

Safety Jargon Buster

ABB's Safety Jargon Buster explains some of the terminology users are likely to encounter when purchasing or handling safety equipment and systems for process applications. If you have a specific question relating to any aspect of process safety and design, please send an email to stuart.nunns@gb.abb.com. Alternatively, you can contact ABB's specialists for advice on 01642 372000.

ABB's *Safety Jargon Buster* uses hyperlinks for quick navigation. A click on any underlined word takes you straight to the relevant entry. Alternatively, use the Quick Navigation Tool below to select a relevant section.

Quick navigation tool:

<#> [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

#

1ooN System

A safety instrumented system made up of a number of independent channels, any of which is sufficient to perform the correct safety function. (Safeguard is a 1oo2 RDA system).

2ooN System

A safety instrumented system made up of a number of independent channels, two of which are required to perform the correct safety function. (Triguard and Plantguard are 2oo3 TMR systems).

A

Acceptable Risk

A very low risk of an accident occurring.

Accreditation

The procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.

Alarm Management

The set of processes and practices for determining, documenting, designing, monitoring, and maintaining alarm messages.

ALARP - As Low As is Reasonably Practical

When a risk has been reduced as much as it practically can, or when further improvements would be disproportionately costly, the risk is said to be As Low as is Reasonably Practical. (IEC61508 Annex B of part 5).

ANSI

American National Standards Institute.

Approved Code of Practice

ACOPs are issued by the Health & Safety Commission with consent of the UK Government which give practical guidance on how to comply with an Act or Regulation. ACOPs are, along with all relevant standards, admissible in evidence in any prosecution brought under the Health & Safety at Work Act.

Approved equipment list

An equipment list developed by an organisation involved in implementing a phase or phases of the safety lifecycle and consisting of a formal process which determines that the equipment to be used is suitable for use in the operating environment and in control, protective, or safety applications. Such processes frequently call equipment to be third-party certified for compliance to IEC 61508.

Architecture

The physical organisation, interconnection, or integration of the equipment of a safety instrumented system that operates according to the design basis. The specific configuration covers the hardware and software elements in a system.

Assessment

The design of a trip system should be assessed to ensure it will meet its design requirements. Assessment should be thorough and should cover design specification, operation, testing, maintenance and system management.

Asset integrity level

A method of specifying the level of integrity needed by systems used to reduce safety risks to assets.

Asset Protection

Functions allocated to system design for the purpose of preventing loss to assets.

Availability

The probability that a system will be able to perform its designated function when required for use.

Average probability of failure

The average probability of failure on demand (Pfd) of an item of equipment or system is the probability that an item or system will be in a failed state when a demand is placed on the item of equipment to operate. The probability is evaluated as the average Pfd for demands which may occur at any time during the time interval, T, between proof tests.

ATEX

The term 'ATEX' is derived from the French Atmospheres Explosive. There are two EU Directives ATEX 95 (94/9/EC) and ATEX 137 (1992/92/EC) concerning, respectively, the supply and use of equipment in potentially explosive atmospheres.

B

Basic process control system (BPCS)

A system which responds to input signals and generates outputs to control the process and its associated equipment.

Black-box

A test design method that treats the system as a "black-box", requiring no knowledge of the internal structure.

Black communications channel

A communications channel connected to safety-related system elements, such that the communications between its interfaces has no safety requirement. With a black channel data from the sending safety system/element is launched into an unknown communications mechanism. Therefore to use a black channel for safety related data, the data (and connected elements) must have built-in mechanisms to detect any interference and with a confidence level of detection that is suitable for the safety application relying on the data. The connecting elements fully comply with the requirements of IEC 61508. A black channel is recognised as having failure modes which could compromise safety function integrity, and these failure modes are compensated by additional diagnostics in a safety wrapper or layer, or by application functions such as handshaking routines which must be demonstrated to achieve the equivalent integrity of a white channel.

Burner management system

An instrumented protective system dedicated to combustion safety that monitors fuel conditions, verifies the presence of pilot and main flame, and ensures proper light-off. It does not control the air-to-fuel ratio, firing rate, boiler feed water, or other related functions.

Bypass

Also referred to as override – an action taken to override, defeat, disable, or inhibit a protective system. These actions prevent operation of the protective system or safety function. Such bypasses must be formally recorded/logged and brought to the attention of operational personnel (by way of alarm, log etc).

C

CA - Competent Authority

A government agency that oversees compliance with safety and environmental legislation. In England and Wales it is the Health & Safety Executive and the Environment Agency, while in Scotland it is the Health & Safety Executive and the Scottish Environment Agency.

CASS - Conformity Assessment of Safety Systems

A third party accredited certification scheme used to demonstrate compliance to IEC61508 comprising functional safety management and product assessment. Assessment and certification is undertaken by bodies such as SIRA, using CASS Registered Assessors from organisations such as ABB.

CENELEC

European Committee for Electrotechnical Standardisation.

Certification

Procedure by which a third party gives written assurance that a product, process or service conforms to the specified requirements. (BS EN 45020).

CE Marking

Marking on a product, comprising the initials CE which attests to the conformity of the product with all applicable EC Directives.

Channel

Element or group of elements that independently perform(s) a function.

CHAZOP - Computer HAZOP

A process covering criticality and failure review of complex programmable electronic systems.

COMAH - Control Of Major Accident Hazards

A regulation which became law on the 1st of April 1999 enacting The European Directive 96/82/EC or 'Seveso II'. Its aim is to prevent and mitigate the affects of major accidents involving dangerous substances which can cause serious harm to people and /or the environment - COMAH regulations treat risk to the environment as seriously as those to people.

Commercial off the shelf system COTS

A commercially available product (hardware, software, system) for which no claim is made for use in a safety application.

Common cause failure

A simultaneous or near-simultaneous failure of several equipment items due to a single cause.

Common Mode Failure

A common cause failure in which items fail in the same manner due to factors such as poor design or maintenance.

Competency

In the context of individuals that have responsibility for any phase or phases of the safety lifecycle, competency is a measure and description of the knowledge, experience, training and qualifications of these individuals and their capability to execute their assigned tasks in accordance with approved practices and procedures.

Competency Management System

A repository of safety-related competency data (knowledge, experience, training and qualifications) and profiles for all individuals eligible to undertake safety-related project activities. In addition the repository will contain a description of the competency assessment process, competency ratings and the means for recording competency assessments.

Competent Authority

See CA.

Compliance

A synonym for conformance.

Component

A part of a system, subsystem, or device which helps achieve an overall function - a smart transmitter is a field device with components such as embedded software, communication protocols, configuration panels, etc.

Configuration

The functional and/or physical characteristics of the hardware and/or software required for the equipment to operate according to the design basis. See architecture.

Configuration management

The systematic application of management policies, procedures, and practices to assess and control changes to the hardware and/or software of a system and to maintain traceability of the configuration to the design basis throughout the system life.

Configuring

See programming.

Conformance

A product or process is said to conform to a standard when it meets the relevant requirements within it.

Conformity Assessment

Procedure for checking that a product, service or system conforms to a standard or specification.

Continuous mode

A dangerous instrumented protective system (IPS) failure causes a hazardous event without further failure.

Control system

Control systems are used to maintain process performance and ensure they remain within safe and economical limits.

D

Dangerous failure

A failure which may put the safety instrumented system in a state in which it is hazardous or fails to function.

De-energise to trip

Circuits where the final elements are energised under normal operation and the removal of power source (e.g. electricity, instrument air) causes the instrumented protective system (IPS) to take its defined action.

Defeat

This term describes the prevention of operation of a trip system by an operator or other personnel, most usually for trip system maintenance or testing, or to allow plant operation when part of a protective system has failed. The practice of operating plant without full protection is not normally an acceptable practice and should be subject to management by a responsible person or persons.

Demand

A condition or event that requires a protective system or device to take appropriate action to prevent or mitigate a hazard.

Demand mode

Dormant or standby operation where the instrumented protective function IPF takes action only when a process demand occurs.

Dependent failure

A failure caused by a combination of individual events, but whose probability is not the simple product of the probability of those events.

Designated architecture

Architecture developed by means of a specified model and designed to meet a defined hardware safety integrity.

Design fault

A systematic failure in the design of a system, caused by a mistake in the design phase.

Detected, revealed, overt

Faults in hardware and software detected by diagnostic tests, proof tests, physical inspection and manual tests, or through normal operation.

Device

A unit or entity of hardware or software, capable of accomplishing a specified task.

Diagnostic coverage

A decrease in the probability of detected dangerous hardware failures, resulting from the operation of automatic diagnostic tests.

Diagnostic test interval

The interval between on-line tests to detect faults that have a specified diagnostic coverage.

Diversity

Diversity is said to exist when there are different ways to perform a required function.

E

Electrical/electronic/programmable electronic (E/E/PE)

Equipment based on electrical and/or electronic and/or programmable electronic technology. (IEC61508 3.2.6)

Electrical/electronic/programmable electronic system (E/E/PES)

A system for control, protection or monitoring based on one or more E/E/PE devices. (IEC61508 3.3.3)

Electromagnetic Immunity

See EMI

Element

Part of a *subsystem* comprising a single component or a group of components that implement part of one or more safety functions. If the failure of the element results in the failure of the safety function then the element itself is classified as a subsystem (in the context of the safety function being considered). If the failure of the element does NOT result in a failure of the safety function then the element is NOT classified as a subsystem and retains its status as an element.

Whether or not an element or a group of elements comprise a subsystem cannot be determined until the top-level architecture of the end-to-end safety function has been defined.

An element may comprise hardware or software, or both hardware and software. Typical examples of elements are temperature transmitters, logic solvers, input modules, output modules, barriers, relays. Elements typically consist of components. A component is the lowest level of entity.

EMI

Electromagnetic Immunity is a measure of a product's ability to function as intended in the presence of electromagnetic activity. This activity can be in the form of electromagnetic waves in the atmosphere, the product's resistance to which is known as radiated immunity; via electromagnetic interference on supply and interconnecting cables, known as conducted immunity, or additionally in the form of electrostatic discharge. To achieve electromagnetic immunity, a product must be able to be tested to the requirements of a particular standard and meet pre-determined functional acceptance criteria described therein.

Energise to trip

Circuits where the final elements require the power to take or maintain the safe state. Where power is required to maintain the safe state of the safety function (typically in energise to trip functions) additional requirements are necessary in terms of power supply diversity and monitoring as defined in clause of IEC 61511, Part 1, clause 11.2.11.

Error

Part of a system state which has been damaged by a fault, and therefore liable to lead to a failure.

EUC - Equipment under control

Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities. (IEC61508 3.2.3)

Event Tree Analysis

Method for illustrating the intermediate and final results of a particular initial event.

External communication

Data exchange between an Instrumented Protective System (IPS) and a variety of other systems or devices. These include shared operator interfaces, maintenance/engineering interfaces, data acquisition systems, host computers etc.

F

Fail safe

The ability of the system to default to a defined process state under any fault condition.

Fail-to-danger fault

A fault which prevents a trip system from responding to a demand or which causes the process to move towards a dangerous condition. These types of faults can only be found through proof testing or when a demand occurs.

Failure

Failure occurs when a unit can no longer perform a required function.

FAT

Factory Acceptance Test – a series of tests conducted in the factory (prior to being shipped to the client's / operator's site) to determine and document whether equipment, hardware and software operates according to its specification, covering functional, fault management, communication, support systems, and interface requirements.

Fault

An abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.

Fault avoidance

Techniques and procedures used to avoid the introduction of faults.

Fault tolerance

The ability of a unit to continue to function despite the presence of faults or errors.

Field devices

Equipment connected to the field side of the safety instrumented system (SIS) logic solver I/O terminals. Such equipment includes field wiring, sensors, final control elements and those operator interface devices hard-wired to SIS logic solver I/O terminals.

Final element

A component of a safety instrumented system which takes the action necessary to achieve a safe state. Examples are valves and switch gear, which can be used to put the equipment in a safe condition by shutting off the flow of fluids or electricity.

FMEA - Failure Mode and Effects Analysis

A technique for identifying potential modes of failure and the undesirable effects which would result.

Fractional Dead Time

See probability of failure on demand average (PFDavg).

FTA - Fault Tree Analysis

Technique for determining the relationship between potential hazards and their possible root causes; concerned particularly with cases where several different causes might combine to produce an undesired effect.

Full variability language

Typically a general purpose computer based high-level language (Ada, C++) that is equipped with an operating system. The operating system provides a real-time multi-programming environment. The high-level language is tailored for the specific application domain resulting in a unique set of programmes for the specific application. This type of language is not typically used in an instrumented protective system (IPS) application. When this type of language is used then more rigour needs to be applied in the specification and use of appropriate Techniques and Measures.

Functional safety

The ability of a safety instrumented system to carry out the actions needed to achieve or maintain a safe state. (IEC61508 3.1.9).

Functional safety assessment

An investigation to judge the functional safety achieved by one or more E/E/PE safety-related systems.

Functional safety audit

An examination to determine the effectiveness and suitability of functional safety procedures.

Functional Safety Management System (FSMS)

The set of processes, procedures, templates, checklists, techniques and measures, etc, specific to an organisation implementing defined phase(s) of the safety lifecycle which comply with the 'management of functional safety' clauses of IEC 61508 (Part 1 clause 6) and IEC 61511 (Part 1 clause 5).

Functional test

Usually referred to as the testing of a safety-related system to ensure that the specified function is working correctly. Note a functional test would not detect that one of the channels in a dual redundant channel architecture was in a faulty condition.....a proof test would since all the elements in the system would need to be tested.

Functional unit

Entity of hardware or software, or both, capable of accomplishing a specified purpose.

G

H

Hardware Fault Tolerance

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

Hardware safety integrity

The degree to which hardware failures in a safety instrumented function would impair its safety integrity. That part of safety integrity relating to random hardware failures in a dangerous mode of failure.

Harm

Physical injury or damage to the health of people either directly, or indirectly as a result of damage to property or to the environment. (IEC61508 3.1.1).

Harmonised European Standard

A European European standard prepared by CEN/CENELEC under a mandate from the Commission, with a view to the fulfilment of the essential requirements (ESR) of a New Approach Directive.

The term harmonised standard shows a direct connection to the compliance with New Approach Directives.

Hazard

Potential source of harm, to people or the environment (IEC61508 3.1.2).

Hazard log

The central control and reference document for demonstrating the safety characteristics of the system. Provides traceability of the hazard management process.

Hazard type

Hazard types need to be defined as part of *hazard and operability (HAZOP)* studies. They are normally defined as:

Hazard Type (A) – safety/environmental/statute/industry standard (or equivalent)

Type A hazards cover any situation where there is a danger to life or a risk of serious injury to people. It also covers anything that might cause significant harm to the environment.

Hazard Type (B) – operational (or equivalent)

Type B hazards apply to situations where there is danger to plant, equipment, production, process materials or market position, including product quality.

Hazardous event

Hazardous situation which results in harm (*IEC61508* 3.1.4)

Hazardous situation

Circumstance in which a person is exposed to hazard(s) (*IEC61508* 3.1.3)

HAZOP - Hazard and Operability Study.

A technique which considers the effects of deviation from the normal operating intent by identifying basic causes, their immediate effects and the resultant consequences.

HRA Hazard & Risk

The process of identifying hazards to the Equipment Under Control (EUC) in all modes of operation, the event sequences leading to the hazards, and the EUC risks associated with the hazards.

HSE Health and Safety Executive

An independent body responsible for the regulation of almost all the risks to health and safety arising from work activity in Britain. Reporting to the Health & Safety Commission.

Human error, mistake

Human action or inaction that produces an unintended result.

Human Machine Interface (HMI)

The means by which information is communicated between the operator and a system typically through computer displays, indicating lights, alarm panels, pushbuttons, alarms. Often referred to as the Man Machine Interface (MMI).

I

IEC - International Electrotechnical Commission

The leading global organisation that prepares & publishes international standards for all electrical, electronic and related technologies. IEC's standards represent the core of the World Trade Organisation's Agreement on Technical Barriers to Trade (TBT).

IEC61508

An international standard that provides a structure for the quantitative and qualitative assessment of "*risk*" encountered in applications of *Electrical, Electronic and Programmable Electronic (E/E/PE)* equipment in industry. It also provides measures to be taken to reduce those risks "as low as reasonably practical" (*ALARP*).

IEC 61511

IEC 61511 is a three-part international standard concerned with *functional safety* instrumented systems for the process industry. It covers the design, integration, installation, use, maintenance, modification and decommissioning of *safety instrumented systems (SIS)*. As the title implies, this standard (unlike *IEC 61508*) is specific to the process industry.

Impact analysis

A way of determining the effect that a change to a function or *component* will have on other functions or components.

Independent department

A department separate from the departments responsible for activities which take place during specific phases of the *safety life cycle* that is subject to *functional safety assessment* or *validation*.

Independent organisation

Organisation which is separate from the organisations responsible for the activities which take place during the specific phases of the *safety life cycle* that is subject to *functional safety assessment* or *validation*.

Independent person

Person who is separate from the activities which take place during the specific phase of the *safety life cycle* that is subject to the *functional safety assessment* or *validation*, and does not have direct responsibility for those activities.

Independent Protective Layer (IPL)

A *device, system*, or human action designed to reduce the likelihood or severity of the impact of an identified hazardous event by a large factor, i.e. at least by a 100 fold reduction in likelihood. An IPL must be independent of other protection layers associated with the identified hazardous event.

Informative

Elements of the IEC61508 standard which provide additional information to assist in the understanding or use of the IEC61508 standard.

Input function

Monitors the process and its associated equipment to provide input information for the logic function.

Input modules

A part of an E/E/PES that acts as the interface to external devices and converts input signals to signals that the E/E/PES can utilise.

Instrument

Apparatus used in performing an action.

Instrumented Protective Function (IPF)

A protective function allocated to an instrumented protective system (IPS) that provides the risk reduction necessary to reduce the risk of an identified hazardous event to below the agreed risk criteria. The risk criteria is that specified by the end user/process owner/operator.

Instrumented Protective System (IPS)

Composed of a separate and independent combination of sensors, logic solvers, final elements, and support systems that are designed and managed to achieve a specified risk reduction. An IPS may implement one or more instrumented protective functions (IPF).

Integrated Control and Safety

Typically refers to a safety-related logic solver that provides a common physical architecture/safety platform for control and safety functions but with full functional independence.

Interlock systems

Interlock systems consist of one or more trip initiators, a logic or relay element and one or more output mechanisms. The logic element is arranged so that in the event of a pre-defined combination of initiators indicating a potential unsatisfactory plant condition, a signal will be passed to the output mechanism to prevent the condition from occurring.

When the initiators indicate normal plant conditions, the trip will be reset without any resetting action being required by the operator.

Interlocks are used less frequently than trips, as the requirement for the operator to manually reset a trip makes a contribution to safety by preventing unobserved re-start of a process when plant conditions return to normal.

Internal communications

Data exchanges between the various devices within a given instrumented protective system. These include bus backplane connections, the local or remote I/O etc.

ISA

Instrumentation, Systems and Automation society.

J

K

L

Layers of Protection Analysis (LOPA)

A process analysis method which takes the data developed in the Hazard & Operability analysis and accounts for each identified hazard by documenting the initiating cause and the protection layers that prevent or mitigate the hazard. The total amount of risk reduction is determined and the need for more risk reduction analysed. If risk reduction is to be provided in the form of a SIS, LOPA allows for the determination of the appropriate SIL for the SIF.

Legacy system

An existing installed protective system typically implemented prior to IEC 61508 which may or may not be supportable. Systems implemented prior to IEC 61508 will in general not have been chosen to provide specific levels of integrity (in terms of dangerous failures).

Limited variability language (LVL)

This language allows the user to customise the functionality of the programmable electronic system (PES) to achieve the specific safety function requirements. LVL consists of sets of basic program elements, such as function blocks and the method for combining them into an application specific program. Many independently certified programmable logic solvers use IEC 61131 compliant programming languages, which comprise ladder logic, functional block diagrams, sequential function charts and Boolean algebra.

Line monitoring

The monitoring of either a Digital Input or Digital Output signal allowing detection of short circuit and open circuit conditions – allowing the Safety Instrumented System (SIS) to take appropriate action.

Logic function

The function which uses input information to produce output information.

Logic solver

Equipment that implements one or more logic functions. Examples include electrical systems, electronic systems, programmable electronic systems, pneumatic systems and hydraulic systems.

Logic solver subsystem

That part of a safety-related system that performs the function logic but excludes the sensors and final elements. The logic solver subsystem typically consists of a Safety Instrumented System (SIS) safety controller and I/O modules, cabinets with appropriate termination panels for connecting the process signal to the logic solver I/O modules, barriers and relays. Power supplies and power distribution for the logic solver and field devices are also normally included.

Logic system

The part of a system that performs the functional logic but excludes the sensors and final elements. The logic system receives the on/off signals from the trip initiators (and also from manual trip initiation) and relays them to the trip mechanisms.

Loss prevention

The activities carried out to minimize any form of accidental loss, including loss through damage to people, property or the environment, and financial loss.

Low complexity E/E/PE safety-related system

An E/E/PE safety-related system where the failure modes of each individual component are well defined and its behaviour under fault conditions can be completely determined.

Low complexity system

A system in which the failure modes of each individual component are well defined and the behaviour of the system under fault conditions can be completely determined.

Low Demand Mode

Where a safety-related system is asked to operate no more than once per year and no greater than twice the proof test frequency.

M

Maintainability

The ability of an item, under given conditions of use, to be retained in or restored to a state in which it can perform a required function, when an error is detected, under given conditions and using stated procedures and resources.

Maintenance (Adaptive)

Maintenance carried out to reflect changes in the operational environment of the system.

Maintenance (Corrective)

Maintenance carried out to rectify detected faults and anomalies.

Maintenance (Perfective)

Maintenance carried out to simplify or improve the system.

Management of Change (MOC)

A formal process implemented by the owner/operator, to document, review, assess the impact of and approve modifications to equipment, procedures, raw materials, process conditions, etc, other than 'replacement in kind' prior to implementation.

Maintenance/engineering interface

The hardware and software constituent parts of the safety-related system provided to allow proper maintenance and modification. It can include instructions and diagnostics which may be found in software, programming terminals with appropriate communication protocols, diagnostic tools, indicators, bypass devices, test devices, and calibration devices. This type of interface typically includes password and access protection mechanisms.

Majority voting

This technique can help to reduce the occurrence of spurious trips by ensuring that tripping only occurs when a majority of measuring devices agree that it is necessary. Majority voting systems commonly incorporate 3 trip initiator systems, where a trip will only occur if 2 of the initiators have detected a demand.

Mandatory

Implies a requirement to conform. This requirement may derive from a variety of sources, such as legislation, governmental or other regulation, or codes of practice agreed by a professional or trade association.

MAPP - Major Accident Prevention Policy

A document describing a company's policy on the prevention of major accidents, concentrating on the safety management system that will be used to put the policy into action.

Mitigation

An action to reduce the consequences of a hazardous event. An example could be emergency depressurization on detection of a fire or gas leak.

Mitigating Layer

A protection layer, which includes mechanical equipment, such as pressure relief systems, blow-out panels and instrumented systems such as safety-related systems, HIPS and reactor kill systems. This layer is designed to reduce the frequency and/or consequence severity of the hazardous event.

Mode of operation

The frequency with which a safety instrumented system will be used. There are two modes:

Low demand mode: Where a safety-related system is asked to operate no more than once per year and no greater than twice the proof test frequency

High demand or continuous mode: Where a safety-related system is asked to operate more than once per year and greater than twice the proof test frequency

Module

A reusable application code that supports a specific function. Examples are a self-contained assembly of hardware components that performs a specific hardware function or a portion of a computer program that carries out a specific function.

Modularity

An attribute of a system, which refers to its being comprised of a structure of highly independent units (or modules) that are discrete and identifiable with respect to translating, testing and combining with other units.

Moon System

A safety instrumented system made up of a number (M) of independent channels, any of which (N) are sufficient to perform the correct safety function. (IEC61508 Annex B of part 6)

MooND System

A safety instrumented system made up of a number (M) of independent channels, any of which (N) are sufficient to perform the correct safety function plus diagnostics. (IEC61508 Annex B of part 6) (Safeguard is a 1oo2D system and Triguard /Plantguard are 2oo3D systems).

MTBF – Mean Time Between Failures

The expected or observed time between consecutive failures.

MTTR - Mean Time to Repair

The expected or observed time required to repair a system or component and return it to normal operations.

N

Necessary risk reduction

The necessary risk reduction (which may be stated either qualitatively or quantitatively) is the reduction in risk that has to be achieved to meet the tolerable risk (process safety target level) for a specific situation.

Non-programmable system

A system based on non-computer hardware devices, such as hardwired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

Normative

Elements of the IEC61508 standard which must be conformed to in order to claim compliance with the standard. These elements will contain the words shall and should. Parts 1 - 4 are normative.

Notified Body

In the context of the EU, notified bodies carry out the tasks pertaining to the conformity assessment procedures referred to in the applicable New Approach directives when a third party is required. The EN 45000 series of standards and accreditation are important instruments to help in establishing conformity with the requirements of the applicable directive.

O

Operations & Maintenance (O&M)

Operation and Maintenance manuals describe the processes necessary to operate and maintain the Safety Instrumented System (SIS).

Operator interface

Components such as CRTs, indicating lights, push-buttons, horns and alarms used to communicate information between the operator and the SIS.

Other technology safety related systems

Safety related systems not based on electrical / electronic /programmable electronic technology, such as a relief valve.

Output function

A function which controls the process and its associated equipment according to information from the logic function.

Output modules

Part of the E/E/PES that acts as the interface to external device and converts output signals into signals that can actuate field devices.

P

Partial testing

Method of proof testing that checks a portion of the failures of a device, e.g. partial stroke testing of valves and simulation of input or output signals.

PFEER - Prevention of Fire & Explosion & Emergency Response Regulations 1995

Legislation relating to offshore installations. The regulations state that the person or company responsible for an installation is also responsible for protecting persons on the installation from fire and explosion and securing effective emergency response.

PHR Process Hazard Review

A team based hazard identification and risk assessment methodology used to achieve continuous safety improvement for ongoing process operations.

PLC - Programmable Logic Controller

A simple yet flexible form of process controller based on the execution of simple programmed logical instructions. (IEC61508 Annex E of part 6).

Prevention

Taking action to reduce the probability of a hazardous event.

Probability of failure on demand (PFD)

The probability of failure on demand of an item of equipment or system is the probability that the item or system will be in a failed state at sometime after a proof test when a demand is placed on the item of equipment to operate.

Probability of failure on demand average (PFDavg)

The average probability of a protective system being in a failed state. It is based on the relationship between the number of demands and the number of hazardous events and is used to describe the total time during which a component, equipment or system is incapable of providing protection. Also sometimes referred to as 'Fractional Dead Time'.

Process control system

Any instrumented system, including basic process control systems and safety instrumented systems, which act either directly or indirectly to control the process and its associated equipment.

Process demand

A process condition (event) that requires a protective system to take action to achieve or maintain a safe state of the process

Process Safety Time

The time between a failure occurring in the process or its control system and the occurrence of the hazardous event. The time for a Safety Instrumented System (SIS) to react to a hazardous event must be less than the process safety time.

Process risk

The risk existing for the specified hazardous events for the process, the basic process control system (BPCS) and associated human factors issues.

Programmable electronics (PE)

Electronic component or device, including both hardware and software and input and output units, forming part of a PES.

Programmable electronic system (PES)

System for control, protection or monitoring based on one or more programmable electronic devices, and including power supplies, sensors, data highways and other communication paths, and other output devices (IEC61508 3.3.2).

Programming

Developing a set of instructions for solving a problem or processing data.

Proof test

A periodic test performed to detect failures in a safety instrumented system so that, if necessary, the system can be restored to an "as new" condition. Failure to carry out proof-testing will result in each unrevealed fail-to-danger fault causing a subsequent dangerous event when the demand occurs.

Protection layer

Any mechanism that reduces risk by control, prevention or mitigation. It could be a mechanical engineering mechanism such as a relief valve, a safety instrumented system or an administrative procedure such as an emergency plan against an imminent hazard.

Protective System Failure

Equipment in a protective system can be affected by various types of faults. These may be categorized as:

Failure type	Consequence
<u>Fail safe</u>	<u>Spurious trip</u>
Neutral fault (e.g. failed indicator lamp)	No effect
Revealed <u>fail-to-danger</u> (e.g. indicator shows faulty measurement)	Repairs can be carried if fault is <u>detected</u>
Unrevealed <u>fail-to-danger</u> (e.g. stuck shutdown valve)	Can only be found during <u>proof-testing</u> or when system fails to operate on demand

Proven by Design

A classification of the type of claim being supported for the parameters of the sub-system, for which the evidence is based on reference to the techniques and measures employed in the design and production of the sub-system.

Proven In Use

A classification of the type of claim being supported for a sub-system requiring sufficient evidence from use to be able to establish a claim for safety performance.

PSM Process Safety Management

A standard issued by US Occupational Safety & Health Administration (OSHA) to help assure safe and healthful workplaces. OSHA has issued the Process Safety Management of Highly Hazardous Chemicals standard (1910.119), which contains requirements for the management of hazards associated with processes using highly hazardous chemicals. The standard emphasizes the management of hazards associated with highly hazardous chemicals and establishes a comprehensive management programme that integrates technologies, procedures, and management practices.

Q

QMR

Quad Modular Redundant architecture. QMR is a systems architecture that provides four separate processing paths through the system. The QMR structure has evolved from 1oo2 dual fail safe systems, where the inner pair of systems provide fail safe and the outer pair, fault tolerance.

QRA Quantified Risk Analysis

A risk analysis technique used in the process industries, involving some qualification of the probability and the severity of the hazard.

Quantified reliability

The required reliability which a trip system needs to achieve to provide the necessary level of protection in the event of a fault.

Quantified design

Design of a trip system to achieve a certain probability of failure on demand average (PFDavg) required for a SIL classification.

Quad Modular Redundant architecture

See QMR.

R

Random hardware failure

A failure, occurring at a random time, which results from a variety of degradation mechanisms in the hardware.

RDA

Refined Duplex Architecture. Safety controllers based on this architecture use two parallel control branches that act independently and with equal priority on the control decision. Any common mode of operation and any common source of failure is reduced to a minimum. Active self-tests instead of voting mechanisms reduce the probability of accumulated unrevealed dangerous failures in the system.

Reasonably foreseeable misuse

Use of a product, process or service under conditions or for purposes not intended by the supplier, but which it is expected may happen (IEC61508 3.1.11).

Recognized test organisations

See notified body.

Redundancy

An additional means of carrying out a required function, in the event the primary method suffers a malfunction.

Refined Duplex Architecture

See RDA.

Reliability

The probability that during a certain period of time a system performs the required functions under the stated conditions.

Residual risk

The risk remaining after protective measures have been taken (IEC61508 3.1.7).

Requirement

A statement of a criterion which must be met if a particular product or process etc is to be seen to be acceptable.

Risk

The combination of the probability of occurrence of harm and the severity of that harm. (IEC61508 3.1.5). As these diminish, the level of risk also diminishes.

Risk Analysis

The estimation of the risk of each hazardous event considering its frequency of occurrence and consequence severity and the identification of safeguards to reduce this risk below the owner/process operator risk criteria.

Risk assessment

A study to determine the risks for a specific hazardous event for the EUC. The determined risks would be:-

- The risk existing for the EUC, the EUC control system and associated human factor issues
- The risk which is accepted in a given context, based on current values of society
- The risk remaining after the addition of risk reduction facilities

Risk Assessment Tree

A method of determining what SIL value to apply to a given process.

Risk Based Safety Analysis

Evaluating a process for safety risks, quantifying them and categorising them as acceptable or unacceptable.

Risk Based Inspection (RBI)

Management system for identifying failure mechanisms and determining the inspection strategy for equipment based on the expected equipment degradation rate and the consequence severity if mechanical integrity is lost or equipment does not perform as expected.

Risk criteria

Qualitative or quantitative measures to determine whether a risk posed by an identified hazardous event is tolerable (or acceptable) versus intolerable (or unacceptable).

Risk estimation

A method of determining the probability of each hazard by considering their associated accidents and accident sequences.

Risk graph

A qualitative method that enables the safety integrity level of a safety instrumented function to be determined from a knowledge of the risk factors associated with the process and basic process control system. The approach uses a number of parameters which together describe the nature of the hazardous situation when safety instrumented systems fail or are not available. These parameters allow a graded assessment of the risks to be made and represent key risk assessment factors.

Risk Matrix

Qualitative or semi-qualitative representation of the risk criteria. The process owner/operator creates a matrix using broad categories to define the tolerable likelihood (or frequency) and consequence severity of identified hazardous events.

Risk Reduction

See Necessary Risk Reduction.

S

Safe failure

A failure which does not put the safety related system in a dangerous or fail-to-function state.

Safe failure fraction (SFF)

The ratio of safe failure to fail to danger.

Safe state

The state of the process when safety is achieved (IEC61508 3.1.10).

Safety

Freedom from unacceptable risk (IEC61508 3.1.8).

Safety case

A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.

Safety critical system

System used for protection when there is a high probability of an accident.

Safety function

A function intended to achieve or maintain a safe state for the process in respect of a specific hazardous event.

Safety functions requirements specification

Specification defining the safety functions that must be performed by the safety-related systems.

Safety instrumented control function

A function of an E/E/PE system needed to prevent a hazardous condition or mitigating the consequences of one arising. The function will have a specified Safety Integrity Level and operate in a high demand/continuous mode.

Safety instrumented control system

The combination of one or more safety instrumented control functions. Safety instrumented control systems are rare within the process industries.

Safety instrumented function (SIF)

A function of an E/E/PE system which is necessary to achieve functional safety. A safety instrumented function can be either a safety instrumented protection function or a safety instrumented control function.

Safety instrumented functions (SIF) requirements specification

A specification defining the safety instrumented functions that must be performed by the SIS. Specifications may be documented in text, flow diagrams, matrices, logic diagrams, etc., as long as the SIFs are clearly conveyed.

Safety instrumented loop

Any loop whose failure to operate could cause a hazard to life.

Safety instrumented protection function

A function of an E/E/PE system needed to prevent a hazardous condition or mitigating the consequences of one arising. The function will have a specified Safety Integrity Level and operate in a low demand mode.

Safety Instrumented System (SIS)

A combination of one or more safety instrumented functions. A SIS is composed of sensor(s), logic solver(s), and final element(s). It can include either safety instrumented control functions or safety instrumented protection functions, or both.

Safety integrity

The probability that a safety instrumented function will perform the required actions under all the stated conditions within a stated period of time.

Safety Integrity Level (SIL)

Safety functions are assigned one of four Safety Integrity Levels. Safety Integrity Level 4 has the highest level of safety integrity, while Safety Integrity Level 1 has the lowest. (*IEC61508* 3.5.6). These levels are defined in terms of the required probability of failure on demand average (PFDavg) (i.e. the average probability that the system will be in a failed state when a demand occurs). See also SIL 1, SIL 2, SIL 3, SIL 4.

Safety integrity requirements specification

Specification that contains the safety integrity requirements of the safety instrumented functions that must be performed by the safety instrumented system(s).

Safety lifecycle

The necessary activities involved in the implementation of safety instrumented function(s) occurring during a period of time that starts at the concept phase of a project and finishes when all of the safety instrumented functions are no longer available for use. The safety life cycle embraces the entire supply chain and has an impact on engineers within all disciplines.

Safety Life Cycle Management Plan

A key safety project deliverable which defines the safety lifecycle model to be used and how the organisation's FSMS will be implemented on the specific project. It includes management responsibilities, processes and procedures to be adhered to, deliverables to be produced, review, audit and assessment activities.

Safety manual

Compilation of configuration, installation, maintenance and support requirements for equipment typically certified under a third-party accredited product certification scheme. The safety manual contains essential (mandatory) information to be complied with when using the equipment. Failure to comply can nullify the certification of the product. Safety manuals are typically associated with 'compliant items' that is those items the manufacturer is claiming compliance to the requirements of *IEC 61508*. The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard.

The safety manual specifies the functions of the compliant item. These may be used to support a safety function of a safety-related system or functions in a subsystem or element. The specification should clearly describe both the functions and the input and output interfaces.

Safety related software

Software that is used to implement safety instrumented functions in a safety instrumented system.

Safety related system

A system designed to reduce the frequency (probability) of the hazardous event and/or the consequences of a hazardous event.

Safety report

As set out in schedule 4 of the COMAH regulations, this must include:-

- A policy on how to prevent and mitigate major accidents
- A management system for implementing that policy
- An effective method for identifying any major accidents that might occur
- Measures (such as safe plant and operating procedures) to prevent and mitigate major accidents
- Information on the safety precautions built into the plant and equipment when it was designed and constructed
- Details of measures (such as fire fighting, relief systems and filters) to limit the consequences of any major accident that might occur
- Information about the emergency plan for the site, which is also used by the local authority in drawing up an offsite emergency plan

Safety requirements specification (SRS)

The SRS is a compilation of information found in the Process Hazards Analysis report, logic diagram, process technology documents, P&ID, SIL determination, etc, including the specification and description of each safety function and for each safety function its target safety integrity level.

Safety software

The software that forms an integral part of a safety instrumented system.

Safety validation

Assurance that software or equipment has been developed using best practice and is suitable for use in safety critical applications.

SAT

Site Acceptance Test – a series of tests conducted on the client/operator's site to determine and document that a new or modified instrumented protective system meets the design basis, is installed in accordance with construction, installation, and software requirements, and is ready for plant commissioning.

Sensor

A device or combination of devices that measures the process condition. These can include devices such as transmitters, process switches, position switches, etc.

SEVESO II EU

Directive 96/82/EC, also known as the Seveso II Directive, aims to prevent, or limit the consequences of, major accidents for people and the environment near establishments that hold or use specific dangerous substances. It is implemented in Great Britain through the Control of Major Accident Hazards (COMAH) Regulations.

Shall

Used to indicate that a requirement must be strictly followed if compliance to the standard is to be claimed.

Should (or it is recommended that)

Indicates a course of action that is preferred over others but not necessarily required.

SIL

See Safety Integrity Level

SIL Achievement

An activity whose objective is the demonstration that for each Safety Instrumented Function (SIF), the target SIL, as derived from SIL determination, has been met in accordance with the requirements of IEC61508. Achievement of SIL, for a safety instrumented function, is dependent on the following parameters:

- Architectural Constraint, in terms of:
 - Safe Failure Fraction (SFF) and
 - Hardware Fault Tolerance (HFT)
- Target Failure Measure, expressed as either:
 - Pfd, or
 - Dangerous Failure Rate
- Systematic Capability, in terms of:
 - Each element that carries out the safety function
 - The method by which the safety instrumented function was designed and implemented

SIL 1

These systems have a probability of failure on demand (PFDavg) of 0.1 – 0.01. This performance can be realised by simple systems usually without resorting to redundancy. They use conventional quality materials and good design practices which are described in the requirement specification procedure. The majority of systems which are quantified are of this grade.

SIL 2

These systems have a probability of failure on demand (PFDavg) of 0.01 – 0.001. To achieve this grade of reliability, systems should be very carefully designed. Use may be made of redundancy, e.g. two identical process measurements, or trip mechanisms. Likely sources of common cause fail-to-danger should be identified and eliminated. The features of SIL 2 systems are described in the requirement specification procedure.

SIL 3

These systems have a probability of failure on demand (PFDavg) of less than 0.001 – 0.0001. This grade of reliability is extremely difficult to achieve and maintain. For this reason it should be recognised that the design of such systems require specialist techniques, which may be

the experience and formal training accessed from the recognised competent engineers with SIL 3 design experience. The features of SIL 3 systems are described in the requirement specification procedure. Such systems are extremely rare in the process industries.

SIL 4

These systems have a probability of failure on demand (PFDavg) of 0.0001 – 0.00001. SIL 4 is the highest level of safety integrity considered necessary. It covers any process where any failure would have a catastrophic effect on the surrounding environment and/or community.

SIL Capability

A measure (expressed on a scale of 1 to 4) of the confidence that an element safety function will not fail due to relevant systematic failure mechanisms when the element is applied in accordance with the instructions specified in the element safety manual.

SIL determination

An activity whose objective is to specify the safety instrumented function (SIF) and determine and specify the target SIL for each safety instrumented function. It is an assessment of the risk reduction required to give a tolerable level of risk. SIL determination typically utilises methods such as Calibrated Risk Graphs and Layer of Protection Analysis (LOPA).

Site Acceptance Test

See SAT.

Software

The programs, procedures, data, rules and any associated documentation pertaining to the operation of a data processing system.

Software functional safety assessment

The process of investigating and arriving at a judgement on the functional safety achieved by the E/E/PES safety-related systems.

Software lifecycle

The range of activities occurring during the life of a unit of software, from conception to permanent disuse.

Software safety integrity

A measure of the likelihood that software will achieve its safety instrumented functions under all stated conditions within a stated period of time.

Software safety integrity level

One of four possible discrete levels for specifying the safety integrity of software in a safety instrumented function.

Software template

Algorithm or collection of algorithms that have been programmed to perform a desired function or set of functions, constructed so it can be used in many different instances.

Software Safety Validation

The process to ensure that the integrated system complies with the specified requirements for software safety at the intended safety integrity level.

Software verification

To the extent required by the safety integrity level, to test and evaluate the outputs from a given software safety lifecycle phase to ensure correctness and consistency with respect to the outputs and standards provided as input to that phase.

SOUP

Software Of Uncertain Pedigree, e.g. commercial operating systems, user interfaces, system libraries, compilers, medical devices and alarm systems. Such software might have been designed specifically for safety-related tasks or be a product that was used in non-safety applications. It is often generic and likely to contain functions that are unnecessary for the system application and subject to continuous change. Quite often, access to design documentation and source code is difficult.

Spurious trip

Expected rate (number of trips per unit time) at which a process shutdown, or disruption, occurs due to the spurious operation of equipment. Other terms used include nuisance trip rate and false shutdown rate

Stage

Point within the safety-lifecycle before or following a phase at which functional safety assessment activities are to be carried out.

Standard

A document which establishes criteria by which the qualities of products or processes may be objectively assessed; each criterion involves a requirement. Standards of this kind are specifically referred to as normative standards.

Subsystem

Entity of the top-level architectural design of a safety-related system where a failure of the subsystem results in a failure of a safety function. A subsystem may consist of a single element or many elements.

System

Set of elements, which interact according to their design. An element of a system can be another system, called a subsystem.

Systematic failure

Failure due to some fundamental error in the design of the system.

Systematic Fault Avoidance Measures

A description of those measures and techniques used to prevent systematic faults being introduced during the design and implementation of the hardware and software subsystem.

Systematic Fault Tolerance Measures

Description of the design features which make the subsystem tolerant against systematic faults.

Systematic safety integrity

Part of the safety integrity of a safety-related system relating to systematic failures in a dangerous mode of failure.

T

Target failure measure

The intended probability of dangerous mode failures. It is specified in terms of either: the average probability of failure to perform the design function on demand (for a low demand mode of operation); or the probability of a dangerous failure per hour (for a high demand or continuous mode of operation).

Template

Application software that can be easily altered to support specific functions, while retaining the original structure.

Test bed

An environment, containing the hardware, instrumentation, simulators, software tools, and other support elements needed to conduct a test.

Test coverage

The degree to which a given test or set of tests addresses all specified requirements for a given system or component.

Test harness

A facility that can simulate the operating environment of software or hardware under development by applying test cases to the software and recording the response.

TMR

Triple Modular Redundant architecture. TMR is a fully triplicated system architecture from input module to output module. It is designed to achieve the highest possible levels of reliability, safety and availability.

TMR¹ was originally invented by August Systems, which became the first to prove that three microprocessors could carry out a single valid control action. This development effort was a result of the NASA space programme in the United States.

The original application of the TMR technology was in Critical Control and Safeguarding systems. This technology was later applied to Emergency Shutdown Systems (ESD) and Fire & Gas systems (F&G) in the oil and gas, refining and petrochemical industries.

Tolerable risk

A risk which is accepted in a given context, based on the current values of society (IEC61508 3.1.6).

Trip

The action of a trip system to prevent a plant fault condition from developing into a hazardous event. Operator action is required to reset the trip when normal conditions have been restored.

Trip initiator

A device which generates a signal to the logic system to initiate a trip in response to a plant fault condition.

Trip system

A device comprised of one or more trip initiators, a logic or relay element and one or more trip mechanisms. The trip system cannot be reset until plant conditions have been restored to a satisfactory state. Resetting the trip system will normally be performed manually by an operator.

Trip system functional auditing

Trip system functional auditing should be periodically carried out to check that a trip system is being maintained, operated and tested to ensure it can deliver the desired levels of performance for the application.

Triple Modular Redundant architecture

See TMR.

TÜV

Third party accredited certification organizations (e.g. TÜV Rheinland) implementing formal certification schemes used to demonstrate compliance to IEC61508 and IEC61511, comprising of functional safety management systems (FSMS) assessments and safety product assessments. ABB's products and functional safety management systems are certified by TÜV.

U

Undetected, unrevealed, covert

In relation to hardware and software, undetected by the diagnostic tests, proof test, operator intervention (for example, physical inspection and manual tests), or through normal operation. Faults of this type will remain hidden until revealed by a demand or proof test.

Utility software

Software tools used for the creation, modification, and documentation of application programs; not required for the operation of the SIS.

V

Validation

The activity of demonstrating that the safety-related system under consideration, before or after installation, meets in all respects the safety requirements specification for that safety-related system. Validation involves consideration of whether the specification of a system sufficiently and accurately represents the needs of the intending user.

Verification

The activity of demonstrating for each phase of the relevant safety lifecycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

Verification Body

The group of competent personnel who have responsibility for performing independent verification activities on a safety project.

Version Management

Documents, hardware and applications software covered under a revision control system. Documents and Applications Software contain revision histories to ensure that changes from initial creation through to current version are traceable and quantifiable. For hardware, module serial number and version are recorded to ensure future replacements and upgrades can be planned and impact of the change assessed.

Voting

Specific configuration of equipment within a subsystem. Voting is often expressed as MooN (M out of N). 'N' designates the total number of devices (or channels) implemented. 'M' designates the minimum number of devices (or channels) out of N required to initiate, take, or maintain the safe state.

W

Watchdog

A combination of diagnostics and an output device (typically a switch) for monitoring the correct operation of the programmable electronic PE device and taking action when an incorrect operation is detected.

White Communication Channel

A communications channel connected to safety-related system elements, such that the entire communications channel including its interfaces complies with the requirements of IEC 61508. The connecting elements also comply fully with the requirements of IEC 61508. A white channel does not contribute to the overall system probability of failure as it will detect and correct for any failures induced by the communications channel.

X

Y

Z