

Integrity of safety-related systems in the gas industry



*Founded 1863
Royal Charter 1929
Patron: Her Majesty the Queen*

***IGEM/SR/15 Edition 5 - with amendments December 2015
Communication 1784***

Integrity of safety-related systems in the gas industry



Price Code: C4H
© The Institution of Gas Engineers and Managers
IGEM House
26-28 High Street
Kegworth
Derbyshire, DE74 2DA
Tel: 0844 375 4436
Fax: 01509 678198

Email: general@igem.org.uk



Documents

Document Sharing Hub

Copyright © 2015, IGEM. All rights reserved

Registered charity number 214001

All content in this publication is, unless stated otherwise, the property of IGEM. Copyright laws protect this publication. Reproduction or retransmission in whole or in part, in any manner, without the prior written consent of the copyright holder, is a violation of copyright law.

ISBN 978 1 905903 60 3

ISSN 0367 7850

Published by the Institution of Gas Engineers and Managers

Previous Publications:

Communication 1419 (1989) – 1st Edition

Communication 1581 (1994) – 2nd Edition

Communication 1649 (2002) – 3rd Edition

Communication 1711 (2005) – 4th Edition

Communication 1746 (2010) – 5th Edition

For information on other IGEM Standards, visit our website, www.igem.org.uk

CONTENTS

SECTION		PAGE
1	Introduction	1
2	Scope	4
3	Tolerable risk and safety-integrity criteria	5
	• 3.1 Individual and societal risk	5
	• 3.1.1 Background	5
	• 3.1.2 Maximum tolerable and broadly acceptable risks	5
	• 3.2 Safety integrity levels (SILs)	10
	• 3.2.1 Introduction	10
	• 3.2.2 Low demand	11
	• 3.2.3 High demand	12
	• 3.2.4 Interpretation of “not-safety-related”	13
	• 3.2.5 Approaches to integrity targeting	13
	• 3.2.6 Template outline of integrity targeting	15
	• 3.2.7 SIL 3 targets	17
	• 3.2.8 Hierarchy of measures	17
4	Random hardware failures	18
	• 4.1 Hardware failures	18
	• 4.2 Failure rate data	18
	• 4.3 Common cause failure (CCF)	18
	• 4.4 Human error	19
5	Architectures (Safe failure fraction (SFF))	21
	• 5.1 Architectures	21
	• 5.2 Alternative to SFF	22
6	Life-cycle activities (hardware and software)	23
	• 6.1 Functional safety life-cycle and safety plan	23
	• 6.2 Functional safety requirements specification	25
	• 6.3 Safety manual	26
	• 6.4 Design review, integration and test	26
	• 6.5 Validation	28
	• 6.6 Modifications	28
	• 6.7 Installation and commissioning	29
	• 6.8 Operation and maintenance	30
	• 6.8.1 Hardware	30
	• 6.8.2 Software	30
	• 6.8.3 Software modifications	31
	• 6.9 Security	32
	• 6.9.1 Access to the system on site	32
	• 6.9.2 Remote access to systems	32
	• 6.10 Proven-in-use	33

7	Life-cycle activities (hardware)	34
• 7.1	Hardware design	34
• 7.1.1	One out of two (1oo2) voting	34
• 7.1.2	Two out of two (2oo2) voting	34
• 7.1.3	Two out of three (2oo3) voting	34
• 7.1.4	Two out of two, reverting to one out of one (1oo2D) voting	34
• 7.1.5	Common cause failure (CCF)	35
• 7.2	Safety monitors	35
• 7.3	Fault tolerance	35
• 7.4	Programmable logic controllers (PLCs)	36
• 7.5	Communicating with field devices	36
• 7.6	Electromagnetic compatibility (EMC)	37
• 7.7	Alarms	37
8	Life-cycle activities (software)	38
• 8.1	Design cycle	38
• 8.1.1	User requirement specification	38
• 8.1.2	Functional design specification	38
• 8.1.3	Software design specification	38
• 8.2	Design methods	38
• 8.3	Processors	39
9	Functional safety management (FSM)	40
• 9.1	Quality Management System (QMS)	40
• 9.2	Functional Safety Management	40
• 9.3	Competence	41
10	Assessments and ALARP	42
• 10.1	Carrying out assessments	42
• 10.1.1	Target risks and SILs	42
• 10.1.2	Random hardware failures and ALARP	42
• 10.1.3	Architectures (SFF)	42
• 10.1.4	Life-cycle activities	42
• 10.1.5	Functional safety capability	42
• 10.2	ALARP	43
• 10.2.1	Principle	43
• 10.2.2	Gross disproportionality	44
• 10.2.3	Cost per life saved	44

11	Applications	46
• 11.1	Burners and combustion management	46
• 11.1.1	Integrity targets	46
• 11.1.2	Generic requirements	46
• 11.1.3	Configurations for full sequence automatic burner control	47
• 11.1.4	Burners in complex plant	48
• 11.1.5	Semi-automatic burner control systems	48
• 11.1.6	Combustion efficiency control systems	48
• 11.1.7	Valve proving systems	48
• 11.1.8	Domestic appliances	49
• 11.2	Supply pressure and volumetric control	51
• 11.2.1	General	51
• 11.2.2	Generic configurations	51
• 11.2.3	Pneumatic overrides	53
• 11.2.4	Boundary control	53
• 11.3	Fire and gas detection and plant shutdown	55
• 11.3.1	Fire and gas detection	55
• 11.3.2	Emergency shutdown	56
• 11.4	Plant and grid management systems	57
• 11.5	Gasholder control	58
• 11.5.1	General	58
• 11.5.2	Typical gasholder arrangements	59
• 11.5.3	Control envelope	59
• 11.5.4	Telemetry	61
• 11.6	Metering and logging	61
• 11.6.1	Flow meters	61
• 11.6.2	Flow meters (pre-payment)	62
• 11.6.3	Data logging	62

APPENDIX

1	Glossary, acronyms, abbreviations, symbols and units	63
2	References	65
3	Rigour of assessment	67
4	A worked example based on a gas detection system	70
5	Relevant guidance	74

FIGURES

1	Criteria per number of fatalities	9
2	Selection of high or low demand SIL	11
3	Typical risk graph	14
4	Fault tree model	16
5	β Model	18
6	Simplified safety life-cycle	24

7	Development life-cycle model	27
8	'V' model	28
9	The ALARP triangle	43
10	Individual risk	44
11	Typical layout of a general purpose single-channel PES used for burner management and supervision	47
12	An example of an automatic oven time control	49
13	Typical automatic sequence control	50
14	Slam-shut PES plus single control PES per stream	52
15	Single slam-shut PES plus pneumatic control	52
16	Single control PES	53
17	Optimisation of output pressure – option (A)	54
18	Optimisation of outlet pressure – option (B)	54
19	Optimisation of output pressure – option (C)	54
20	Typical fire/gas detection system	56
21	Duplex ESD system	57
22	Typical gasholder height monitoring and control sensors	60

TABLES

1	Typical fatality frequencies	5
2	Target individual risks	6
3	Target multiple fatality risks	6
4	Target individual risks for injury	7
5	Environmental risk targets	10
6	Low demand rate SILs	11
7	High demand rate SILs	12
8	Elements leading to maximum tolerable failure rate	15
9	Possible SIL outcomes	17
10	Moon factor from Betaplus	19
11	Permissible SILs for systems with redundancy	22

SECTION 1 : INTRODUCTION

- 1.1 This Standard supersedes IGE/SR/15 Edition 5, Communication 1746, which is obsolete.
- 1.2 This Standard has been drafted by an Institution of Gas Engineers and Managers (IGEM) Panel, appointed by IGEM's Gas Transmission and Distribution Committee, and has been approved by IGEM's Technical Co-ordinating Committee on behalf of the Council of IGEM.
- 1.3 The purpose of this Standard is to provide recommendations for the design and implementation of safety-related systems. The contents will be of most relevance to managers, engineers and technicians with responsibility (particularly for design and/or safety assessment) during the appropriate phases in the lifecycle of a control or safety system.
- 1.4 The Standard is intended to satisfy the need for industry specific guidance to supplement BS EN 61508. Other supplementary documents are described in Appendix 5 and listed in Appendix 2. In particular IEC 61511 is frequently invoked in respect of this industry (See Appendix 5). This fifth edition continues to update the recommendations and reflects that the principles of BS EN 61508 are not confined to programmable equipment.
- 1.5 Major differences between Editions 4 and 5 are the revision of the targets relating to maximum tolerable risk, enhancements to the Section on integrity targeting and revision of the material relating to life-cycle activities (in particular with regard to the 2010 issue of BS EN 61508). Specific examples of the latter include an alternative to the safe failure fraction metric, the use of safety manuals etc.
- 1.6 Any system is deemed to be safety-related where a failure, singly or in combination with other failures/errors, could lead to death or injury or damage to the environment. An application cannot be excluded from this category merely by identifying alternative means of protection. A formal safety integrity assessment, as described in Section 10, is required in order to establish if a piece of equipment can be categorised as "not safety-related". Therefore, the presence of over-rides or alternative forms of protection, for example pressure relief, does not, of itself, render other equipment "not safety-related".

The same techniques given in this Standard can be applied to design systems to protect property.
- 1.7 This Standard applies to both new equipment under design and to existing equipment. The targets, in both cases, will be the same but the means of assessment may differ. Existing equipment may well be assessed by "proven-in-use" historical data (Sub-Section 6.10) whereas new designs will require the use of predictive techniques.
- 1.8 Functional safety involves identifying specific hazardous failures which lead to serious consequences (for example, death) and then establishing maximum tolerable frequency targets for each mode of failure. Equipment whose failure contributes to each of these hazards is identified and usually referred to as "safety-related".
- 1.9 In practice, a hazard analysis of the plant, system or site, for example a Hazard Identification Study (HAZID), will have identified the hazardous failure mode(s). More formal hazard identification is often carried by means of a HAZOP (Hazard and Operability Study). In consequence, further studies may be needed to assess the adequacy of the control and safety systems and a safety integrity assessment would normally follow. Any HAZOP will need to take account of the

possibility that non-hazardous systems might become hazardous as a result of foreseeable modifications or abnormal operation. HAZOPs vary from formal (detailed) studies of plant performance to broad overviews of the hazards perceived. In practice, for the majority of gas installations, the hazardous conditions are generally “high or low pressure”, “high or low flow”, “high or low temperature” or “overflow or underfill”. The HAZOP need not always be arduous since it can be based on experience of a large number of similar studies, addressing similar hazards.

1.10 Functional Safety is the term used to refer to the Integrity (expressed both quantitatively and by means of safety integrity levels (SILs) called for in respect of safety-related systems).

►1.11 Over the last few years there has been a dramatic proliferation of industry and sector specific guidance documents. These now occupy three chapters of Reference Appendix 2.5 item 1 (now version 4.0) which is itself by no means a total coverage.◀

1.12 This Standard makes use of the terms “should” “shall” and “must” when prescribing particular requirements. Notwithstanding Sub-Section 1.14:

- the term “must” identifies a requirement by law in Great Britain (GB) at the time of publication
- the term “shall” prescribes a requirement which it is intended will be complied with in full and without deviation
- the term “should” prescribes a procedure which, it is intended, will be complied with unless, after prior consideration, deviation is considered to be acceptable.

Such terms may have different meanings when used in legislation, or Health and Safety Executive (HSE) Approved Codes of Practice (ACoPs) or guidance, and reference needs to be made to such statutory legislation or official guidance for information on legal obligations.

1.13 The primary responsibility for compliance with legal duties rests with the employer. The fact that certain employees, for example “responsible engineers”, are allowed to exercise their professional judgement does not allow employers to abrogate their primary responsibilities. Employers must:

- have done everything to ensure, so far as it is reasonably practicable, that “responsible engineers” have the skills, training, experience and personal qualities necessary for the proper exercise of professional judgement
- have systems and procedures in place to ensure that the exercise of professional judgement by “responsible engineers” is subject to appropriate monitoring and review
- not require “responsible engineers” to undertake tasks which would necessitate the exercise of professional judgement that is not within their competence. There should be written procedures defining the extent to which “responsible engineers” can exercise their professional judgement. When “responsible engineers” are asked to undertake tasks which deviate from this, they should refer the matter for higher review.

1.14 It is widely accepted that the majority of accidents in industry can be primarily attributed to human factors because hazards may not have been foreseen, risks may have been inadequately assessed, safety system designs may have significant limitations and working practices may be flawed.

It is therefore necessary to give proper consideration to the management of these human factors and the control of risk. To assist in this, it is recommended that due regard be paid to HSG48.

- 1.15 Notwithstanding Sub-Section 1.11, this Standard does not attempt to make the use of any method or specification obligatory against the judgment of the responsible engineer. Where new and better techniques are developed and proved, they should be adopted without waiting for modification to this Standard. Amendments to this Standard will be issued when necessary, and their publication will be announced in the Journal of the Institution and other publications as appropriate.
- 1.16 Requests for interpretation of this Standard in relation to matters within its scope, but not precisely covered by the current text, should be addressed in writing to Technical Services, IGEM, IGEM House, High Street, Kegworth, Derbyshire, DE74 2DA and will be submitted to the relevant Committee for consideration and advice, but in the context that the final responsibility is that of the engineer concerned. If any advice is given by or on behalf of IGEM, this does not relieve the responsible engineer of any of his or her obligations.
- 1.17 Amendments are shown throughout the document by ► ◄.
- 1.18 This Standard was published in December 2015.

SECTION 2 : SCOPE

- 2.1 This Standard is applicable to safety-related control and protection systems in the gas and process industries, including gas terminals, transmission, distribution and storage and industrial, commercial and domestic gas installations. It is also relevant to offshore installations. In view of the general similarity of equipment in its many applications, this Standard is considered to be suitable for wider application in the process industries.
- 2.2 The scope of this Standard embraces the whole of the control or safety system concerned. It extends from field sensors (or other input devices) through to the field devices (for example, valves, pumps, fans) and includes human factors. The term process refers to all the equipment of the physical process together with the control and protection systems.
- 2.3 This Standard applies to all electrical and electronic systems. Although not specifically included in BS EN 61508, the principles can also be applied to mechanical and/or pneumatic items. Some equipment configurations (for example, IGEM/TD/13) have been formally assessed and shown generally to meet current risk targets (however, see A2.5 (4)).
- 2.4 The term “programmable electronic system” (PES) is the generic description used for all electronic control systems which employ digital computing. PESs consist of both electronic hardware and software code which provides the functionality.
- 2.5 An assessment includes the following elements:
- identify hazards and establish maximum tolerable risks so as to target appropriate SILs for safety functions
 - establish if the hardware reliability meets the requirements implied by the integrity targets
 - ensure that the principle that risks need to be shown to be “as low as reasonable practicable” (ALARP) has been applied to the reliability assessment
 - establish if the architectures, i.e. measures associated with redundancy and proportions of hazardous failures, have been met
 - demonstrate that the life-cycle methods and controls have been applied appropriate to the SIL in question
 - show that all the organizations (from user to equipment supplier) have suitable functional safety competence.
- 2.6 The content of this Standard is largely aimed at designers and safety assessors but, nevertheless, some essential aspects of operation and maintenance are included.

SECTION 3 : TOLERABLE RISK AND SAFETY-INTEGRITY CRITERIA

3.1 INDIVIDUAL AND SOCIETAL RISK

3.1.1 Background

3.1.1.1 Reference shall be made to Table 1.

3.1.1.2 Perception of risk is influenced by the consequences. Thus, equipment damage is more acceptable than personal injury which, in turn, is more acceptable than fatality. Fatality of a member of the public is perceived as being less acceptable than fatality of an employee within the industry (see Tables 2 and 3). In all cases, acceptability reduces as the number of fatalities increases. Such perceptions should be taken into account when setting targets.

Risk involves two measures:

- the frequency (probability) of the event
- the consequences of the event (often described by the number of potential fatalities).

CAUSE OF DEATH	INDIVIDUAL ANNUAL RISK PER MILLION (risk per year)	SEVERITY AND PERCEPTION
All causes, entire population	10,300 (10^{-2})	Average death rate for whole population. Essentially involuntary.
All types of accident, entire population	250 (2.5×10^{-4})	Voluntary risk. Mainly single fatalities. Substantial efforts aimed at reduction (legislation, design, emergency response etc.)
All forms of road accident	60 (6×10^{-5})	Voluntary risk. Usually single fatalities. Tolerated but general agreement that improvement needed.
Accidents at work, extractive (including oil and gas) and utility supply industries	50 (5×10^{-5})	Voluntary. Mainly single fatalities (multiple fatalities rare but great public concern when they arise). Regarded as tolerable but continuing drive for improvement.
Accidents at work, all manufacturing industry	13 (1.3×10^{-5})	
Accidents at work, all employees	8 (8×10^{-6})	
Rail accident	~1 (1×10^{-6})	Voluntary. Mainly one or a few fatalities. Generally perceived as acceptable but great public concern over multiple fatalities in major accidents when they occur.
Gas incident (fire, explosion, carbon monoxide (CO) poisoning)	0.7 (7×10^{-7})	Voluntary. Usually, one or a few fatalities. Generally perceived as acceptable
Lightning	0.05 (5×10^{-8})	Largely involuntary. Mainly single fatalities. Generally, perceived as negligible risk.

TABLE 1 - TYPICAL FATALITY FREQUENCIES

3.1.2 Maximum tolerable and broadly acceptable risks

3.1.2.1 In order to set a quantified safety integrity target, a target Maximum Tolerable Risk should be determined.

Note: In this context, "individual risk" is the frequency of fatality for a hypothetical person in respect of a specific hazard. This is different from "societal risk" which takes account of multiple fatalities. Society has a greater aversion to multiple fatalities than single ones in that killing 10 people in a single incident is perceived as worse than 10 separate single fatalities.

3.1.2.2 Table 2 shows the limits of tolerability for "individual risk" and is based on a review of R2P2 and HSG87 (See A2.2). The former indicates a maximum

tolerable risk to an employee of 10^{-3} pa for all risks combined. Table 1 shows the actual risk of accidents at work per annum to be well below this. Therefore a target maximum tolerable risk of 10^{-4} pa should be applied for all process related risks combined, leaving a margin to allow for other types of risk.

3.1.2.3 At the lower end of the risk scale, a broadly acceptable risk should be defined.

Note: This is the risk below which one would not, normally, seek further risk reduction. It is approximately 2 orders of magnitude less than the total of random accident risks to which one is exposed in everyday life.

MAXIMUM TOLERABLE INDIVIDUAL RISK (per annum)		
	R2P2	IGEM/SR/15
Employee	10^{-3}	10^{-4}
Public	10^{-4}	10^{-5}
BROADLY ACCEPTABLE RISK (per annum)		
Employee and Public	10^{-6}	10^{-6}

TABLE 2 - TARGET INDIVIDUAL RISKS

3.1.2.4 Multiple fatalities should affect the choice of Maximum Tolerable Individual Risk. The targets in Table 3 reflect an attempt to take account of societal risk concerns in a relatively simple way by adjusting the Individual Maximum Tolerable Risk figures.

MAXIMUM TOLERABLE INDIVIDUAL RISK (per annum)			
	1-2 Fatalities	3-5 fatalities	6 or more fatalities
Employee	10^{-4}	3×10^{-5}	10^{-5}
Public	10^{-5}	3×10^{-6}	10^{-6}
BROADLY ACCEPTABLE RISK (per annum)			
Employee and Public	10^{-6}	3×10^{-7}	10^{-7}

Note: These figures represent an adjustment to the individual maximum risk targets. Thus, for example, the maximum tolerable risk for each individual employee involved in a 10 fatality scenario would be 1×10^{-5} pa.

TABLE 3 - TARGET MULTIPLE FATALITY RISKS

3.1.2.5 The geographical location, that is, site or part of a site, for which a risk is being studied, may be one having multiple potential sources of fatality. The question arises as to how many potential separate hazards an individual (or group) in any one place and time is exposed to. Therefore, in the event of exposure to several hazards at one time, the analyst should seek to allow for this by specifying a more stringent target for each hazard. For example, a study addressing a multi-risk installation might need to take account of an order of magnitude of sources of risk. On the other hand, an assessment of a simple district pressure regulator valve implies a limited number of sources of risk (perhaps only one).

A typical assessment confined to employees on a site might use the recommended 10^{-4} pa maximum tolerable risk (for 1-2 fatalities) but may address 10 sources of risk to an individual in a particular place. Thus, an average of 10^{-5} pa would be used as the Maximum Tolerable Risk across the ten hazards and, therefore, for each of the 10 safety functions involved (See second example at the end of Sub-Section 3.1). By the same token, the Broadly Acceptable Risk would be factored from 10^{-6} pa to 10^{-7} pa.

3.1.2.6 Consideration shall be given to how long an individual is exposed to a risk. Earlier practice has been to factor the maximum tolerable failure rate by the

proportion of time it offers the risk (for example, an enclosure which is only visited 2 hours per week). However, that approach would only be valid if persons (on site) suffered no other risk outside that 2 hours of his/her week. Off site the argument might be different in that persons may well only be at risk for a proportion of the time. Thus the proportion of exposure time is taken (See first example at the end of Sub-Section 3.1) as the working proportion of the week.

3.1.2.7

There is also the question of social aversion to injuries to vulnerable groups (for example, the elderly). In such cases additional measures should be applied.

Table 4 caters for the lesser consequence of injury. As for fatality, targets should be set and an integrity assessment should be carried out. In general, a decrease in one order of magnitude is used for each of the targets.

MAXIMUM TOLERABLE RISK (per annum)	
EMPLOYEE	10^{-3}
PUBLIC	10^{-4}
BROADLY ACCEPTABLE RISK (per annum)	
EMPLOYEE AND PUBLIC	10^{-5}

TABLE 4 - TARGET INDIVIDUAL RISKS FOR INJURY

3.1.2.8

In any event, the final choice of Maximum Tolerable Risk (in any scenario) should form part of the "safety argument" put forward by a system user. Although there are no absolute rules, the foregoing provides an overview of current practice.

Example calculation of risk targeting (1)

A gas release is judged as a potential single on-site fatality and a three fatality off-site scenario. Both on and off site, person(s) are believed to be exposed to that one risk from the installation.

ON SITE

Proportion of time system can offer the risk	75%	40 weeks pa
Probability of ignition	5%	Based on an assessment of the gas cloud and ignition sources
Person at risk	25%	Working week (42 hrs/168 hrs)
Probability of fatality	75%	Judgment

From Table 3, the maximum tolerable risk is 10^{-4} pa. Thus, the maximum tolerable failure rate (leading to the event) is calculated as:

$$10^{-4} \text{ pa} / (0.75 \times 0.05 \times 0.25 \times 0.75) = 1.4 \times 10^{-2} \text{ pa.}$$

OFF SITE

Proportion of time system can offer the risk	75%	40 weeks pa
Probability of ignition	5%	Based on an assessment of the gas cloud and ignition sources
Person(s) at risk	33%	Commercial premises adjoin
Probability of 3 fatalities	10%	Offices well protected

From Table 3 the maximum tolerable risk is 3×10^{-6} pa. Thus the maximum tolerable failure rate (leading to the event) is calculated as:

$$3 \times 10^{-6} \text{ pa} / (0.75 \times 0.05 \times 0.33 \times 0.1) = 2.4 \times 10^{-3} \text{ pa.}$$

Thus, 2.4×10^{-3} pa, being the more stringent of the two, is taken as the maximum tolerable failure rate target for the equipment.

Example calculation of risk targeting (2)

A particular gas release is judged as not being an on-site risk due to its being unattended. It is judged as potentially leading to three fatalities off site during 20 hours per week and to 10 fatalities during 5 hours per week. Persons are believed to be exposed to approximately 3 risks (including this one) from the installation.

OFF SITE (3 fatalities)

Proportion of time system can offer the risk	100%	Continuous use
Probability of ignition	25%	Based on an assessment of the gas cloud and ignition sources
3 Persons at risk	12%	20 hrs per week
Probability of 3 fatalities	10%	See assessment document "x"

From Table 3, the maximum tolerable risk is 3×10^{-6} pa. However, there being 3 simultaneous risks, the target for each becomes $3 \times 10^{-6} \text{ pa} / 3 = 1 \times 10^{-6}$ pa. Thus the maximum tolerable failure rate (pertaining to the gas release event) is calculated as:

$$1 \times 10^{-6} \text{ pa} / (0.25 \times 0.12 \times 0.1) = 3.3 \times 10^{-4} \text{ pa}.$$

OFF SITE (10 fatalities)

Proportion of time system can offer the risk	100%	Continuous use
Probability of ignition	25%	Based on an assessment of the gas cloud and ignition sources
10 Persons at risk	3%	5 hrs per week
Probability of 10 fatalities	3%	See assessment document "x"

From Table 3, the maximum tolerable risk is 10^{-6} pa. However, there being 3 simultaneous risks, the target becomes $10^{-6} \text{ pa} / 3 = 3.3 \times 10^{-7}$ pa for each. Thus, the maximum tolerable failure rate (pertaining to the gas release event) is calculated as:

$$3.3 \times 10^{-7} \text{ pa} / (0.25 \times 0.03 \times 0.03) = 1.5 \times 10^{-3} \text{ pa}$$

Thus, 3.3×10^{-4} pa, being the more stringent of the two, is taken as the maximum tolerable failure rate target for the equipment.

Note: The above failure rate targets do not in themselves infer a Safety Integrity Level (SIL) target and are not to be converted until the number of levels of protection has been defined (see Sub-Section 3.2)

►3.1.2.9 Societal risk

There is the separate issue of societal risk. An individual risk target reflects the exposure of one individual to multiple events, whereas societal risk reflects the exposure of multiple individuals to the same event. Instead of addressing the risk to an individual, the concern is with the tolerability of multiple fatality events (irrespective of the individual identities of the victims).

The number of potential fatalities should be assessed. This number may vary at different times of the day. The following example shows how a weighted average can be arrived at when overlapping groups of people are at risk over different periods of time:

For 4 hours per day, 60 persons are at risk
For 17 hours per week 10 persons are at risk
For 24 hours per day, 1 person is at risk.

Therefore, the weighted average of exposure is:

$$4/24 \times 60 + 17/168 \times 10 + 24/24 \times 1 = 12 \text{ fatalities.}$$

The next step is to address the Maximum Tolerable Risk. Unlike the Individual Risk criteria (see Table 3), which address the probability as applying to an Individual, the criterion becomes the frequency of a fatal event (irrespective of the individuals concerned). Whereas individual risk addresses a specific person(s), societal risk

addresses the risk to a potentially changing group irrespective of their identity (for example the continuously changing occupants of a rail tunnel).

So, the criteria are expressed as frequencies for the event rather than risk to an individual, (see Figure 1). Therefore, for the 12 fatality scenario above a maximum tolerable failure rate for the event of 10^{-3} pa is suggested.

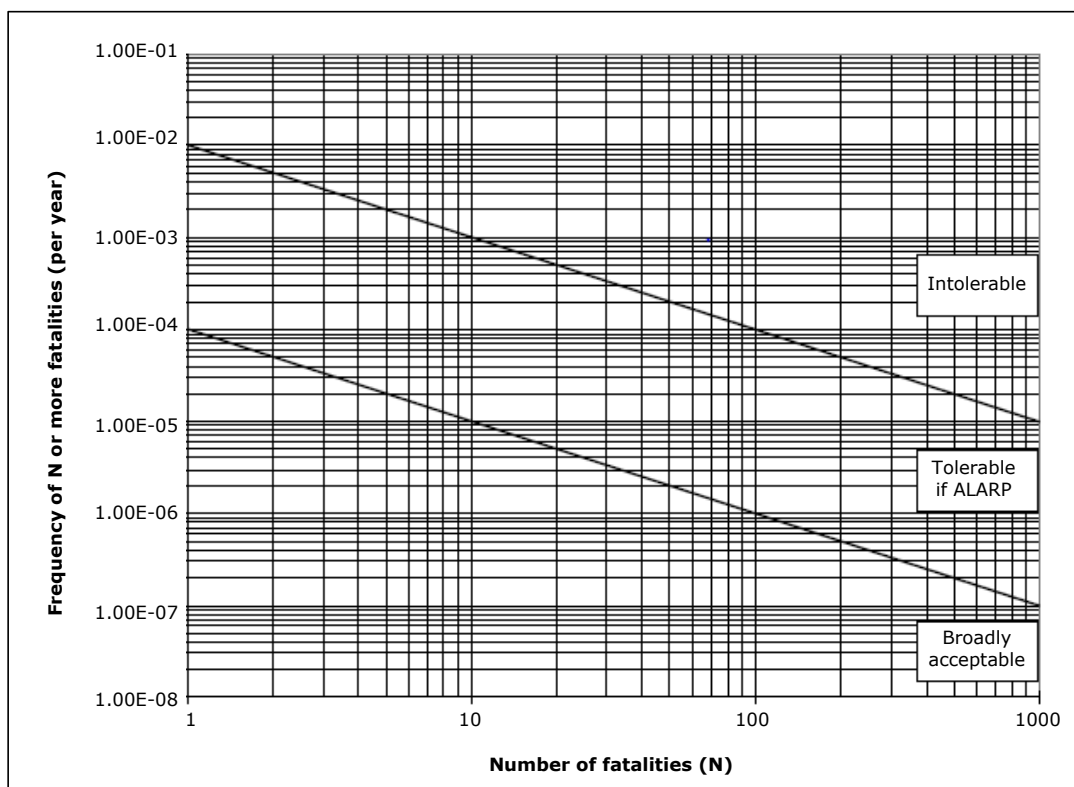


Figure 1 - criteria per number of fatalities

Note 1: This figure has no specific provenance but can be related to HSE document R2P2 by virtue of a 50 fatality target of 1 in 5,000 years (2×10^{-4}) maximum tolerable risk therein.

Note 2: Although expressed in log by log format, it is a relationship which can be summarised (where N is the number of potential fatalities) as:
Maximum Tolerable Frequency (societal) = 10^{-2} pa/ N^{-1}
Broadly Acceptable Frequency (societal) = 10^{-4} pa/ N^{-1}

Note 3: The propagation to fatality of an event is calculated as for Involuntary Risk but ignoring the element which addresses what proportion of the time anyone is at risk, it having been taken account of already in the Societal Risk concept.

3.1.2.10 Environmental and Production loss

Safety-integrity is normally associated with failures that lead to death or injury. BS EN ISO 61508 should be applied to failures leading to environmental damage and loss of production. Reference A2.5 offers some suggested criteria (see Table 5).

TARGET MAX TOLERABLE FREQUENCY PA	CRITERIA ENVIRONMENT	CRITERIA COMMERCIAL
10^{-7}	Catastrophic Incident, 5 years effect on water, supply, food chain, or housing	>£500M
10^{-6}	Massive/significant incident (e.g. 1,000 fish/animals) 1-5 year effect on water, supply, food chain, or housing. Possibly International	<£500M
10^{-5}	Major Offsite Incident (e.g. Pollution of ground water, impact on fauna/flora). c1 year effect on water, supply, food chain, or housing	<£50M
10^{-4}	Major Offside Incident (e.g. Reservoir clean up, river remedial action) c1 month effect on water, supply, food chain, or housing	<£5M
10^{-3}	Significant Incident with minor contamination, no effect on water course	<£500,000
10^{-2}	Non-serious 'nuisance'/ odour Incident	<£50,000
10^{-1}	Trivial on-site incident/release	<£5,000

TABLE 5 - ENVIRONMENTAL RISK TARGETS◀

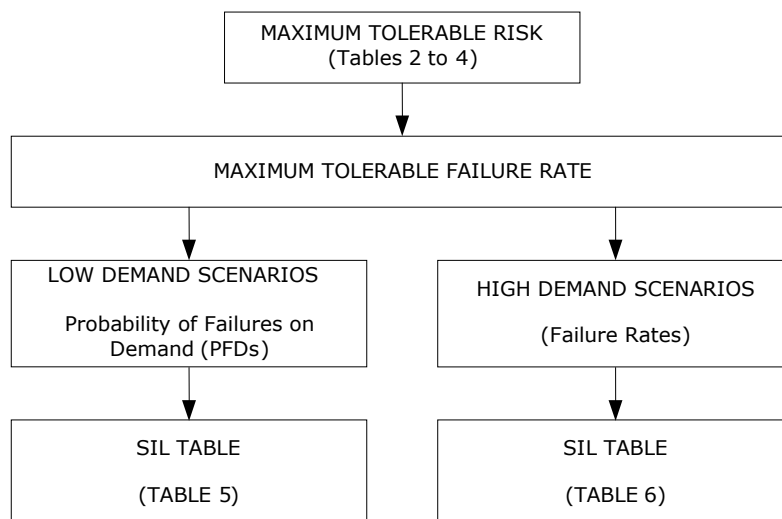
3.2 Safety integrity levels (sils)

3.2.1 Introduction

The term SIL refers to one of four specific bands of rigour which define life-cycle procedures and techniques aimed at minimising systematic failures.

If the assessment were to involve only traditional reliability prediction, wherein the predicted hardware reliability is compared with a target, there would be no need for the concept of discrete SILs. However, because the rigour of adherence to design/quality assurance activities cannot be quantified, a number of discrete levels of "rigour", which cover the credible range of integrity, are described. The practice is to divide the spectrum of integrity targets into four levels (see Tables 5 and 6).

There are two types of safety-integrity target and these are defined in Sub-Sections 3.2.2 and 3.2.3 and Tables 5 and 6. Figure 2 indicates how to select either Table 5 or Table 6.

**FIGURE 2 - SELECTION OF HIGH OR LOW DEMAND SIL****3.2.2****Low demand**

This type of target (and its associated SIL) applies to “add-on” levels of protection for which the probability of failure on demand is the target. Thus, it is a dimensionless quantity (probability) being the ratio of the predicted failure rate to a target failure rate. It thus provides a measure of risk reduction. Demands on the risk reduction will tend to be infrequent because they arise from the failure of the equipment for which the protection is provided i.e. the protection is only called upon when the equipment under control fails. The SILs are defined by BS EN 61508 as shown in Table 6.

An everyday example of a low demand safety function is the motor car air bag. Gas industry examples include fire and gas detection equipment and shutdown functions protecting against high/low pressure or flow etc.

SAFETY INTEGRITY LEVELS. LOW DEMAND RATE	
SAFETY INTEGRITY LEVEL (SIL)	PROBABILITY OF FAILURE TO PERFORM SAFETY FUNCTION ON DEMAND
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Note: Avoiding a SIL 4 is preferable because achieving it requires very significant levels of design effort and analysis. Additional levels of risk reduction would also need to be introduced such that lower SIL targets are required for each element of the system.

TABLE 6 - LOW DEMAND RATE SILs**Example of establishing a low demand rate SIL target**

Assume that the hazard is the overpressure of pipework due to a pressure control system failing “open”.

Assume a Maximum Tolerable Risk target of 10^{-5} pa (public fatality assuming exposure to only one hazard, Table 3).

Assume that 1 in 10 overpressure incidents have been assessed as leading to a fatality.

Assume that it has been assessed that the control system will fail “open” and overpressure the pipework at the rate of 0.05 pa.

Since 0.05 pa would not meet the above maximum tolerable risk, it is proposed to implement an add-on safety system involving instrumentation to measure pressure and to initiate shut-down measures.

The PFD target is obtained as follows:

Maximum Tolerable Failure rate leading to fatality is 10^{-5} pa / $10^{-1} = 10^{-4}$ pa.

However, the actual process failure rate is 0.05 pa = 5×10^{-2} pa.

Thus, to meet the safety criteria, the protection system has a target maximum probability of failure on demand (PFD) no worse than:

10^{-4} pa / 5×10^{-2} pa = 2×10^{-3} .

The target is dimensionless and is, thus, a risk reduction factor expressed as a PFD.

Therefore, the requirement is SIL 2 as described in Table 11.

The 0.05 pa failure rate of the equipment under control may have been derived from empirical failure data or from a predictive assessment which would require valve failure rates, proof-test intervals and repair times to be assessed.

3.2.3

High demand

A quite different type of scenario, which does not involve risk reduction by a protection system (as in the above example) applies directly to a hazard as opposed to a dormant failure pending a demand on its function. This type of target (and its associated SIL) applies to any equipment where the safety integrity target needs to be met without the benefit of “add-on” levels of protection. In other words, the Maximum Tolerable Failure rate applies to the whole system which is treated as a “black box”. The SILs are defined by BS EN 61508 as shown in Table 7.

An everyday example of a high demand safety function is motor car braking. Gas industry examples include a pre-payment gas meter where interruption and then spurious reinstatement of supply leads to un-ignited gas.

SAFETY INTEGRITY LEVELS. HIGH DEMAND RATE	
SAFETY INTEGRITY LEVEL (SIL)	DANGEROUS FAILURES PER ANNUM
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Note 1: BS EN 61508 states the same targets expressed in units of per hour.

Note 2: Avoiding a SIL 4 is preferable because achieving it requires very significant levels of design effort and analysis. Additional levels of risk reduction would also need to be introduced such that lower SIL targets are required for each element of the system.

TABLE 7 - HIGH DEMAND RATE SILs

Example of setting of a high demand rate SIL target

Assume that the hazard is a pre-payment gas meter (clause 11.6.2) where interruption by a solenoid valve, and the spurious reinstatement of supply, leads to un-ignited gas in the premises.

Assume a Maximum Tolerable Risk target of 10^{-5} pa (public fatality assuming exposure to only one hazard, Table 3).

Assume, for example, that 1 in 2000 (5×10^{-4}) of such incidents have been assessed as leading to a fatality.

The failure rate target is obtained as follows:

Maximum Tolerable Failure rate leading to fatality is:

10^{-5} pa / $5 \times 10^{-4} = 2 \times 10^{-2}$ pa.

Thus, to meet the safety criteria, the equipment has a target maximum dangerous failure rate of 2×10^{-2} pa.

The target has dimensions of "rate". Therefore, Table 9 is indicated from which a SIL 1 target is inferred.

3.2.4 Interpretation of "not-safety-related"

3.2.4.1 BS EN 61508 allows a control system to be classified as "not-safety-related" despite its contribution to the plant operation. Control systems in this Standard should be thought of as an integrity target of less than SIL 1.

3.2.4.2 For less than SIL 1 targets the term SIL 0 (although not used in the Standard) is in common use and is considered appropriate.

In order to demonstrate this, the calculated target SIL should be less onerous than SIL 1, and it should be shown that:

- failure rate assumptions are supported by field data
- all foreseeable dangerous failures have been addressed in the assessment
- the equipment does not have a rating of SIL 1 or higher for some other function
- the control system is separate from, and independent of, any safety-related risk reduction system.

Note: Nevertheless, although such equipment has been designated "not-safety-related", the quality assurance requirements of SIL 1 are recommended as good engineering practice.

3.2.5 Approaches to integrity targeting

Consideration shall be given to using one of the following approaches:

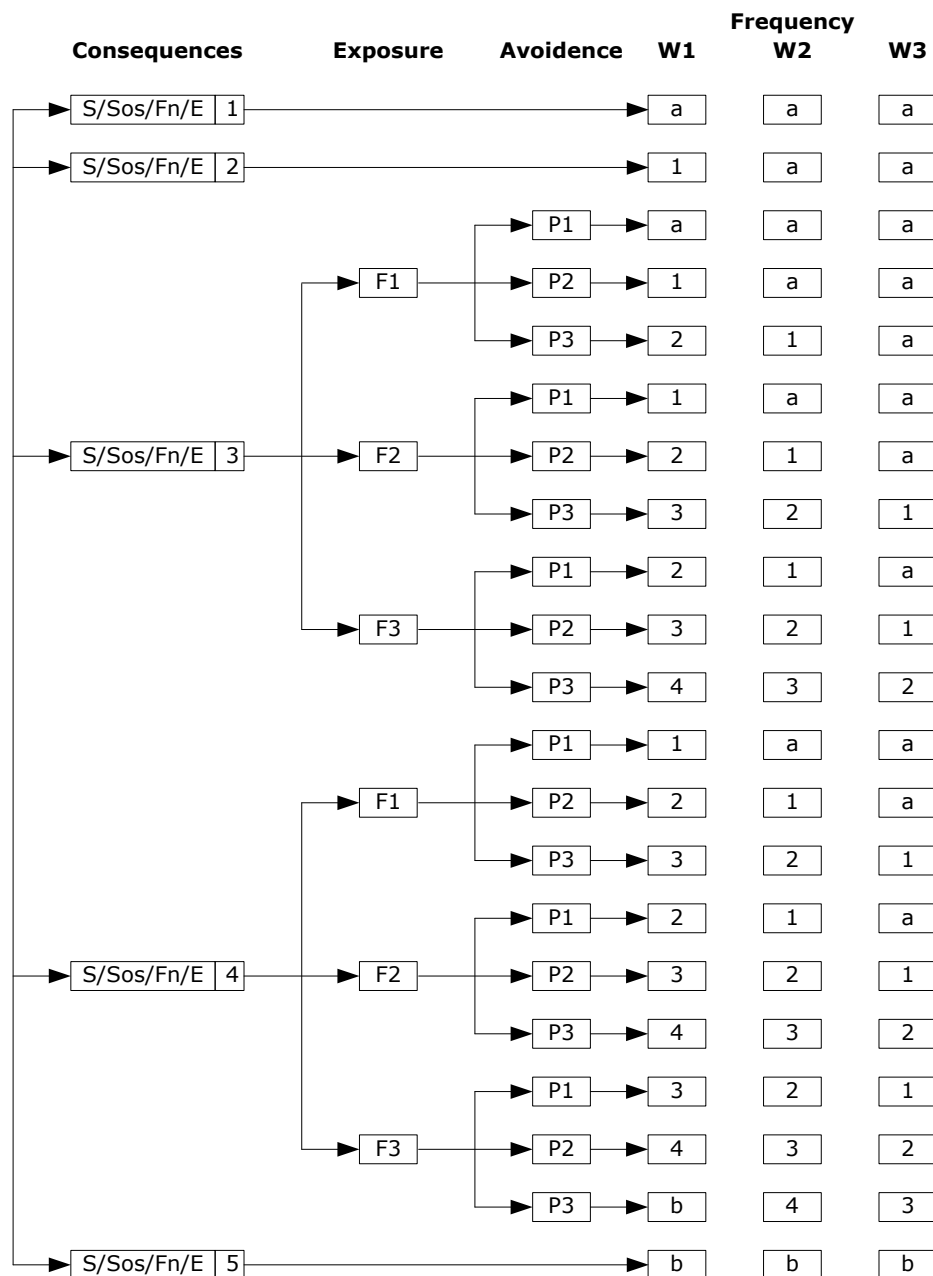
(a) Risk graph approach

If resources permit, the methods described in Sub-Section 3.2.6 should be used. Thus, a Maximum Tolerable Risk should be established having regard to Table 3. However, a less precise "risk graph" algorithmic approach is acknowledged in BS EN 61508. This should only be used for general guidance in view of the wide risk ranges of the parameters in the tables.

A typical risk graph is shown in Figure 3.

Successive cascading decisions involving only "order of magnitude" choices, carry the potential for gross inaccuracy.

The risk graph does not readily admit multiple levels of protection. This is dealt with in Sub-Section 3.2.6. Furthermore, due to the nature of the rule based algorithm, which culminates in the request for a demand rate, the risk graph is only applicable to low demand SIL targets. It should only be used as a screening tool when addressing large numbers of safety functions. Then, any target of SIL 2 or greater should be subject to the quantified risk approach.



Note: In the above figure, the key for items consequences, exposure and avoidance are defined in the specific guidance document from which it comes. Each is specified by specific quantified bands. The frequency of demand on the protection (W1-W3) is also quantified.

FIGURE 3 - TYPICAL RISK GRAPH

(b) Levels of Protection Analysis (LOPA)

This involves a more structured approach in which propagations to fatality and the effectiveness of protection levels are assessed, sometimes to the nearest order of magnitude.

The approach is very similar to the Quantified Risk Assessment (QRA) methodology but may not fully describe multiple layers of protection or human factors.

(c) Quantified Risk Assessment (QRA)

This is described in Sub-Section 3.2.6.

3.2.6 Template outline of integrity targeting

3.2.6.1 This involves factoring the maximum tolerable risk according to totally external levels of protection and factors which limit the propagation to fatality of the event. Table 8 gives examples of the elements which might be considered. These are not necessarily limited to the items described below and the analyst(s) should be open ended in assessing the factors involved.

FACTOR INVOLVING THE PROPAGATION OF THE INCIDENT OR DESCRIBING AN INDEPENDENT LEVEL OF PROTECTION	PROBABILITY (EXAMPLE)	THIS COLUMN IS USED TO RECORD ARGUMENTS, JUSTIFICATIONS REFERENCES ETC TO SUPPORT THE PROBABILITY USED
The profile of time at risk	60%	Quantify whether can arise all or some of the time. This may be <100% as for example if: - flow, temp, pressure etc profiles are only sufficient at specific times, for the risk to apply - the process is only in use for specific periods.
Unavailability of separate mitigation (i.e. another level of protection)	20%	Mitigation outside the scope of this study and not included in the subsequent modelling which assesses if the system meets the risk target. Examples are: - a down stream temp, pressure etc measurement leading to manual intervention - a physical item of protection (for example, vessel; bund) not included in the study.
Probability of the scenario developing	70%	Examples are, quantify whether: - the vessel/line will succumb to the over-temp, over pressure etc. - the release has an impact on the passing vehicle.
Person(s) exposed (i.e. being at risk)	25%	Proportion of time during which some person or persons are close enough to be at risk should the event propagate. Since a person may be exposed to a range of risks during the working week, this factor should not be erroneously reduced to the proportion of time exposed to the risk in question. If that were repeated across the spectrum of risks then each would be assigned an artificially optimistic target. The working week is approximately 25% of the time and thus that is the factor which would be anticipated for an on-site risk. In the same way, an off-site risk may only apply to a given individual for a short time.
Probability of subsequent ignition	90%	Quantify whether the released material ignites/explodes
Fatality ensues	25%	The likelihood that the event, having developed, actually leads to fatality

TABLE 8 - ELEMENTS LEADING TO A MAXIMUM TOLERABLE FAILURE RATE

The maximum tolerable failure rate is then targeted by taking the maximum tolerable risk and factoring it according to the items assessed. For example, taking the probabilities given in Table 8 (assuming a 10^{-5} pa involuntary risk):

Maximum Tolerable Failure Rate =

$$10^{-5} \text{ pa} / (0.6 \times 0.2 \times 0.7 \times 0.25 \times 0.9 \times 0.25) = 2.1 \times 10^{-3} \text{ pa}$$

- 3.2.6.2 The overall system then should be described using AND/OR logic which may typically be expressed as a Fault Tree model as shown in Figure 4.

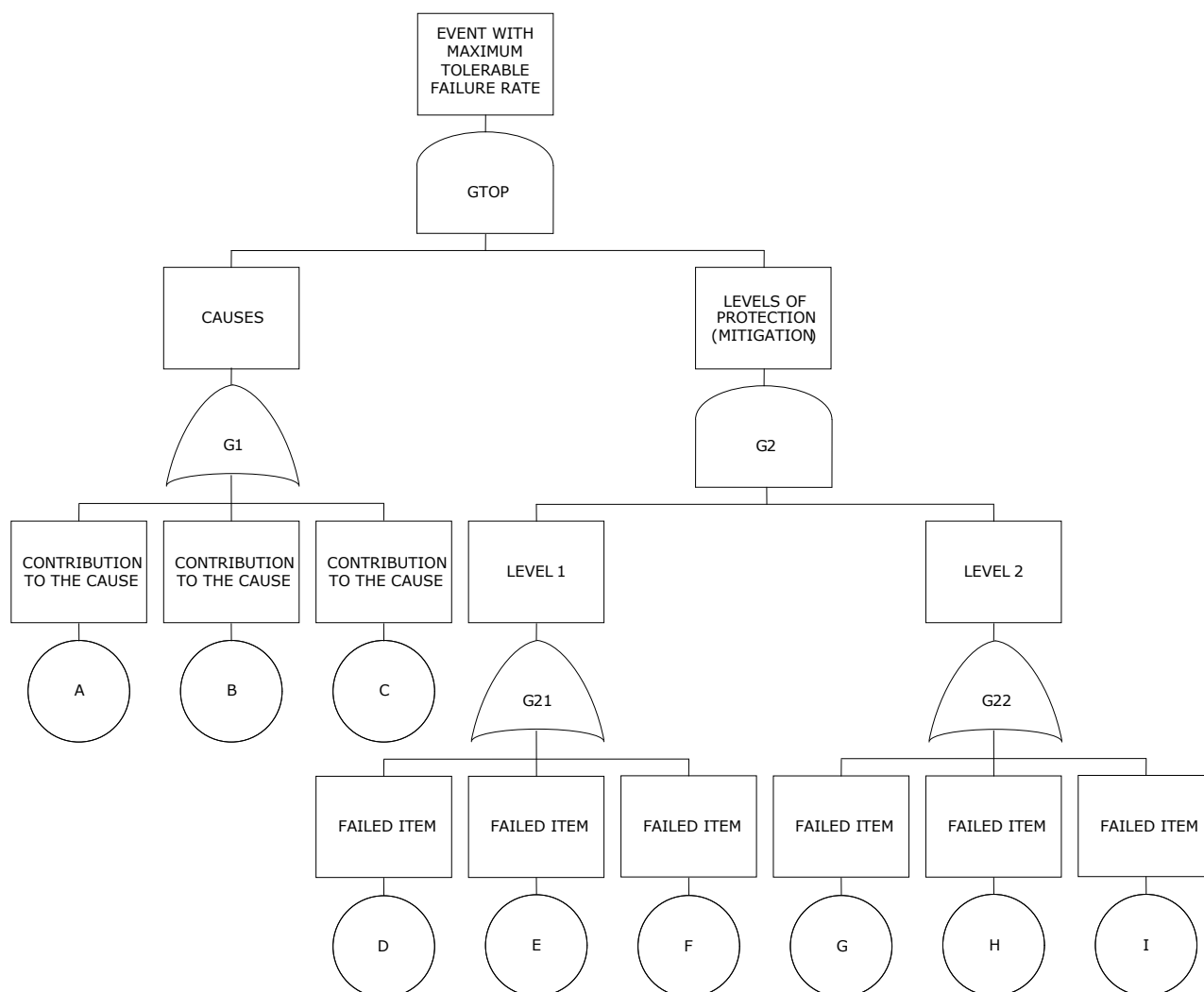


FIGURE 4 - FAULT TREE MODEL

In the Fault Tree (see Figure 4), Gate G1 would be described using the rate parameter. Dividing the target Maximum Tolerable Failure Rate associated with GTOP by the rate for Gate G1 provides a target PFD for the protection.

Independent levels of protection are then modelled as shown by gates G21 and G22 in Figure 4. It is important to remember that the use of an AND gate (for example, Gate G2) implies that the events below that gate are totally independent of each other.

A greater number of levels of protection (i.e. Gates below G2) leads to less onerous PFDs being allocated for each and, thus, lower integrity requirements will apply to each.

A maximum tolerable failure rate of 5.3×10^{-4} pa was used as an example. Assume that the frequency of causes (i.e. Gate G1) is 10^{-1} pa. Thus the target PFD associated with Gate G2 becomes:

$$5.3 \times 10^{-4} \text{ pa} / 10^{-1} \text{ pa} = 5.3 \times 10^{-3}$$

Note: The result is dimensionally correct, as a rate/rate becomes a PFD.

A common mistake is to describe the scenario as “a SIL 2 safety system”. This would only be the case if the mitigation was a single element and not decomposed into separate independent layers.

In Figure 4 there are two levels of protection for which the product of the two PFDs needs to be less than 5.3×10^{-3} .

Depending on the equipment in question this could involve a number of possibilities. Examples are shown in Table 9.

	Level 1 PFD	Level 1 SIL	Level 2 PFD	Level 2 SIL
Option A	2×10^{-1}	< 1	2.65×10^{-2}	1
Option B	7.3×10^{-2}	1	7.3×10^{-2}	1
Option C	7×10^{-1}	< 1	7.57×10^{-3}	2

TABLE 9 - POSSIBLE SIL OUTCOMES

As can be seen, the safety integrity level is inferred only when the PFD associated with each level of protection has been assigned/assessed. Each of the options is equally “correct” in providing a safety argument. However, the pair of SIL 1 levels is likely to be favoured.

3.2.7 **SIL 3 targets**

3.2.7.1 A SIL 4 target should be avoided and additional levels of risk reduction, leading to lower SIL targets for each level of mitigation, should be engineered.

3.2.7.2 A SIL 3 target may become appropriate. There is a significant difference between SIL 2 and SIL 3, in terms of the rigour of design activities (in contrast to that between SILs 1 and 2). In such cases the scenario shall be carefully considered.

Key aspects of SIL 3 which may lead to significant additional cost are:

- re-validation of the entire system following software modifications
- the need to provide voted instrumentation (where instruments are not available to meet the stringent diagnostic constraints given in Sub-Section 5.1)
- significant additional independent validation
- limited choice of vendors offering instruments which demonstrate compliance
- additional simulation during testing.

3.2.8 **Hierarchy of measures**

There is a hierarchy of measures which should be addressed when assessing a particular risk. This implies that some measures should be considered before others as shown chronologically in the following list:

- eliminate the hazard
- reduce the consequences of the hazard
- reduce the frequency of the hazard
- provide levels of protection to mitigate the hazard.

SECTION 4 : RANDOM HARDWARE FAILURES

4.1 HARDWARE FAILURES

So-called random hardware failures refer to those hardware failures which are attributable to specific component failures and to which failure rate data can be ascribed. The concept involves the assumption of repeatability of failure rate data, hence systems are assessed by combining the failure rates of the component parts. Generally, they are the constant failure rate (middle of the bathtub curve) failures which, traditionally, describe hardware reliability

Traditional reliability prediction techniques, for example fault tree analysis, block diagram modelling and failure mode and effect analysis, should be used to assess whether a proposed safety-related system meets the SIL target. They are described in "Reliability, Maintainability and Risk" (see A2.5) to which reference should be made if appropriate, and are not dealt with in detail in this Standard. However, a number of essential issues are dealt with briefly in the following Sub-Sections.

4.2 FAILURE RATE DATA

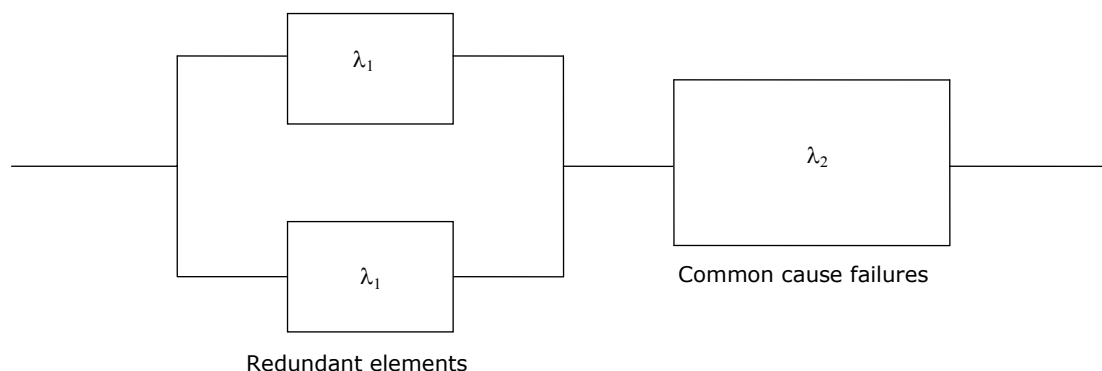
4.2.1 There exist numerous sources of failure rate data. Due to the wide variability of failure rates quoted it is difficult to apply conformity of choice in the assessment process. Specialist advice shall be sought to obtain this data.

4.2.2 Care shall be exercised in the use of failure rate data provided by equipment manufacturers rather than by users. There are numerous reasons why this can be highly optimistic.

4.3 COMMON CAUSE FAILURE (CCF)

Redundancy (for example, voting of instrumentation, duplication of processes) increases the reliability of a scenario by requiring coincident failures to occur. The mathematics associated with random coincident failures is extremely optimistic. Such redundancy is downgraded by the fact that a proportion of failures will involve some feature common to both items and thus defeat the redundancy.

The usual approach to modelling this is the BETA (β) model, which assumes that a fixed proportion (β) of the failures are due to a common cause. The estimation of β is determined by system-type based on very limited historical data. This is illustrated in the reliability block diagram (Figure 5).



Note: $\lambda_2 = \beta \lambda_1$ where (λ_1) is the failure rate of a single redundant unit and (λ_2) is a notional element modelling the CCF rate.

FIGURE 5 - β MODEL