SIF loop

All the devices within the SIS that are necessary to perform the required functionality of the SIF.
See *safety instrumented function (SIF)* and *safety instrumented system (SIS)*.

societal risk

Societal concerns due to the occurrence of multiple fatalities in a single hazardous event.
See *asset risk*, *corporate risk policy*, *environmental risk*, *group risk*, *hazardous event*, *individual risk,* and *risk*.
[Based on HSE *R2P2*.]

sufficient independence

The probability of a dependent failure (caused by a specified failure mode affecting more than one channel or system) is sufficiently low for it not to affect in any material manner the target safety integrity of a specified SIF.
See *common cause failure (CCF)*, *dangerous failure*, *failure mode*, *safety integrity* and *safety instrumented function (SIF)*.

systematic failure

Failure related to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors.
Note 1 to entry: The cause of systematic failures of the software may be known as 'bugs'.
Note 2 to entry: Corrective maintenance without modification would usually not eliminate the failure cause that involves the failure under particular conditions.
Note 3 to entry: A systematic failure can be reproduced by deliberately applying the same conditions, although not all reproducible failures are systematic.
Note 4 to entry: Examples of faults leading to systematic failures include human error that originates in:

– the SRS;
– the design, manufacture, installation, operation or maintenance of the hardware, and
– the design or implementation of software (including application program).

Note 5 to entry: Similar devices designed, installed, operated implemented or maintained in the same way are likely to contain the same faults. Therefore, they are subject to common cause failures [CCFs] when the particular conditions occur.
[Replicated from IEC 61511-1, clause 3.2.81.]
See *common cause failure (CCF), failure*, *human error*, *safety requirements specification (SRS)*,

target failure measure
The performance required from the SIF and specified in terms of either the average probability of failure to perform the SIF on demand for demand mode of operation [PFD_{avg}] or the average frequency of a dangerous failure for continuous mode of operation [PFH].
Note 1 to entry: The relationship between the target failure measures and the SIL are given in [IEC 61511-1] Tables 4 and 5 [Tables 1/C.1 and C.2 respectively in this technical publication].
[Replicated from IEC 61511-1, clause 3.2.83.]
See *average probability of dangerous failure on demand (PFD_{avg})*, *continuous mode*, *dangerous failure*, *demand mode SIF*, *mode of operation (of a SIF)* and *safety instrumented function (SIF)*.

target risk
Risk that is intended to be reached for a specific hazardous event taking into account the dangerous failures associated with the process, the control system associated with the process, the SISs and any ORRMs.
[Based on IEC 61508-4, clause 3.1.10.]
See *basic process control system (BPCS)*, *dangerous failure*, *hazardous event*, *other risk reduction measure (ORRM)*, *risk* and *safety instrumented system (SIS)*.

tolerable risk
Level of risk that is accepted in a given context based on the current values of society.
Note 1 to entry: See IEC 61511-3 Annex A.
[Replicated from IEC 61511-1 clause 3.2.84.]
Note 2: In GB, a tolerable risk is one that has been demonstrated to be ALARP. It lies between the upper and lower tolerable boundaries (the upper risk boundary bordering the intolerable region and the lower boundary bordering the broadly acceptable region).
See *as low as reasonably practicable (ALARP)* and *risk*.

worst case scenario
The highest severity of the specified consequence identified with a scenario that is theoretically possible regardless of the likelihood.
[Based on Kim *et al* (2003).]
See *worst credible case scenario*.

worst credible case scenario
The highest severity of the specified consequence identified with a scenario that is considered reasonably foreseeable.
[Based on Kim *et al* (2003).]
See *worst case scenario*.

A.3 GLOSSARY OF ACRONYMS AND ABBREVIATIONS

a.k.a.	also known as
ALARP	as low as reasonably practicable
AST	above-ground storage tank
ATEX	*atmosphères explosibles* (explosive atmospheres)
BPCS	basic process control system

CBA	cost benefit analysis
CCF	common cause failure
CCPS	Center for Chemical Process Safety
CDOIF	Chemical and Downstream Oil Industries Forum
CM	conditional modifier
C&E	cause and effect [chart]
C&I	control and instrumentation
COMAH	*Control of major accident hazards [regulations]*
CPU	central processing unit
CTF	catastrophic (storage) tank failure
DCS	distributed control system
DETR	Department of the Environment, Transport and the Regions
DF	disproportion factor
DSEAR	*Dangerous substances and explosive atmospheres regulations*
EC&I	electrical, control and instrumentation
EI	Energy Institute
EMI	electromagnetic interference
ESD	emergency shutdown
EU	European Union
FPL	fixed programme language
FSA	functional safety assessment
FSM	functional safety management
FTA	fault tree analysis
GB	Great Britain
H&RA	hazard and risk assessment
HAZID	hazard identification [study]
HAZOP	hazard and operability [study]
HEF	hazardous event frequency
HEP	human error probability
HFT	hardware fault tolerance
HSE	Health and Safety Executive
HSL	Health and Safety Laboratory
IChemE	Institution of Chemical Engineers
IE	initiating event
IEC	International Electrotechnical Commission
IET	Institution of Engineering Technology
IPL	independent protection layer
ISA	The International Society of Automation
ISD	inherently safer design
ISO	International Organization for Standardization

LL	low low [level]
LOPA	layers of protection analysis
LT	level transmitter
LVL	limited variability language
MATTE	major accident to the environment
MoC	management of change
ORRM	other risk reduction measure
NA	The National Archives
P&ID	piping and instrumentation diagram
PES	programmable electronic system
PFD	probability of dangerous failure on demand
PFD_{avg}	average probability of dangerous failure on demand
PFH	probability of failure (average frequency of dangerous failures) per hour
PFP	passive fire protection
PHA	process hazard analysis
PL	protection layer
PLC	programmable logic controller
PLm	protection layer (mitigation)
PLp	protection layer (prevention)
PRV	pressure relief valve
PSC	Process Safety Committee
PSD	process shutdown
PSLG	Process Safety Leadership Group
QHRA	quantified human reliability analysis
QRA	quantitative risk assessment
R2P2	*Reducing risks, protecting people*
RRF	risk reduction factor
RRM	risk reduction measure
SFAIRP	so far as is reasonably practicable
SIF	safety instrumented function
SIL	safety integrity level
SINTEF	Stiftelsen for Industriell og Teknisk Forskning
SIS	safety instrumented system
SPA	Source Protection Area
SRS	safety requirements specification
SSSI	Site of Special Scientific Interest
UK	United Kingdom
UKPIA	United Kingdom Petroleum Industry Association
VCE	vapour cloud explosion

A.4 GLOSSARY OF SYMBOLS

λD	dangerous failure rate
F_E	target harmful event frequency
F_P	proposed new target harmful event frequency
I	current
P	pressure

ANNEX B
REFERENCES AND BIBLIOGRAPHY

The information provided in this annex comprises references to legislation, technical publications, internet sites, etc. that are referred to in this technical publication. This annex also includes bibliographies of further reading, which are not referred to herein. All items were correct at the time of writing. Readers should consult the pertinent organisations for details of the current versions. To assist, internet addresses are provided.

For international standards, the pertinent national standard should be used.

Center for Chemical Process Safety (CCPS)
https://www.aiche.org/ccps

References

Process safety glossary (accessed 4 September 2018)

Bibliography

Layer of protection analysis: *Simplified process risk assessment*

Department of the Environment, Transport and the Regions (DETR)
https://www.gov.uk/government/organisations/department-of-the-environment-transport-and-the-regions

Bibliography

Guidance on the interpretation of major accident to the environment for the purposes of the COMAH regulations

http://webarchive.nationalarchives.gov.uk/20130402151656/http:/archive.defra.gov.uk/environment/quality/chemicals/accident/documents/comah.pdf (accessed 20 February 2018)

Guidelines for environmental risk assessment and management: Green leaves III

https://www.gov.uk/government/publications/guidelines-for-environmental-risk-assessment-and-management-green-leaves-iii (accessed 20 February 2018)

Management of harm to the environment: Criteria for the management of unplanned releases

Energy Institute (EI)
https://publishing.energyinst.org

References

Guidance on quantified human reliability analysis (QHRA)

Guidance on achievement, operation and maintenance of functional safety employing safety instrumented systems in support of IEC 61511

Research Report: Atmospheric pressure above-ground storage tank loss of containment incidents involving petroleum, petroleum products, or other fuels

European Union (EU)
http://eur-lex.europa.eu

References

Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work ('Framework directive')

Directive 1999/92/EC of the European Parliament and of the Council of 16 December 1999 on

minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres ('*ATEX protection of workers directive*')

Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC ('Seveso III' directive)

Health and Safety Executive (HSE)
http://www.hse.gov.uk

References
ALARP suite of guidance, http://www.hse.gov.uk/risk/expert.htm (Accessed 20 February 2018)

Assessing compliance with the law in individual cases and the use of good practice

http://www.hse.gov.uk/risk/theory/alarp2.htm (accessed 20 February 2018)

CDOIF Guideline: Environmental risk tolerability for COMAH establishments

https://webcommunities.hse.gov.uk/connect.ti/COMAHSF/view?objectId=651141 (Accessed 20 February 2018)

Cost benefit analysis (CBA) checklist http://www.hse.gov.uk/risk/theory/alarpcheck.htm (accessed 20 February 2018)

HSE principles for cost benefit analysis (CBA) in support of ALARP decisions http://www.hse.gov.uk/risk/theory/alarpcba.htm (accessed 20 February 2018)

Management of instrumented systems providing safety functions of low/undefined safety integrity http://www.hse.gov.uk/foi/internalops/og/og-00046.htm (Accessed 20 February 2018)

Process Safety Leadership Group: Final report – Safety and environmental standards for fuel storage sites (a.k.a. HSE *PSLG Final report*) [http://www.hse.gov.uk/comah/buncefield/fuel-storage-sites.pdf] (Accessed 20 February 2018)

Reducing risks, protecting people ('R2P2') http://www.hse.gov.uk/risk/theory/r2p2.pdf (Accessed 20 February 2018)

Research Report 716: *A review of layers of protection analysis (LOPA) analyses of overfill of fuel storage tanks* http://www.hse.gov.uk/research/rrhtm/rr716.htm (accessed 20 February 2018)

Bibliography

Offshore Information Sheet No. 3/2006, *Guidance on risk assessment for offshore installations*

http://www.hse.gov.uk/offshore/sheet32006.pdf (accessed 4 September 2018)

COMAH 2015 safety report assessment manual (SRAM): *13 Environmental aspects of safety report assessment* http://www.hse.gov.uk/comah/sram/docs/s13.pdf (accessed 20 February 2018)

The Institution of Engineering Technology (IET)
https://www.theiet.org

References
Code of practice: Competence for safety related systems practitioners.

Institution of Chemical Engineers (IChemE)
http://www.icheme.org

References
Using risk graphs for safety integrity level (SIL) assessment – A user-guide for chemical engineers

International Electrotechnical Commission (IEC)
http://www.iec.ch

References

IEC 61508 series: Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 61511 series: Functional safety – Safety instrumented systems for the process industry sector

IEC 62443 series: Industrial communication networks – Network and system security

Bibliography

IEC 62061: Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)
https://www.iso.org http://www.iec.ch

References

Guide 51 Safety aspects – Guidelines for their inclusion in standards

Journals, conference proceedings

References

Kim D, Moon I, Lee Y and Yoon D, *Automatic generation of accident scenarios in domain specific chemical plants*, Journal of Loss Prevention in the Process Industries 16, 121–132 (2003)

Stiftelsen for Industriell og Teknisk Forskning (SINTEF)
https://www.sintef.no

References

Reliability data for safety instrumented systems, *PDS data handbook*

Technis
http://technis.org.uk

References

FARADIP.THREE V6.4

FARADIP.THREE V8.0

The International Society of Automation (ISA)
https://www.isa.org

References

TR84.00.04 Part 1-2015 *Guidelines on the implementation of ANSI/ISA-84.00.01-2004 (IEC 61511)*

The National Archives (NA)
http://www.legislation.gov.uk

References

Control of major accident hazards ('COMAH') regulations 2015, SI 2015/No. 483
Dangerous substances and explosive atmospheres regulations 2002 ('*DSEAR*'), SI 2002/No. 2776

United Kingdom Petroleum Industry Association (UKPIA)
http://www.ukpia.com

References

SIL1 Human factors assessment tool

ANNEX C
DETAILED GUIDANCE ON SIL DETERMINATION

C.1 INTRODUCTION

The purpose of this annex is to provide sufficient technical background in the key concepts of functional safety in relation to SIL determination, in order that the technical concepts underpinning the guidance provided in this technical publication are understood, and to provide a sound basis for further learning development.

This annex builds on the basic introduction given in Section 2, which sets out the terminology and concepts used in this technical publication.

This annex provides detailed guidance on the:

– Numerous terms that are used within functional safety, and which might otherwise detract from users gaining a better understanding of the underpinning technical concepts.
– Relevant process safety aspects that give rise to risks, and which should be reduced by PLs to achieve a defined target risk (e.g. tolerable), such that safety and environmental risks are reduced to ALARP.
– Role of a SIS and the SIFs it performs in achieving specified risk reduction for the specified hazardous events.
– Concept of the SIL of a SIF and its importance in SIS design.
– Role of PLs in providing the necessary risk reduction for IEs that lead to the specified hazardous event.
– Impact that CMs have in reducing the frequency of the specified consequence arising.

C.2 WHAT SIL DETERMINATION ACHIEVES

The objective of SIL determination is to identify and define SIFs that are necessary to reduce the risk to ALARP by determining:

– Whether it is necessary to employ a SIS to carry out a specific SIF, where there may be a shortfall in the risk reduction achieved by ORRMs to meet the target risk (i.e. the target harmful event frequency for the specified consequence).
– The SIL of the SIF together with its target failure measure (e.g. RRF), where it has been determined that there is a shortfall in the risk reduction needed to meet the target risk for the specified target harmful event frequency.
– Whether the target risk has been reduced to ALARP or whether further risk reduction is necessary to achieve a tolerable risk.

For SIL determination, the hazardous event should be properly identified by undertaking a hazard analysis (e.g. HAZOP study), and RRMs should be put in place to either prevent the hazardous event using PLs (prevention) or to mitigate the consequences of the hazardous event using PLs (mitigation).

Whilst the focus of this technical publication is the determination of the SIL of the specified SIF, when the latter is acting as a PL, non-SIF RRMs (i.e. ORRMs) should be adequately addressed with respect to their specification, design and ongoing operation and maintenance. For example, there should be a clear rationale for the basis of the design of the non-SIF PL for the specified safety function, and there should be procedures to maintain the required probability of failure of the safety function throughout the life of the process plant.

The risk is reduced if:

– the frequency of the hazardous event is reduced by carrying out the SIF within the SIS (this is referred to as a PL(prevention)), and/or
– the consequence of the hazardous event is reduced by carrying out the SIF within the SIS (this is referred to as a PL(mitigation)).

See 2.4.3 and Figure 7.

Example: PL(prevention): a SIF being carried out by a SIS acting as a PL(prevention) opens a valve in a pressure vessel, which prevents the pressure in the vessel exceeding a safe value. In this example, the SIF within the SIS reduces the frequency of the hazardous event from occurring from 1 in 10 years to 1 in 200 years, thereby reducing the frequency parameter of the risk and giving a lower risk.

Example: PL(mitigation): a SIF being carried out by a SIS acting as a PL(mitigation) is a fire and gas system that does not prevent the hazardous event from taking place (release of flammable vapour, which may ignite and lead to a serious fire), but mitigates the effect of the consequence of the fire by, for example, activating a high pressure water mist system. In such a situation, the consequence may have been reduced from two fatalities to five people being injured, which reduces the severity of the harm parameter, leading to a lower risk.

Figure C.1 illustrates the concept of prevention and mitigation using a bow-tie diagram, which:

– provides a logical sequence of risk reduction on the left-hand side of the hazardous event achieved through HEF reduction using PL(prevention), and
– indicates the concept of mitigation in a cause-consequence diagram on the right-hand side of the hazardous event using PL(mitigation).

Figure C.1 shows several potential IEs (IE1–IE4) and one potential consequence (A). Also shown is one CM (see C.9); CMs are relevant in the SIL determination process.

There should be sufficient independence between:

– PL1.1 and PL1.2 and PL1.3;
– PLs (PL1.1, PL1.2, PL1.3) and IE1;
– PL2.1 and PL1.3;
– PLs (PL2.1, PL1.3) and IE2;
– PL3.1 and PL3.2 and PL1.3;
– PLs (PL3.1, PL3.2, PL1.3) and IE3;
– PL4.1 and PL4.2 and PL1.3;
– PLs (PL4.1, PL4.2, PL1.3) and IE4, and
– PL5.1 and (PL1.1, PL1.2, PL2.1, PL3.1, PL3.2, PL4.1, PL4.2) and (IE1, IE2, IE3, IE4).

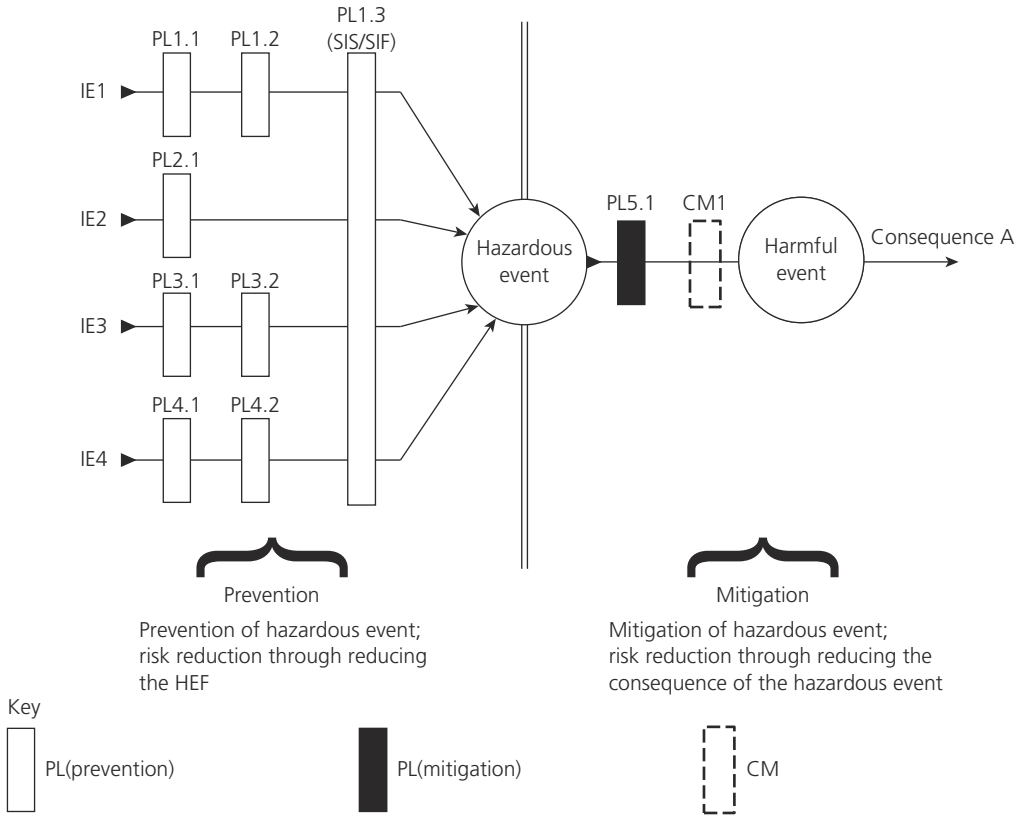

Figure C.1: PLs (prevention) and PLs (mitigation) illustrated through a bow-tie diagram

Notes:

1. The hazardous event has one specified potential consequence with its own harmful event frequency.
2. PL5.1, which is a PL(mitigation), reduces the severity of the specified consequence to Consequence A.
3. CM1 reduces the frequency of the specified consequence (i.e. reduces the harmful event frequency of Consequence A).
4. Here, PL1.3, which is the SIS/SIF, is designed to prevent IE1-IE4. In practice, the SIS/SIF may be incapable of preventing all the IEs and other means of providing the required protection would have to be employed.

C.3 DETERMINING HAZARDOUS EVENTS

Hazard analysis risk assessment underpin the SIL determination process. These should be carried out on the process plant and its associated equipment, including the BPCS. The hazard analyses and risk assessments should address all reasonably foreseeable process plant and control system situations, including normal operation, start-up, shutdown, maintenance, modification and process upset and emergency shutdown.

The hazard analysis and risk assessment should determine the hazardous events, and for each specified hazardous event: