line blocks
9	0.30		LIC2 fails (valve etc) and shuts control valve
10	1.0		Control valve blocks
11		0.25	Operator intervention failed
12		0.020	High level trip to stop flow failed

OR
Causes with alarm not operational (1.5/yr)
OR
&
By-pass left open after start-up (0.10/yr)
Pressure rises (0.40/yr)
&
Causes with alarm operational (0.10/yr)
OR
High pressure due to gas break-through (1.6/yr)
OR
Causes with alarm not operational (1.5/yr)
OR
Level in letdown vessel rises (1.3/yr)
&
Causes with alarm operational (0.33/yr)
OR
Level in letdown vessel rises to Xhi (1.8/yr)
&
Over-filled with liquid (0.037/yr)
OR
Pressure in letdown vessel rises to RV set pressure (1.6/yr)

The demand rate, D, is thus 1.6 times/year. Say the relief valve will fail to lift fully 0.015 times/year and is overhauled every two years. Then the hazardous event rate for overpressure of the vessel is calculated from equation D.5.12 because DT is high.

H = 0.015 x (I - exp (- 1.6 x 2/2))
= 0.015 x 0.8
= 0.012/year
or once in 80 years

The extent to which the vessel will be overpressurised would depend on the extent to which the relief valve failed to lift. If, say, there is a 5% chance that the failure causes the valve to stick shut then in that case the vessel would almost certainly rupture as the pressure available is almost six times the design pressure of the vessel at risk. Hence the hazardous event rate for rupture of the vessel would be:

H = 0.5 x 0.012
= 0.006/y

If the operator most at risk spends 50% of his time in the hazardous area and a study of similar incidents suggests that there would be at least a 1/100 chance that he could be killed then from equation D.6.1

FAR = $H \times P_{exp} \times Pf \times 10^8 / 8760$
= $0.006 \times 0.5 \times 0.01 \times 10^8 / 8760$
= 0.34

Circumstances might be such that this would be considered acceptable but uncertainty about some of the data (e.g. the probability of fatality occurring might well be greater than 1 in 100) could mean that some improvement was deemed necessary.

There are certain simple improvements which could be carried out at little cost e.g.

a. Modify the impulse lines to make them less prone to blockage
b. Put the low level alarm on a separate initiator
c. Fit a high pressure alarm on the let down vessel

Modification (a) could reduce demands on the relief valve by about half. Either alarm, particularly (b), would increase the chances of operator intervention and those demands for which there was previously no operator intervention could also be reduced. Overall, the demand rate on the relief valve could be reduced to about 0.2/y i.e. an improvement of eight times, most likely sufficient.

A simple estimate of the amount of money that might be spent on such modifications can be obtained as follows:

H= 0.006 /year
C_H = \$1M(say)
Hence $H \times C_H$ = \$6,000 /year

It could therefore be justifiable to spend up to about \$15000 of capital to significantly reduce the hazardous event rate. Hence more sophisticated additional protection could be considered, for instance a low level trip, to stop the liquid flow. This would not only reduce the hazardous event rate but also greatly reduce the number of times material would be discharged from the relief valve.

D.9.3 A control loop with a trip "tagged" on - assessment of a Protective system

Figure D-21 shows a reactor which is pressure controlled by a valve in the gas inlet. If the pressure in the reactor rises above the control point, the bursting disc is liable to rupture. With the aim of reducing the frequency of the disc rupturing, a pressure switch has been installed on the pressure transmitter output to initiate a shut down on high reactor pressure. A very superficial examination shows that this arrangement achieves little improvement. The main causes of high reactor pressure are:

a. Failure of the transmitter to a low output
b. Failure of the controller to a high output or manual control error e.g. on start up
c. Control valve failing open (valve or positioner fault)

If fault 1 occurs, the pressure switch will not operate. A safe shut down is likely for fault 2. If fault 3 occurs, it is unlikely that the valve will respond to the shutdown system. Thus, if fault modes 1, 2 and 3 occur with equal frequency, the protective system only has the potential to reduce the frequency of rupture of the disc by about one third.

Similar systems are sometime specified where a separate transmitter is installed to operate the pressure switch but which again uses the control valve for shut down. Such a system only has the potential to reduce the demand rate on the bursting disc by about two thirds.

The protective system's effectiveness is sharply improved when, in addition to its own transmitter, it also has its own shut down valve. The integrity of this simple system can be further improved, at little extra cost, by arranging to close the control valve as well, when the protective system operates, as shown in Figure D-22.

In assessing this system the following points should be borne in mind.

- When a demand arises due to failure of the control valve, it should be assumed that only one shut down valve is potentially available.
- Demands may arise as a result of a control loop failure, which also affects the protective system. Examples of such dependent failures might be failure of a common power supply to the transmitters or blockage of both pressure impulse lines.

Thus the demand rate on the bursting disc is reduced to:

D = Demand rate resulting from dependent failures of control loop and protective system
+ Demand rate due to control valve failure x PFDavg1
+ Demand rate due to other control system faults x PFDavg2

where PFDavg = PFDavg of protective system (1 out of 1 shut down valves)

PFDavg2 = PFDavg of protective system (1 out of 2 shutdown valves)

This is shown diagrammatically by the fault tree in Figure D-23. Typically, a protective system like this could reduce the frequency of rupture of the bursting disc by one to nearly two orders of magnitude compared with the system in Figure D-21. This example illustrates the importance of keeping instrumented protective systems separate from control systems. Also, that qualitative assessment can often be adequate to demonstrate a need for some improvements to a system.

FIGURE D-21 UNSATISFACTORY ARRANGEMENT WITH TRIP "ADDED ON" TO CONTROL LOOP

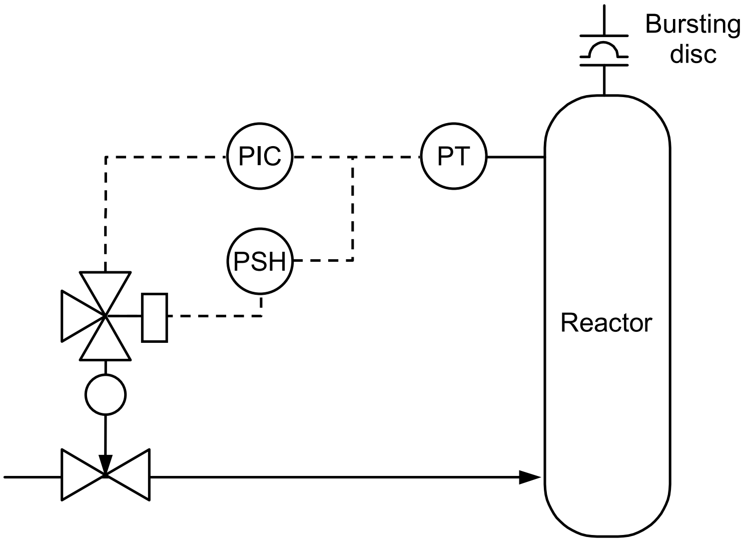


FIGURE D-22 IMPROVED ARRANGEMENT WITH INDEPENDENT TRIP

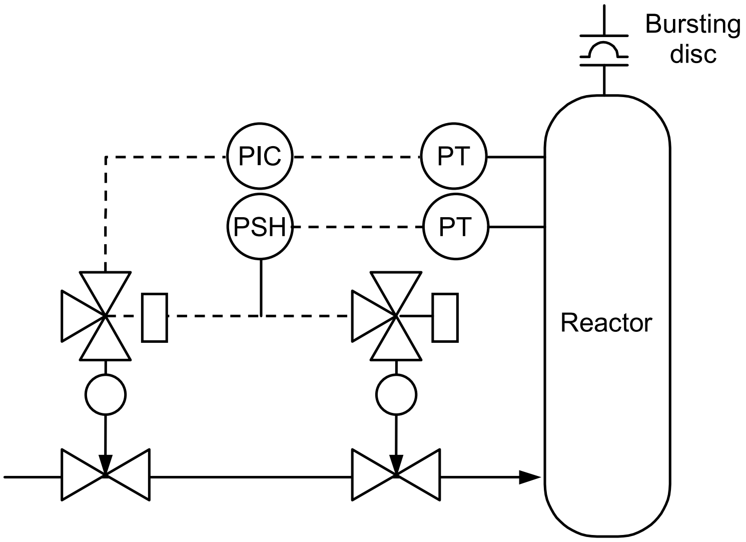
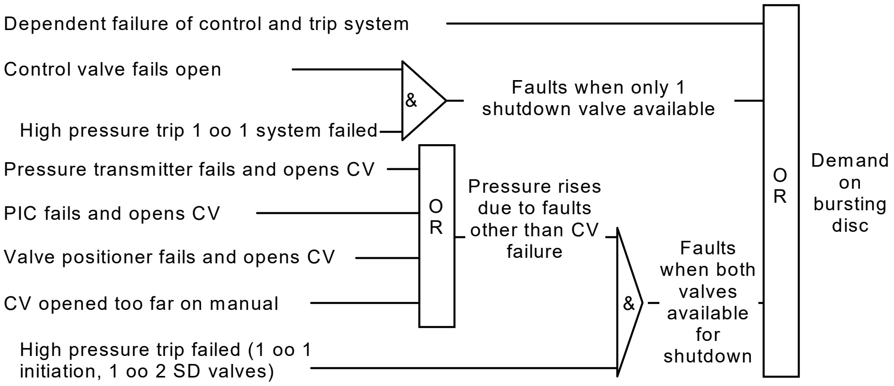


FIGURE D-23 FAULT TREE FOR DEMANDS ON BURSTING DISC FOR MODIFIED TRIP SYSTEM


Dependent failure of control and trip system
Control valve fails open
High pressure trip 1 oo 1 system failed
&
Faults when only 1 shutdown valve available
Pressure transmitter fails and opens CV
PIC fails and opens CV
Valve positioner fails and opens CV
CV opened too far on manual
OR
Pressure rises due to faults other than CV failure
High pressure trip failed (1 oo 1 initiation, 1 oo 2 SD valves)
&
Faults when both valves available for shutdown
OR
Demand on bursting disc

D.10 Pitfalls

There are a number of pitfalls to watch out for when doing a hazard analysis. Some are noted below:

D.10.1 Not getting adequate information

If a realistic analysis is to be carried out then it is clearly vital that the problem is properly understood and correct information obtained.

D.10.2 Not getting the logic right

Perhaps the most important factor in any analysis is getting the logic right, hence checking and testing of the logic and fault trees is very necessary.

D.10.3 Not developing demand and fault trees in small steps

Working in small steps helps get the logic right.

D.10.4 Not recognising dependent failure effects

The need to be always on the lookout for dependent failures has been stressed in sections D.4 and D.7.

D.10.5 Failing to use realistic data

Data from an actual similar system is best: but often not available and so the analyst turns to a data book. Such data must be used with circumspection as the situations for which it is truly valid will rarely be precisely known.

D.10.6 Wrong combinations of data

Common sources of error are the combination of frequencies through AND gates and the addition of frequencies to probabilities at OR gates (see section D.5.2 and D.5.3).

D.10.7 Not getting data in consistent or correct units

Errors can arise, for instance, when “time” appears in various units, e.g. months and years, and is not converted to a common basis.

When data is collected from plant operating history it is mostly obtained as frequencies and the conversion of these frequencies to failure rates can be easily overlooked.

D.10.8 Not recognising situations of high demand rate when the simple expression

$H = D \times PFDavg$ does not apply.

If in doubt always check the value of the parameters DT and θT to decide whether the more rigorous equation should be used (see Section D.5.3.3). Remember the rule of thumb that to be effective the frequency of testing of a simple protective system should mostly be such that there should be less than one demand per proof test period.

D.10.9 Over-estimating the reliability of protection

In calculating the PFDavg for a protective system it is possible to get a very low PFDavg by redundancy and frequent testing e.g. a 1 out of 3 trip system where $\theta = 0.5$ and $T = 1$ month has a PFDavg given by $PFDavg = \theta^3T^3/4 = 1.8 \times 10^{-5}$ which is equivalent to nearly ten minutes per year.

As described previously, dependent failure probability must be assessed as it is very likely that dependent failures will dominate the overall achieved PFDavg.

Expert advice may need to be sought for the assessment of those situations.

D.10.10 Overconfidence in numerical values.

Sometimes the uncertainty in numerical data can be over-looked and too high an accuracy ascribed to a quantified hazardous event rate. Sensitivity checks should always be done on critical parts of the analysis and judgement used to maintain a sense of reason.

D.10.11 Failure to check the credibility of the result.

It is always sensible whenever possible to test results against the judgement of experienced people.

D.10.12 Failure to follow through and check / verify the validity of assumptions.

D.10.13 Most analyses require some assumptions to be made.

The analysis will be invalid if those assumptions are not justified.

D.10.14 Failure to check that subsequent modifications or changes do not invalidate the analysis.

An analysis may only be valid for a very specific set of circumstances. Changes may require the analysis to be updated.

Finally, but by no means least.

D.10.15 Failure to recognise one's limitations and seek expert advice.

This document has aimed to give sufficient information to enable straight forward hazard analyses to be performed. The analysis of a complex system, particularly with redundant and diverse protective systems can become involved and expert help is essential.

D.11 Bibliography

Recommended Reading

Title	Process Safety Analysis - An Introduction
Author	Skelton, B
Publisher	ICHEME
Year	1997
ISBN	085295378X
Description	Focuses on process industry issues; parallels the approach to Hazards and Safety in this document. Written as a student text book.

Title	Hazard Identification and Risk Assessment
Author	Wells, G
Publisher	ICHEME
Year	1996
ISBN	0852953534
Description	Good introductory text looking at hazard and risk quantification techniques.

Title	Reliability, Maintainability and Risk
Author	Smith, D J
Publisher	BH
Year	1993
ISBN	0750637528
Description	Covers all the main aspects of reliability; includes methodology for dependent failure. Highly useful text.

Human Factors

Title	A Guide to Practical Human reliability Assessment
Author	Kirwan, B
Publisher	Taylor & Francis
Year	1994
ISBN	0748401113
Description	An excellent guide to the methods of human reliability assessment.

Title	Human Reliability and Safety Analysis Data Handbook
Author	Gertman, D I & Blackman, H S
Publisher	Wiley
Year	1994
ISBN	0471591106
Description	Interesting overview of human factors; strong influence from US nuclear industry

Title	A Guide to Task Analysis
Author	Kirwan, B & Ainsworth, L K
Publisher	Taylor & Francis
Year	1992
ISBN	0748400583
Description	An excellent guide to the methods of task analysis.

Title	An Engineer's view of Human Error
Author	Kletz, T
Publisher	ICHEME
Year	1991
ISBN	0852952651
Description	Primarily a discussion on the issues of human error. Some review of error probabilities but mostly review of situations, and organisational issues.

Title	Human Error
Author	Reason, J
Publisher	CUP
Year	1990
ISBN	0521314194
Description	Classic discussion of the nature and origins of human error.

Programmable Systems

Title	Use of Computers in Safety Critical Applications
Author	-
Publisher	HSC
Year	1998
ISBN	0717616207
Description	Report of Study into systems for Sizewell B - considers practical PFD limits

Title	Safety Critical Computer Systems
Author	Storey, Neil
Publisher	Addison Wesley
Year	1996
ISBN	0201427877
Description	Discusses the issues of design, management and operation of Programmable Systems

Further References

The following references are included for continuity. Most of them are somewhat "historic" but some may nevertheless be of interest to the analyst.

A number of references are given for further reading to amplify and extend the various aspects of hazard analysis that have been introduced in this document. The list is not fully comprehensive and many further references can be obtained from those given.

Hazard Analysis

1. “Hazard Analysis - a quantitative approach to safety”
Kletz, T A
I. Chem. E Symposium Series No 34 (19Th) p 75

2 “Evaluate risk in plant design”
Kletz, T A
Hydrocarbon Processing 56 No 5 (1977), p 297

3 “Practical applications of hazard analysis”
Kletz, T A
A.I.Ch.E, Loss Prevention, Volume 12, (1979), p 34

4 “Operability Studies and Hazard Analysis”
Lawley, H G
Chemical Engineering Progress, 70, No 4, (1974), ~ 45

5 “The Design of New Chemical Plants Using Hazard Analysis”
Gibson, S B
I.Chem.E Symposium Series No 47, (1976), p 127

6 “A Guide to Hazard and Operability Studies”
Knowlton, R E
Chemical Industry Safety and Health Council of the
Chemical Industries Association, 1977

7 “From System Reliability to long term safety assurance”
Hensley, G
Second National Reliability Conference, March 1979, Paper 2A/2

8 “Loss Prevention in the Process Industries” (Chapters 8 & 9)
Lees, F P
Butterworths, London, 1980

9 “Safety Technology in the Chemical Industry A problem in hazard analysis with solution”
Lawley, H G
Reliability Engineering 1 (1980) p 89

10 ‘Hazards of Oxychlorination”
Illidge J T and Woistenholme J
A.I.Ch.E, Loss Prevention, Volume 12, (1979) p 103

11 “Canvey - an investigation of potential hazards from operations in the Canvey Island/Thurrock area”
Health and Safety Executive, 1978, H.M.S.0. London

12 “An. assessment of accident risks in U.S. Commercial nuclear power plants”
Report WASH 1400
Atomic Energy commission, 1975, Washington DC

Fault tree analysis and evaluation

13 "The propagation of faults in process plant: a state of the art review"
Andow P K, Lees F P and Murphy C P
I Chem. E Symposium Series No 38, (1980), p 225

14 "Fault tree analysis for system reliability"
Grosetti, P A
Instrumentation Technology, August 1971, ~ 52

15 "Reliability and fault tree analysis"
Barlow R E, Fussel J B and N D Singpurwalla, editors
S. I.A.M. Philadelphia 1975

16 "Computer aided fault tree synthesis"
Powers G J and Lanp S A
Chem. Eng. Prog. 72, No 4, (1976), p 89

17 "A synthesis strategy for fault trees in chemical processing systems"
Powers G J and Tomkins F C
A.I.Ch.E, Loss Prevention, Volume 8, (1974), p 91

18 "A formal methodology for fault tree construction"
Fussel J 3
Nuclear Sci. Eng. 52, p 421

19 "Safety and reliability decision making by loss rates"
Browning R L
A.I.Ch. E, Loss Prevention, Volume 7, 1973, p 1

20 "Computer aided operability studies for loss control"
Lihou D A, Rahimi R and Fletcher J P
3rd International Symposium on Loss Prevention in the Process Industries,
Basle, September 1980, p 579

21 "Reliability Quantification techniques used in the Rasmussen Study (WASH 1400)"
Vesely W B
p 775-803 of reference 15
See also reference 4, 8 (chapters 7 and 9) and 9

Criteria

22 "What risks should we run?"
Ketz T A
New Scientist, 74 No 1051, (1977), p 320

23 "The Development and Application of Quantitative Risk Criteria for Chemical Processes"
Bulloch B C
I. Chem. B Symposium Series No 39a, (1974), p 289

24 "The Quantitative measurement of process safety"
Gibson S B
I. Chem.E Symposium Series No 49, (1977), p 1

25 "Experience in the reduction of risk"
Farmer F R
I. Chem. E Symposium Series No 34, (1971) p 82

26 "Methods of determining the optimum level of Safety expenditure"

Melinek S J
Building Research Establishment, paper CP88/74

27 "A scale or measuring risks".
Reissland J and Harries V
New Scientist, 15 September 1979, p 809

28 "The application of hazard analysis to risks to the public at large"
Kletz T A
Proceedings of the Symposium on Chemical Engineering in a Changing World, edited by Koetsier ':W T, Elsevier, 1976, p 397

29 "Quantification of toxic gas emission hazards"
Sellars J G
I. Chem. B. Symposium Series No 47, (1976), p 127

30 "Major hazards - Should they be prevented at all costs?"
Gibson S B
Eurochem Conference "Chemical Engineering in a Hostile World",
Birmingham, June 1977

31 "Major Accident Criteria"
Lowe D R T
Eurochem 80 Conference, Birmingham, June 1980, paper 5/1

32 "Criteria for decisions on acceptability of major fire and explosion hazards with particular reference to the chemical and fuel industries'.
Rasbash D J
I. Chem. E Symposium Series No 58, (1980), p 25

33 "Accident fatality number - a supplementary risk criterion"
Lees F P
as ref 20 p 426

34 "Individual risk - a compilation of recent British data"
Grist D R
Safety and Reliability Directorate (UKAEA) SR.D R 125, HMSO, 1978
See also reference 1, 8 (chapters 4 and 9), 11 and 12

Protective Systems

35 "Specifying and designing protective systems"
Kletz T A
A.I.Ch.E. Loss Prevention, Volume 6 (1972), p 15

36 "High pressure trip systems for vessel protection"
Lawley H G and Kletz T A
Chemical Engineering, 12 May 1975, p 81

37 "High integrity protective systems"
Stewart R M
The Chemical Engineer, October 1974, p 622

38 "Design and Maintenance of Instrument Trip Systems"
Gibson M R and Knowles G
1st National Conference on Reliability, Nottingham
September 1977, paper NRC 4/11

39 "Factors influencing the limitations to fractional dead time that can be achieved in real protective systems"
Robinson B W

As reference 38, paper NRC 3/1
40 "Optimal test intervals for safety systems"
Lihou D A and Kabir Z
Terotechnica 1. (1980), p 207
41 "On line trip testing"
Hullah J
Chem. Eng. Prog. April 1976, p 72
42 "Common Mode Failure Considerations in the design of systems for protection and control"
Euler E P
Nuclear Safety, 10 No 1 (1969)
43 "Study of Common Mode Failures"
Edwards G T and Watson I A
as reference 34, SRD R 146, HMSO, 1979
44 "Safety assessment of automatic and manual protective systems for reactors"
Green A E
UKAEA, Report AHSB (S) R 172
See also reference 7, 8 (chapter 13) and 10

Failure data for equipment

45 "The reliability of instrumentation"
Lees F P
Chem. Ind. March 1976, p 195
46 "Some data on reliability of instruments in the chemical plant environment"
Anyakora S N, Engel GFM and Lees FP
The Chemical Engineer, November 19, p 396
47 "A review of instrument failure data"
Lees F P
I.Chem. E Symposium Series No 47, (1976), p 73
48 "Plant and process reliability"
Hensley G
Instrument Practise, November 19Th
49 "The uses, availability and pitfalls of data on reliability"
Kletz T A
Process Technology International 18 No 3 (1973), p 111
50 "Accident data - the need for a new look at the sort of data that are collected and analysed"
Kletz T A
Journal of Occupational Accidents, 1 No 1 (1976), p 95
51 "Problems of data collection"
Gibson S B
Symposium "Safety in the Chemical Industry" UMIST, April 1978
52 "Comparison of Predicted and Actual Hazard Rates" Taylor A
2nd National Reliability Conference, March 1979, Paper 4B/l
53 "Instruments - how reliable can you get?"
Anon
Process Eng. June 1978, p 50
54 "Learn from equipment failure"

Turner B
Hydrocarbon Processing, November 1977, p 317

55 "Field data from the chemical industry"
Gibson M R
2nd National Reliability Conference, Birmingham, 1979, paper 2B/2
See also reference 8 (chapter 7) and 36

Human error

56 "A quantitative approach to the evaluation of the safety function of operators on nuclear reactors"
Ablitt J F
UKAEA, Report ARSB (5) R160, 1969

57 "Design Techniques for Improving Human Performance in Production"
Swain A D
Industrial and Commercial Techniques Limited, Seminar Handbook 1972 et sec

58 "The nature of human error"
Rigby L V
Chemical Techno1ogy, December 1971, p 712

59 "The human operator in process control"
Edwards E and Lees F P (editors)
Taylor and Francis, London, 1971+

60 "Design approaches to reducing human error in process plants"
Embrey D
I Chem. E Design 79, University of Aston, September 1979

61 "Hazard analysis and the human element"
Howland A
as reference 20, p 174

62 "Process alarm systems as a monitoring tool for the operator"
Kortland D and Kragt H
as reference 20, p 801
See also reference 8 (chapter 14) 21 and 44

D.12 Notation

C	Annual cost of hazardous event (= H CH) $/y
CH	Total cost of hazardous event ($)
CM	Annual cost of reducing hazard ($/y)
D	Demand rate (times/year)
PFDavg	PFDavg
q	Fail to danger failure rate (faults/year)
FAR	Fatal Accident Rate (fatalities/l08 exposed hours)
H	Hazardous event rate (times/year)
m	Number of channels requiring to register the trip condition before a protective system with redundancy will function.
N	Total number of channels in a protective system with redundancy.
P, p	Probability
Pf	Probability that exposure to the hazardous event will prove fatal.
Pexp	Proportion of time that the person most at risk spends in the hazardous area.
r	Number of channels of a protective system that have to fail-to-danger before the system will fail to perform correctly on demand.
S	Fail Safe (spurious) failure rate (faults/year)
t	Time (years)
T	Proof test period (years)

D.13 Summary of rules for constructing fault trees

Aims: To do as simple a study as possible i.e. get the maximum benefit from the minimum of work. This requires:

b. The correct logic

c. The most significant causes to be identified

d. A 'broad brush" fault tree to be drawn initially and only the areas of significant concern developed in greater detail

Requirements:

a. A physical description of the system

b. A logical description of the system

c. A clear definition of the hazardous event of concern

d. A plant visit (if the system exists)

Key points for drawing up the fault tree:

a. The fault tree is composed of events joined by “AND” and “OR” gates

b. Start with the hazardous event

c. Draw a demand tree first, and then create the fault tree from the demands with the protective systems added

d. Think in small steps

e. Check very carefully for dependent failures

f. There is not necessarily a single "correct" fault tree

g. Have a reasonable and adequate description at every gate

h. Check the logic of a completed tree by working along each branch to the final event

D.14 Summary of rules for combining events for the evaluation of fault trees

These rules only apply directly when the events are totally independent of each other.

Probability (P)

$P_{(A \text{ or } B)} = P_A + P_B - P_AP_B$

$= P_A + P_B$ (if P_A and P_B are small)

$P_{(A \text{ and } B)} = P_AP_B$

Frequency (F)

$F_{(A \text{ or } B)} = F_A + F_B$

where t_A, t_B are the duration of the events

$t_{(A \text{ and } B)} = t_At_B/(t_A + t_B)$

NB: F and t must be in consistent units e.g. y^{-1} and y respectively

PFDavg:

For single channel protective system:

PFDavg = $\theta T / 2$

where θ = fail to danger failure rate, T = Proof test period, and $\theta T << 1$

NB: θ and T must be in consistent units

Hazardous event Rate (H)

H = D x PFDavg (if $\theta T << 1$ and $DT << 1$)

where D = demand rate on the protective system, and θ = fail danger rate of the protective system.

If DT is large then: $H = \theta (1 - \exp(-D T /2))$

If there is no proof testing: $H = \theta D/ (\theta +D)$

NB: θ,D and T must all be in consistent units.

D.15 Terms relating to Numerical Hazard Analysis

ABNORMAL CONDITION

Any disturbance, change or circumstance which could, by itself or combined with other circumstances, cause a hazardous event if it went unchecked.

CHANNEL

One set of equipment to perform a given function in a protective system having redundancy.

COMMON MODE EFFECT

See DEPENDENCY

DEMAND

The requirement for a protective or stand-by system to operate owing to an abnormal process condition or process equipment failure.

DEMAND RATE

The rate at which demands occur (usually per year).

DEMAND TREE

A demand tree is a model that graphically and logically represents the various combinations of events and conditions, both fault and normal, that, if they occurred unchecked, would cause the hazardous event to occur. Protective systems are not included. A demand tree is often drawn prior to a fault tree. Events and conditions are linked through logic gates.

DEPENDENCY

There are 2 different types of dependency:

Functional dependency

A single failure or condition which results, in turn, in the coincidental failure of multiple systems (e.g. electrical supply failure, or instrument air failure, failure of an item common to control and protection or to different channels of the protective system (e.g., blockage of a pressure measurement connection common to control and trip systems).

Classic dependency

The failure of multiple items of equipment due to a common cause or in a common mode, e.g., common maintenance error, vibration, high temperature, faulty batch of equipment.

DIVERSITY

The performance of the same overall protective function by a number of independent and different means. This helps to reduce dependency.

EXPOSURE

A person is exposed to a hazardous event if that person is in an area where there is a finite probability of injury by the hazardous event if it occurred.

FAILURE

A condition of a device under which it is rendered incapable of performing adequately in the desired manner. Failures may be apparent i.e. revealed or hidden i.e. unrevealed.

FAIL SAFE

Failure resulting in a safe process condition; normally attributed to protective systems in which the fail safe fault causes the system to actuate and cause a spurious trip

FAIL TO DANGER

Failure which results either directly in a hazardous process condition, or which renders stand-by equipment incapable of operation on demand. Such a failure in a protective system normally remains unrevealed until discovered by testing or by a demand.

FATAL ACCIDENT RATE (FAR)

The number of fatalities occurring in $l0^8$ exposed person hours (or approximately the number of deaths from industrial injury in a group of 1,250 men exposed to the same hazard during their working lives.) (Used to be called FAFR - Fatal Accident Frequency Rate, but this is dimensionally incorrect and should not be used)

FAULT TREE

A fault tree is a model that graphically and logically represents the various combinations of possible events, both fault and normal, occurring in a system that cause the hazardous event to occur. It is developed either directly or from a demand tree by including other means (i.e. operator interventions) that can function to prevent the hazardous event occurring.

FRACTIONAL DEAD TIME

An obsolete term, replaced by PFDavg.

HAZARD

A Hazard is a physical situation with potential to cause loss, damage or undesirable effect on plant, equipment, product, people, the environment or profit.

HAZARDOUS EVENT

The occurrence of an incident with potential to cause loss, damage or undesirable effect on plant, equipment, product, people, the environment or profit.

HAZARDOUS AREA

The area within which a person is deemed to be exposed to the hazard.

HAZARDOUS EVENT RATE

The rate at which the hazardous event occurs, usually expressed as per year.

LOGIC GATES

Events and conditions in demand and fault trees are linked by either of two basic logic gates:

OR gate - output event will exist if any one or more of input events exist.

AND gate - output event will exist only if all input events exist together simultaneously

LOGIC DIAGRAM (Fault tree)

A diagrammatic representation in which all the equipment that must work (or fail) and all the actions that need to be performed correctly (or incorrectly) are linked to indicate the possible route(s) from a defined starting condition to a defined objective which can be either “success” or “failure”.

‘LOGIDRAW’

An ICI-developed Windows 95 computer program for preparing and printing fault trees. It is available as part of the ABB Process Engineering Library (PEL).

PFDavg (Average Probability of Failure on Demand)

The average probability of a protective system failing to perform its design function on demand. This can be a predicted value, or achieved value or a target value.

PROBABILITY

A measure of the uncertainty of the outcome of an event expressed numerically between 0 = impossibility and 1 = absolute certainty.

PROOF TESTING

A method of ensuring that a component, equipment or system possesses all the required performance characteristics and is capable of responding to input conditions in the manner desired.

PROTECTIVE SYSTEM

All the equipment which protects a plant from the effect of abnormal conditions. It may be fully automatic or require some manual action. It may be mechanical, e.g. a relief valve, or instrumented e.g. a trip or alarm system.

RATE

The number of events per unit operating (on-line) time.

REDUNDANCY

The performance of the same overall function by a number of independent means.

RELIABILITY

The probability that an item of equipment will perform in the manner desired.

SPURIOUS TRIP

A protective system operating, without a demand, as a result of a fail-safe fault in the system.

TRIP

An instrumented protective system or the event of operation of such a system.

UNAVAILABILITY/ UNRELIABILITY

The probability that an item of equipment will not be able to perform in the manner desired.

VOTING SYSTEM

An arrangement of a protective system whereby a specified number of channels of a system with redundancy have to respond correctly to an abnormal condition before the protective system will perform its function.