Activities at Specific Stages of the Lifecycle		IEC 61511-1 sub-clauses
6.7.5.12	Results of proof testing should be clearly recorded. If a test identifies faults, the cause and any other relevant data should be recorded. The down time for all repairs should be recorded.	16.3.3 **
6.7.6 Review of Operational Performance		
6.7.6.1	Discrepancies between expected and observed SIS behaviour should be reviewed and appropriate corrective action taken. For offshore applications, this is a specific requirement for "Safety-Critical Elements" under the PFEER regulations.	16.2.6
6.7.6.2	Results of proof tests should be periodically reviewed to ensure that integrity specifications (SIL or PFD) are being satisfied. Where improvement is necessary, test frequencies should be increased or equipment or configuration changes made to reduce undetected dangerous failure rate. For a SIF, the PFD being achieved (the fractional dead time) is half the number of proof test failures divided by the number of proof tests, assuming any faults are repaired in a relatively short time. See Annex F.	16.2.6
6.7.6.3	Down times (from fault occurrence to effected repair) should be reviewed for each SIF, to ensure that design assumptions remain valid or to take corrective action.	**
6.7.6.4	Functional and integrity specifications of SIFs should be reviewed and revalidated periodically so that their ongoing suitability, including where there may be creeping changes in process hazards, can be examined. End users should set an appropriate interval dependent on the nature of their processes.	5.2.5.3 5.2.6.2
6.8 Modification and Decommissioning		
6.8.1 Introduction		
6.8.1.1	This sub-clause addresses Phases 7 and 8 of the SIS lifecycle, as defined in IEC 61511. See Figure 1.	-
6.8.2 Modification		
6.8.2.1	Any proposed modification should be addressed from the earliest relevant phase of the safety lifecycle dependent on the scope and complexity of the proposed change.	17.2.3

Activities at Specific Stages of the Lifecycle		IEC 61511-1 sub-clauses
6.8.2.2	Modifications to existing facilities should consider not only the direct scope of the change, but also the full extent to which existing facilities may be impacted. For example, addition of new hardware to an existing SIF may affect the PFD of the SIF and more frequent testing or changes to existing systems may be required to maintain the SIL or PFD of the SIF.	17.2.3
6.8.2.3	Where an existing plant would be impacted by the modification, a detailed analysis should be carried out for all interfaces. If existing plant including SIS information is inadequate, the end user should specify the extent of re-evaluation of existing systems.	17.2.3
6.8.2.4	Proposed modifications should be reviewed and authorised in accordance with a formal Management of Change procedure that requires approval from all relevant disciplines.	17.2.1
6.8.2.5	Operations and maintenance personnel should be advised of changes and training should be provided as necessary.	16.2.4
6.8.3 Decommissioning		
6.8.3.1	Decommissioning of facilities involving SIS should be managed as a modification. See Section 6.8.2 above.	18.2
6.8.3.2	Particular attention should be paid during the planning and execution of decommissioning to the sequencing of activities, so that protection against process hazards is always provided.	18.2 **
6.8.3.3	Where decommissioning is for part of the plant and parts of the logic in the logic solver, the retained functions in the logic solver should be proven.	12.6 16.3.1.6

This page is intentionally blank.

Annex A SIL Determination Methods and Calibration

A.1 Introduction

This Annex describes two methods commonly used for SIL determination in the UK process industries, risk graphs and layer of protection analysis (LOPA). Both of these methods are listed and described in more detail in IEC 61511-3. This Annex also describes how these methods should be calibrated, which means setting residual risk levels that are tolerable to the end user. None of the methods listed in IEC 61511-3 are calibrated.

Note that the techniques mentioned assume low demand mode of operation and are not appropriate for high demand or continuous mode operation. They also assume that causes of demand and the SIF are independent. Fully quantitative techniques should be used where there are common causes between them.

A.2 Risk Graphs

The risk graph in Figure A.1 and associated guidance in Table A.1 are taken from IEC 61511-3 Annex D. The demand rate (*W*) definitions include a factor *D* that the end user should assign a value to. Comment 6 in Table A.1 states "*D* is a calibration factor, the value of which should be determined so that the risk graph results in a level of residual risk which is tolerable taking into consideration other risks to exposed persons and corporate criteria."

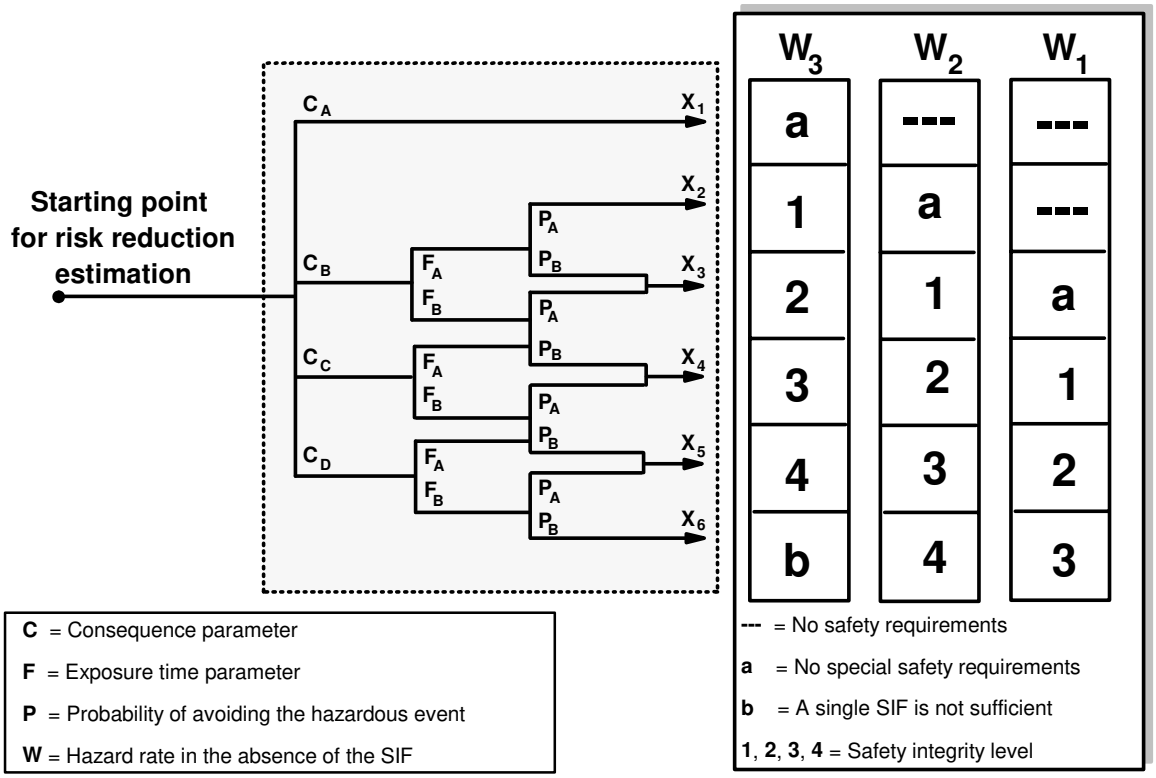

Figure A.1 Risk graph

The residual risk after a SIF of SIL given by the risk graph is a range of values. The maximum risk of fatality is given by taking the "worst" value for each of the four parameters considered and the "worst" end of the associated SIL range. Because this risk graph is linear, the residual risk is the same for any path through it for all cases where the consequence parameter selected is C_B or higher.

Taking the one fatality case, which is at the "worst" end of C_C, the "worst" occupancy, no possibility of avoiding the hazardous event and a demand rate of D per year requires a SIL 3 SIF. The "worst" end of the SIL 3 range has a PFD of 1×10^{-3}.

The highest residual risk of fatality is therefore $D \times 10^{-3}$ per year. The lowest residual risk of fatality is about five orders of magnitude lower than this. This figure is the risk to people from a single hazard where a SIF plays a mitigating role.

The appropriate value of the D factor should be decided by the end user, based on the number of hazards with the potential for fatal injuries that personnel might be exposed to, and the organisation's corporate risk criteria. A further consideration is whether the chosen value of D can be shown to provide an ALARP (as low as reasonably practicable) solution given estimated costs to increase the SIL further and the associated safety benefit expressed in financial terms.

Table A.1 Risk graph parameter explanations

Risk parameter		Classification	Comments
Consequence (*C*) Number of fatalities (statistical). This can be calculated by determining the numbers of people present when the area exposed to the hazard is occupied and multiplying by the vulnerability to the identified hazard. The vulnerability is determined by the nature of the hazard being protected against. The following factors can be used, but a more suitable number between 0 and 1 may be chosen. *V* = 0.01 Small release of flammable or toxic material. *V* = 0.1 Large release of flammable or toxic material. *V* = 0.5 As above, but also a high probability of catching fire or highly toxic material. *V* = 1 Rupture or explosion.	C_A C_B C_C C_D	Minor injury (not reportable under RIDDOR and fully recoverable, e.g. First Aid injury) Range 0.01 to 0.1 statistical fatalities Range >0.1 to 1.0 Range >1.0 to 3.0 with not more than 10 people exposed	1. The classification system has been developed to deal with injury and death to people. 2. For the interpretation of C_A, C_B, C_C and C_D, the consequences of the accident and normal healing should be taken into account. 3. For over 3 statistical fatalities, use more quantitative risk assessment techniques.
Occupancy (*F*) This is calculated by determining the proportional length of time that any individual is exposed to hazards where SIFs are used as mitigation during a normal working period. *Note 1: If the time in the hazardous area is different depending on the shift being operated, the maximum should be selected.* *Note 2: It is only appropriate to use F_A where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up or during the investigation of abnormalities.*	F_A F_B	Rare to more frequent exposure to the hazards. Occupancy less than 0.1 Frequent to permanent exposure to the hazards	3. See Comment 1 above. 4. Note that the definition of occupancy differs from that in IEC 61511-3 Annex D in taking account of all the SIF-related hazards that individuals are exposed to in a normal working period. The classification definitions have also been modified accordingly.
Possibility of avoiding the hazardous event (*P*) if the protection system fails to operate.	P_A P_B	Adopted if all conditions in column 4 are satisfied Adopted if *any* of the conditions are not met	5. P_A should only be selected if all the following are true: • facilities are provided to alert the operator that the SIS has failed; • independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area; • the time between the operator being alerted and a hazardous event occurring exceeds one hour or is definitely sufficient for the necessary actions.
Demand rate (*W*). The number of times per year that the hazardous event would occur in absence of SIF under consideration. To determine the demand rate, it is necessary to consider all sources of failure that can lead to one hazardous event. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance that can be claimed if the control system is not to be designed and maintained according to IEC 61511 is limited to below the performance ranges associated with SIL 1.	W_1 W_2 W_3	Demand rate less than 0.1*D* per year Demand rate between 0.1*D* and <*D* per year Demand rate between *D* and <10*D* per year For demand rates 10*D* or higher per year higher integrity is needed	6. The purpose of the *W* factor is to estimate the frequency of the hazard taking place without the addition of the SIS. If the demand rate is very high, the SIL has to be determined by another method or the risk graph recalibrated. It should be noted that risk graph methods might not be the best approach in the case of applications operating in continuous mode. See IEC 61511-1 3.2.43.2. 7. *D* is a calibration factor, the value of which should be determined so that the risk graph results in a level of residual risk that is tolerable, taking into consideration other risks to exposed persons and corporate criteria.

In 'Reducing Risks, Protecting People' published in 2001[7], the Health and Safety Executive suggests that "an individual risk of death of one in a million per annum for both workers and the public corresponds to a very low level of risk and should be used as a guideline for the boundary between the broadly acceptable and tolerable regions" (paragraph 130).

Converting this guideline figure for individual risk to the equivalent risk to any person from a single hazard, which is the role of a SIF, depends on how people are deployed in relation to the hazards and the number of such hazards involving SIFs that any individual person is exposed to.

Also in 'Reducing Risks, Protecting People' (Appendix 3, paragraph 13), the HSE suggest a figure of £2,000,000 as an appropriate value for preventing a fatality. A typical cost on a whole life basis of increasing the SIL of a SIF by one level is £30,000. The following assumptions are made:

- safety benefits are obtained over a 15 year period;
- the value of future safety benefits are not discounted;
- the value of preventing a fatality is not inflated.

The safety benefit in financial terms from increasing a SIL by one level, and thereby reducing the risk of $D \times 10^{-3}$ per year by 90%, is:

- safety benefit = £2,000,000 $\times$ 0.9 $\times$ D $\times$ 0.001 / year = £1,800 $\times$ D / year;
- the cost of increasing SIL by one is £30,000 / 15 per year = £2,000 / year.

This simple cost–benefit analysis suggests with the assumed values, it is just not worth spending more to increase safety integrity level when D = 1. However, this includes no gross disproportion element required in the demonstration of ALARP. Inclusion of gross disproportion can suggest a maximum value for D of 0.1.

If D of 0.1 is chosen, this implies maximum risk of 1×10^{-4} in a year from a single hazard where a SIF plays a role in prevention. It also means an upper limit of one demand per year. A higher demand rate than one per year is, in any event, bordering on operating in the high demand or continuous mode, because testing would need to be significantly more frequent than annually to be able to use PFD definitions of SILs.

This analysis does not include consideration of special factors, e.g. societal risk, which may apply when large numbers of people are exposed. Specialist advice should be sought in this case.

For environmental and commercial risks using the risk graph, the F parameter is not used, which is equivalent to selecting F_B in the safety risk graph.

Example equivalence between safety, environment and economic consequences is shown in Table A.2. End users should determine if this equivalence is appropriate for their circumstances. Commercial consequences include the cost of damage repair, cost of lost or deferred production, and any penalties for non-delivery of product. With a value of the calibration factor D of 0.1 using these commercial consequence definitions in the risk graph in Figure A.1, a maximum annual risk for each hazard is implied using an SIF of £1,000 per year in most cases.

Again, the end user should decide if this is appropriate or if an alternative calibration is more appropriate.

Note that this Guide uses the term SIL as in IEC 61511 where it principally applies to safety risks. Users may choose to use the term EIL to describe the integrity performance required to manage environmental risks and CIL for

commercial risks and the term IL to describe the most onerous of SIL, EIL and CIL and hence the required performance of the SIF.

Table A.2 Example consequence equivalence

Conse-quence parameter	Safety conse-quences (statistical fatalities)	Safety conse-quence assuming the hazard has a immediate potential of harm, i.e. $V = 1$	Environmental consequences	Commercial conse-quences
C_A	Minor injury (not reportable)	Minor injury (not reportable)	Minor release	Up to £100,000
C_B	0.01 - 0.1	Serious permanent injury	Local impact	>£100,000 - £1 million
C_C	>0.1 - 1	Death of one person	Regional impact	>£1 million - £10 million
C_D	>1	Death of more than one person	National impact	>£10 million

A.3 Layer of Protection Analysis (LOPA)

The LOPA method of SIL determination is described in IEC 61511-3, Annex F. The LOPA report is shown in Table A.3.

The severity level in column 2 categorises the worst credible safety consequences of the impact event. Each severity level needs to have an associated maximum likelihood and this sets the tolerable residual risk level in the LOPA method. As for the risk graph, this is not stated in IEC 61511-3. The mitigated event likelihood, which is the likelihood of the impact event with its associated safety consequences after an SIF is included, should not exceed the defined maximum likelihood.

For a single fatality event, if a maximum likelihood of 1×10^{-4} in a year is used as discussed in Table A.2, because the intermediate event likelihood is 3×10^{-5}/year in the example in the first row, an SIF with maximum PFD of 0.32 (below the SIL 1 range and sometimes known as SIL 0) is required to come below the maximum likelihood.

Note: For the mathematics of LOPA to be valid, there needs to be independence between initiating events and layers of protection and between the layers of protection. Where there is common cause, either a dependent layer should not be credited at all or reduced credit (higher PFD) used. Where credit is claimed when there is common cause, it should be justified.

LOPA provides a PFD target which should be achieved or bettered in SIF implementation and throughout its operational life. While this PFD target would lie in a SIL PFD range, it is the PFD and not the SIL that sets the required performance of the SIF.

Table A.3 Layer of protection analysis (LOPA)

#	1	2	3	4	5	6	7	8	9	10	11	12	13
					Protection layers/ safeguards								
	Impact event description F.3 F.14.1	Severity level F.4 F.14.1	Initiating cause F.5 F.14.2	Initiation likelihood F.6 F.14.3	General process design F.14.4	BPCS F.14.5	Alarms, etc. F.14.6	Additional mitigation, restricted access F.8 F.14.7	IPL bunds, pressure relief F.9 F.14.8	Intermediate event likelihood F.10 F.14.9	SIF PFD F.11 F.14.10	Mitigated event likelihood F.12 F14.10	Notes
1	Fire from distillation column rupture	Possible 1 death (Example: Company max for single fatality event is 1×10^{-5}/yr)	Loss of cooling water to overhead condenser	0.3/yr Team estimate 1 in three year event based on plant experience	1 No credit for secondary containment, restriction orifice or check valve	0.1 Indepen-dent pressure control loop spills fluids to flare system on high pressure	1 Is alarm but from same pressure sensor credited in column 6 so not independent and no credit claimed	0.1 Occupancy at time of the event assumed 1 as operator likely in area in response to high pressure alarm. Vulnerability (probability of fatality) assumed 0.1	0.01 Relief valve is fully rated for this event and on clean duty	3×10^{-5}/yr Add Intermediate Event Likelihoods for all causes of same hazardous event where same SIF, then check against maximum allowable likelihood = 3.1×10^{-5}/yr	0.32 Required PFD to achieve 1×10^{-5}/yr = 1/3.1 =0.32 which is in SIL 0 range.	1×10^{-5}/yr May choose to implement as SIL 1 function which would reduce Mitigated Event Likelihood below 1×10^{-5}/yr	High pressure assumed sufficient to cause loss of contain-ment of column
2	Fire from distillation column rupture	Possible 1 death	Steam control loop failure on reboiler (full steam)	0.1/yr Team estimate 1 in 10 years. Not occurred in past 7 years operating experience.	1 No credit	0.1 Pressure spilloff to flare as above	0.1 Independent alarm indicates high steam flow and time to respond before loss of containment event	0.1 Occupancy 1 Vulnerability 0.1 as above	0.01 Relief valve is fully rated for this event and on clean duty	1×10^{-5}/yr	See above	See above	Same as above
The sub-clause references are to IEC 61511-3, Annex F.													

A.4 Comparison of Risk Graphs and LOPA

SIL determination is not an exact science. Risk graphs and LOPA are both semi-quantitative methods and can be calibrated against numerical risk criteria.

LOPA is more quantitative than risk graphs; the range of uncertainty in residual risk using LOPA is less than with risk graphs. Thus, if a given maximum residual risk is not to be exceeded, LOPA would, on average, produce lower SILs than risk graphs. LOPA is a more flexible method than risk graphs and better represents more complex functions with multiple other protection layers and safeguards. However, LOPA can take longer to use.

It is possible to gain the benefits of using both methods for a minimum expenditure of effort using risk graphs as a screening tool to assess all hazards involving SIFs. Where risk graphs suggest SIL 2 or higher is required, there may be benefit to be gained from re-assessing those functions using LOPA or a quantitative method, and take these results as the final results. The number of SIL 1 functions would likely be reduced if LOPA or a quantitative method is applied where risk graphs suggest SIL 1 or higher rather than SIL 2 or higher.

LOPA and risk graphs require facilitation by someone who is skilled in their use and in the principles of risk analysis.

Annex B Technology Issues

B.1 Introduction

This Annex provides an introduction to the range of technologies available for the implementation of safety functions, with reference to how each type of technology typically relates to the standard in terms of demonstrating compliance.

B.2 Assessment and Certification

IEC 61511-1 requires that equipment should be assessed for conformance with IEC 61508 or meet the "prior use" requirements. This assessment is generally design based rather than physical testing. Section 5.7 indicates the advantages of independent certification or conformance assessment, with this being preferable but not always possible.

Where the "prior use" approach is taken, operational data is used to give a statistical probability of each failure type. This method requires evidence of the quality of the recorded data and of the proportion of actual failures recorded. "Prior use" may be used as an alternative to adopting the recommended techniques and measures to avoid systematic faults.

The level of organisational independence of an assessor is dependent on the SIL compliance being sought: SIL 1 compliance may be achieved by self-assessment by an independent person in the same department or organisation, whereas SIL 3 should be assessed by an independent department or organisation. IEC 61508-1 Table 5 provides guidance on this topic, though the standard considers systems rather than components or subsystems.

Product assessment is not a simple pass/fail issue because standard products are used in diverse applications. Therefore, there are often limitations to the use of a product in safety applications. These are documented in the assessment report.

The assessment report may further reference other documents such as FMEDA calculations. When considering a product for use in a safety application, the manufacturer/supplier should be prepared to supply all the relevant assessment evidence, or at least make it available for inspection.

The assessment is a measure of the capability of the product to perform as part of an overall SIF at the quoted SIL, and does not take into account the total SIF architecture. For example, 10 devices might be required for a SIF, in which case the device's PFD or failure rate would be considerably lower than that for the overall SIF. The combination of the devices has a major impact on the SIF calculation, e.g. in terms of voting.

When considering technology for SIS realisation, suitable validation should be available for claims regarding the SFF and hardware fault tolerance. The higher the SIL requirement, the more substantiation and validation is required from the supplier.