ABB FSM TECHNICAL AUTHORITY

Functional safety jargon buster

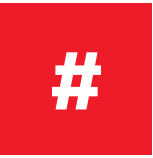
An explanation of terminology

—

ABB functional safety jargon buster explains some of the terminology users are likely to encounter when purchasing or handling safety devices and systems for process applications. If you have a specific question relating to any aspect of process safety and design, please email oilandgas@gb.abb.com. Alternatively, you can contact ABB's global functional safety specialists network for advice via +44 (0)1480 475321.

ABB's functional 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.

Contents



1ooN system
Usually used for a subsystem of Safety Instrumented Function (SIF) and its ability to perform the safety function. In this context the architecture consists of N channels connected, such that either channel can process the safety function. This system is N minus 1 fault tolerant e.g. 1oo2 is single fault tolerant (HFT=1).

2ooN system
Usually used for a subsystem of a SIF and its ability to perform the safety function. In this context the architecture consists of N channels connected such that at least two channels are required to process the safety function. This system is N minus 2 fault tolerant e.g. 2oo4 is double fault tolerant (HFT=2).

A

Acceptable risk
The terms ‘acceptable risk’ and ‘tolerable risk’ are considered to be synonymous. Tolerable risk is the level of risk which is accepted in a given context based on the current values of society.

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 ALARP. (IEC 61508 Annex B of part 5).

ANSI
American National Standards Institute.

Application program
The software that forms an integral part of a SIS.

Application program - pre-existing
Existing software already available and not developed specifically for a new project or safety related system.

Application program life-cycle
Activities occurring during a period of time that starts when the application program is conceived and ends when the application program is permanently disused. An application program life-cycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase and modification phase. Software, including application program, cannot be maintained; rather, it is modified.

Application programming languages
- Fixed program language (FPL) language in which the user is limited to adjustment of a few pre-defined and fixed set of parameters
- Limited variability language (LVL) programming language for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application as defined by the associated safety manual
- Full variability language (FVL) language designed to be comprehensible to computer programmers and that provides the capability to implement a wide variety of functions and applications

Approved Code of Practice (ACOP)
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 devices list
A list developed by an asset owner consisting of devices that on the basis of positive history of operation are approved for use in their facility. Any devices that have had a history of not performing as desired, will have been removed from this list.

Architecture
The physical organisation, interconnection, or integration of the 'hardware and software elements' of a 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 independently 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
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 and operate within specified limits when required for use. This is a measure of the 'uptime' and is defined in units of percent. Availability is a function of failure rates and repair rates.

Average probability of failure
The average probability of failure on demand (PFDavg) of an item of equipment or system is the probability that a device 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 PFDavg 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 from the process, its associated equipment, other programmable systems and/or operators and generates output signals causing the process and its associated equipment to operate in the desired manner but which does not perform any safety instrumented function.

Beta factor
Factor in units of percent indicating common cause failure susceptibility. It is the fraction of failure rates that is attributed to single cause which results in simultaneous failure of all devices within the voting group e.g. over temperature in an area where 2oo3 voted flow transmitters are installed can lead to simultaneous failure of all 3 devices.

Black-box testing
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 recognized 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 (and assists the operator in starting and stopping the burners and prevents mis-operation and damage the the fuel preparation and burner equipment) and that can monitor the 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 or facility to prevent all or parts of the SIS functionality from being executed. 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 organizations such as ABB.

CENELEC - European Committee for Electrotechnical Standardization
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
Device or group of devices that independently perform(s) a specified function. The devices within a channel could include input / output (I/O) devices, logic solvers, sensors, and final elements.

CHAZOP
Computer HAZOP A process covering criticality and failure review of complex programmable electronic systems, including Cyber security and assessment to determine the potential for malevolence threats to the automation 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 (COTS)
A commercially available product (hardware, software, system and services) that can be bought and used under government contract. COTS typically requires configuration that is tailored for specific uses and the key characteristic that differentiates COTS from customized product.

Common cause failures
Concurrent failures of different devices, resulting from a single event, where these failures are not consequences of each other. All the failures due to a common cause do not necessarily occur exactly at the same time and this may allow time to detect the occurrence of the common cause before a SIF is actually failed. Common cause failures can also lead to common mode failures.

Common mode failure
Concurrent failures of different devices characterized by the same failure mode (i.e. identical faults). Common mode failures may have different causes and common mode failures can also be the result of common cause failures.

Compensating measure
Temporary implementation of planned and documented methods for managing risks during any period of maintenance or process operation when it is known that the performance of the SIS is degraded.

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 specific configuration of hardware and software components in a system e.g. arrangement of SIS subsystems, the internal structure of a SIS subsystem or the internal structure of SIS application programs.

Configuration 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.

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
Continuous mode of operation is where the SIF retains the process in a safe state as part of normal operation.

Control system
A system that responds to input signals from the plant and/or an operator and causes the plant or equipment to operate in the desired manner. Control systems usually involve one or more input devices, a controller, one or more output devices, power supplies, and any associated information connections. If the control system has a safety role, either as an integral part of the process plant or as a separate protection system, it will be a safety-related system.

Cyber security
Cyber security is the sum of efforts invested in addressing cyber threats. Processes and practices to protect networks, computers, programs and data from attack, damage or unauthorized access.

D

Dangerous failure
A failure which impedes or disables a given safety action. A failure is 'dangerous' only with regard to a given SIF. When fault tolerance is implemented, a dangerous failure can lead to either:

- A degraded SIF where the safety action is available but there is either a higher PFD (demand mode of operation) or a higher likelihood of initiating an hazardous event (continuous mode of operation), or
- A disabled SIF where the safety action is completely disabled (demand mode of operation) or the hazardous event has been induced (continuous mode of operation)

De-energize to trip
Circuits where the final elements are energized under normal operation and the removal of power source (e.g. electricity, instrument air) causes the safety instrumented function (SIF) to take its defined action.

Defeat
See Bypass

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

Demand mode
A SIF operating in either low demand mode or high demand mode.

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, i.e. two events A and B are dependent, only if: P(A and B) > P(A) × P(B).

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

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

Detected, revealed, overt
Relating to hardware and software failures or faults which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods

- Overt is used for failures or faults which announce themselves when they occur
- Detected is used for failures or faults which do not announce themselves when they occur and which remain hidden until detected by some means
- Revealed is used for failures or faults that become evident due to being overt or as a result of being detected

Device
Hardware, with or without software, capable of performing a specified function.

Diagnostic coverage
Fraction of dangerous failures rates detected by diagnostics. Diagnostics coverage does not include any faults detected by proof 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. Diversity may be achieved by different physical means, different programming techniques, or different design approaches.

E

Electrical / electronic / programmable electronic (E/E/PE)
Devices based on electrical and/or electronic and/or programmable electronic technology.

Electrical / electronic / programmable electronic system (E/E/PES)
A system for control, protection or monitoring based on one or more E/E/PE devices.

Electromagnetic immunity
See EMI

Element
An IEC 61508 term used to define a 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.

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.

Energize 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 energize 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
Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretically correct value or condition.

EUC - Equipment under control
Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

Event tree analysis
A method of fault propagation modeling. The analysis constructs a tree-shaped picture of the chain of events leading from an initial event to various potential outcomes.

External communication
Data exchange between an Safety Instrumented Function (SIF) 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. A characteristic of a device which causes a device to move to a safe state when it loses energy e.g. electrical, pneumatic, hydraulic etc.

Failure
Loss of ability to perform as required. A failure of a device is an event that results in a fault state of that device and such failures are either random or systematic.

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
Inability to perform as required, due to an internal state A fault of an item results from a failure, either of the item itself, or from a deficiency in an earlier stage of the lifecycle, such as specification, design, manufacture or maintenance. A fault of a device results in a failure when a particular set of circumstances is encountered.

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.

FDRT
Fault Detection Reaction Time

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 SIS or BPCS device connected directly to the process or located near the process which directly prevents the hazardous event from occurring and brings the process to a safe state (protection function) or mitigates a hazardous event (mitigation function). Examples are valves and switch gear, which can be used to put the process plant into 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 Safety Instrumented Function (SIF) 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
Part of the overall safety relating to the process and the BPCS which depends on the correct functioning of the SIS and other protection layers.

Functional safety assessment
An investigation, based on evidence, to judge the functional safety achieved by one or more SIS and/or other protection layers.

Functional safety audit
A systematic and independent examination to determine whether the procedures specific to the functional safety requirements comply with the planned arrangements, are implemented effectively and are suitable to achieve the specified objectives. A functional safety audit may be carried out as part of a FSA.

Functional Safety Management System (FSMS)
The set of policy and strategy with the methods for evaluating their achievement, processes, procedures, templates, checklists, techniques and measures, etc, specific to an organization 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) that are necessary to ensure the functional safety objectives are met. FSM is solely aimed at the achievement and maintenance of the functional safety of SIS.

Functional test
Test in which the system is exposed to different factors simulating service conditions, in order to obtain information about service ability including evaluation of test results. Note that subsystem which is composed of devices voted in fault tolerance configuration can provide a designed function however it does not mean every channel is functional. A proof test aims in restoring the system to an 'as new' condition so it checks functionality of each channel in any subsystem configuration.

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

G

Grey channel
A non-safety critical communication line between two modules that are regarded as safety critical.

H

Hardware fault tolerance
The ability of a functional item to continue to perform the required Safety Instrumented Function (SIF) in the presence of one or more dangerous faults or errors in hardware.

Hardware safety integrity
Part of the safety integrity of the SIS relating to random hardware failures in a dangerous mode of failure. The two failure measures that are relevant in this context are the average frequency of dangerous failure (continuous mode of operation) and the average probability of failure on demand (demand mode of operation).

Harm
Physical injury or damage to the health of people, or damage to property or to the environment.

Harmful event
Hazardous event which has caused harm. Whether or not a hazardous event results in harm depends on whether people, property, or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred. A hazardous event which has caused harm is termed a harmful event.

Harmonized European Standard
A European standard prepared by CEN/CENELEC under a mandate from the Commission, with a view to the fulfillment of the essential requirements (ESR) of a new approach directive. The term harmonized standard shows a direct connection to the compliance with new approach directives.

Hazard
Potential source of harm, to people, the environment or damage to property. The term includes danger to persons arising within a short time scale (e.g. fire and explosion) and also those that have a long-term effect on a person's health (e.g. release of a toxic substance or radioactivity).

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.

Hazardous event
Hazardous situation that can cause harm. Whether or not a hazardous event results in harm depends on whether people, property or the environment are exposed to the hazardous situation and, in the case of harm to people, whether any such exposed people can escape the consequences of the event after it has occurred.

Hazardous situation
Circumstance in which people, property or the environment are exposed to one or more hazards.

HAZOP - Hazard and Operability study
A process hazards analysis procedure which considers the effects of deviation from the normal operating intent by identifying basic causes, their immediate effects and the resultant consequences.

Hazard and risk assessment
The process of identifying hazards and hazardous event of the process and associated equipment in all modes of operation, the sequence of events leading to the hazardous event, and the EUC process risks associated with the hazardous event, requirements for risk reduction, the safety functions required to achieve the necessary risk reduction and if any of the safety functions are SIFs.

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
Intended or unintended human action or inaction that produces an inappropriate result.

Human factors
Human factors refer to the environmental, organisational, job factors and human individual charateristics, which influence behaviour at work in a way which can affect health and safety.

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

IEC 61508
This is a basic safety publication. A major objective is to facilitate the development of product and application sector international standards based on the IEC 61508 series. This standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic elements that are used to perform safety functions which reduce risk to a tolerable level.

IEC 61511
IEC 61511 is a three-part international standard concerned with functional safety instrumented systems for the process industry. It covers process hazard and risk assessment, and 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 organization
Organization which is separate from the organizations 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 Protection Layer (IPL)
Any independent mechanism that reduces risk by control, prevention or mitigation. It can be a process engineering mechanism such as the size of vessels containing hazardous chemicals, a mechanical mechanism such as a relief valve, a SIS or an administrative procedure such as an emergency plan against an imminent hazard. These responses may be automated or initiated by human actions.

Informative
Elements of the IEC 61508 and IEC 61511 standards which provide additional information to assist in the understanding or use of the standards.

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 utilize.

Instrument
Apparatus used in performing an action typically found in instrumented systems.

Instrumented system
A system composed of sensors (e.g. pressure, flow, temperature transmitters), logic solvers (e.g. programmable controllers, distributed control systems, discrete controllers), and final elements (e.g. control valves, motor control circuits)

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.

L

Layers of Protection Analysis (LOPA)
A method of analyzing the frequency of harmful event based on frequency of impact event and probability of failure of independent protection layers and additional factors such as person occupancy in hazardous zone or a person unable to escape consequences.

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)
A programming language for commercial and industrial programmable electronic controllers with a range of capabilities limited to their application as defined by the associated safety manual. This type of language is designed to be easily understood by process sector users, and provides the capability to combine predefined, application specific, library functions to implement the SRS. LVL provides a close functional correspondence with the functions required to achieve the application.

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 performs the transformations between input information (provided by one or more input functions) and output information (used by one or more output functions). Logic functions provide the transformation from one or more input functions to one or more output functions.

Logic solver
A device forming part of either a BPCS or SIS that performs one or more logic function(s) Examples are: electrical systems, electronic systems, programmable electronic systems, pneumatic systems, and hydraulic systems. Sensors and final elements are not part of the logic solver.

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 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 behavior of the system under fault conditions can be completely determined.

Low demand mode
Mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year.

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 to review implemented by owner/operators, to document, 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 consequences of the hazardous event.

Mode of operation
The way in which a SIF operates which may be either low demand mode, high demand mode or continuous mode.

a. Low demand mode: mode of operation where the SIF is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is no greater than one per year
b. High demand mode: mode of operation where the SIF, is only performed on demand, in order to transfer the process into a specified safe state, and where the frequency of demands is greater than one per year
c. Continuous mode: mode of operation where the SIF retains the process in a safe state as part of normal operation

Module
A reusable part of a SIS application program (can be internal to the program or set of programs) that performs a specified 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 (e.g. final element start / stop / test sequence).

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.

ModPack
A ModPack is an extensive package of modifications additional to the original scope of the safety related project (not a single small modification).

MooN
A SIS or part thereof made up of (N) independent channels, which are so connected, that (M) are sufficient to perform the SIS (IEC 61511-1 ed2 3.2.41).

MooND
A SIS or part thereof made up of (N) of independent channels, which are so connected that (M) are sufficient to perform the correct safety instrumented function with additional diagnostic capability and additional channels wired in series to utilize the diagnostic signal to de-energise the channel output. (IEC61508 Annex B of part 6) (Safeguard is a 1oo2D system and Triguard /Plantguard are 2oo3D systems).

MRT - Mean Repair Time
The expected overall repair time. MRT encompasses:

- The time spent before starting the repair
- The effective time to repair
- The time before the component is put back into operation

MTBF - Mean Time Between Failures
The expected or observed time between consecutive failures.

MTTR - Mean Time to Restoration
The expected or observed time required to repair a system or component and return it to normal operations. MTTR encompasses:

a. The time to detect the failure
b. The time spent before starting the repair
c. The effective time to repair
d. The time before the component is put back into operation

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

N

Necessary risk reduction
Risk reduction to be achieved by the SIS(s) and/or other protection layers to ensure that the tolerable risk is not exceeded.

Non-programmable system
A system based on non-computer hardware devices (i.e. a system not based on programmable electronics [PE] or software), such as hardwired electrical or electronic systems, mechanical, hydraulic, or pneumatic systems.

Normative
Parts or clauses of the IEC safety standards which must be conformed to in order to claim compliance with the standard. These elements will contain the words shall and should.

Notified body
A notified body, in the European Union, is an organization that has been accredited by a member state to assess whether a product meets certain preordained standards. Assessment can include inspection and examination of a product, its design and manufacture.

O

Operations and Maintenance (O&M)
Operation and Maintenance manuals describe the processes necessary to operate and maintain the SIS. The key requirement for an organization responsible for operation and maintenance of the SIS is to maintain the designed functionality and safety integrity of the SIS during the whole operation and maintenance phase.

Operating environment
The conditions inherent to the installation of a device that potentially affects its functionality and safety integrity, such as:

- External environment, e.g. winterization needs, hazardous area classification
- Process operating conditions, e.g. extremes in temperature, pressure, vibration
- Process composition, e.g. solids, salts or corrosives
- Process interfaces
- Integration within the overall plant maintenance and operating management systems
- Communication through-put, e.g. electro-magnetic interference
- Utility quality, e.g. electrical power, air, hydraulics

Operating mode
The process operating mode for any planned state of process operation, including modes such as start-up after emergency shutdown, normal start-up, operation, and shutdown, temporary operations, and emergency operation and shutdown.

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

OSP - Output Set as Predefined

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.

Phase
The period within the SIS safety lifecycle where activities described in the IEC 61511 series take place.

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 Dangerous Failure on Demand (PFD)
Unavailability of the system to perform the specified safety function when a demand occurs.

1. There are two types of demands for the system: proof test and safety demand (on hazardous event)
2. The [instantaneous] unavailability is the probability that an item is not in a state to perform a required function under given conditions at a given instant of time
3. If periodically tested, the PFD of a SIF is represented by a saw tooth curve with a large range of probabilities ranging from low, just after a test, to a maximum, just before a test

Probability of Dangerous Failure on Demand Average (PFDavg)
Average unavailability over a given interval

1. “Failure on demand” means the “failure likely to be observed when a demand occurs”
2. There are two types of demands for the system: proof test and safety demand (on hazardous event).
3. PFDavg encompasses both the failure occurred before the demand and the failure occurring due to the demand itself

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 period between a failure occurring in the process or the basic process control system (with the potential to give rise to a hazardous event) and the occurrence of the hazardous event if the SIF is not performed. This is a property of the process only. The SIF has to detect the failure and complete its action soon enough to prevent the hazardous event taking into account any process lag (e.g. cooling of a vessel).

Process risk
The risk arising from the process conditions caused by abnormal events (including BPCS malfunction). The risk in this context is that associated with the specific hazardous event in which SIS are to be used to provide the necessary risk reduction (i.e. the risk associated with functional safety).

Programmable Electronics (PE)
Item based on computer technology which may be comprised of hardware, software, and of input and/or output units. This term covers micro-electronic devices based on one or more central processing units (CPU) together with associated memories.

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.

Programming
Programming coding process of designing, writing and testing a set of instructions for solving a problem or processing data.

Proof test
Periodic test performed to detect dangerous hidden faults in a SIS so that, if necessary, a repair can restore the system to an ‘as new’ condition or as close as practical to this condition.

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

Failure type	Consequence
Fail safe	Spurious trip
Neutral fault (e.g. failed indicator lamp)	No effect
Revealed fail-to-danger (e.g. indicator shows faulty measurement)	Repairs can be carried if fault is detected
Unrevealed fail-to-danger (e.g. stuck shutdown valve)	Can only be found dueing prooftesting 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.

Prior use
The main intent of the prior use evaluation is to gather evidence that the dangerous systematic faults have been reduced to a sufficiently low level compared to the required safety integrity. Prior use data can contribute to a database for the calculation of hardware failure rates. This type of assessment is made by end user. It is based on data collected from operation of a specific device in a specific environment and process condition. It is a site specific approach.

Proven in use
Demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required SIL. This type of assessment is made by the device manufacturer and is based on field returned data so does not address any specific end user environmental and process conditions. The input data base is also limited to failures which are communicated to manufacturer by the end user. It is product specific approach.

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 PSM 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 program that integrates technologies, procedures, and management practices.

Q

Quality
The totality of characteristics of an entity that bear on its ability to satisfy stated and implied needs.

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.

R

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.

Recognized test organizations
See notified body.

Redundancy
The existence of more than one means for performing a required function or for representing information. Redundancy is used primarily to improve reliability or availability.

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.

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. As these diminish, the level of risk also diminishes. The probability of occurrence includes the exposure to a hazardous situation, the occurrence of a hazardous event, and the possibility to avoid or limit the harm.

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 categorizing 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 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 favours a given safety action. A failure is 'safe' only with regard to a given safety function. When fault tolerance is implemented, safe failure can lead to either:

- Operation where the safety action is available but with a higher probability of success on demand (demand mode of operation) or a lower likelihood to cause a hazardous event (continuous mode of operation)
- A spurious operation where the safety action is initiated

When no fault tolerance is implemented, safe failures result in the initiation of the safety action regardless of the process condition. This is also known as a spurious trip. A spurious trip may be safe with regard to a given safety function but may be dangerous with regard to another safety function.

Safe Failure Fraction (SFF)
The property of a safety related element that is defined by the ratio of the average failure rates of safe plus dangerous detected failures and safe plus dangerous failures.

Safe state
The state of the process when safety is achieved.

Safety
Freedom from unacceptable risk.

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 requirements specification
The specification containing the functional requirements for the SIFs and their associated SIL.

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 SIL 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 safety function to be implemented by a SIS. A SIF is designed to achieve a required SIL which is determined in relationship with the other protection layers participating to the reduction of the same risk.

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 SIL and operate in a high and low demand mode.

Safety Instrumented System (SIS)
A system composed of sensors (e.g. pressure, flow, temperature transmitters), logic solvers (e.g. programmable controllers, distributed control systems, discrete controllers), and final elements (e.g. control valves, motor control circuits) used to implement one or more SIFs. A SIS is composed of any combination of sensor(s), logic solver(s), and final elements(s). It also includes communication and ancillary equipment (e.g. cables, tubing, power supply, impulse lines, heat tracing).

Safety Instrumented System (SIS) - safety lifecycle
The necessary activities involved in the implementation of SIFs occurring during a period of time that starts at the concept phase of a project and finishes when all of the SIF are no longer available for use. The safety lifecycle embraces the entire supply chain and has an impact on engineers within all disciplines.

Safety integrity
The ability of the SIS to perform the required SIF as and when required.

Safety Integrity Level (SIL)
Discrete level (one out of four) allocated to the SIF for specifying the safety integrity requirements to be achieved by the SIS.

Safety life cycle management plan
A key safety project deliverable which defines the safety lifecycle model to be used and how the organizations 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
This is documented information that defines how a SIS device, subsystem or system can be safely applied. 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.

Safety related software
Application program 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)
This is a specification containing the functional requirements for the SIFs and their associated safety integrity levels. The SRS is a compilation of information found in the PHA 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 SIL.

Safety validation
Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled.

SAT - Site Acceptance Test
A series of tests conducted on the client / operators site to determine, document and validate that a new or modified system meets the design basis, is installed in accordance with construction, installation, and software requirements, and is ready for plant commissioning.

Sensor
Part of the BPCS or SIS that measures or detects the process condition. Examples are transmitters, transducers, process switches, and position switches.

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 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 verification
An activity whose objective is the demonstration that for each SIF, the target SIL, as derived from SIL determination, has been met. SIL verification comprises an assessment of safety function, hardware safety integrity and systematic safety integrity in accordance with the requirements of the safety requirements specification (SRS).

SIL capability
A measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual.

SIL determination
An activity which refers to two safety life-cycle phases i.e. Hazard and risk assessment and allocation of safety functions to protection layers, whose objective is to specify the SIF and determine and specify the target SIL for each SIF. It is an assessment of the risk reduction required to give a tolerable level of risk. SIL determination may utilize methods such as calibrated risk graphs and LOPA.

SIS subsystem
An independent part of a SIS whose disabling dangerous failure results in a disabling dangerous failure of the SIS. A SIS is basically made of three SIS subsystems: Sensors, logic solver and final elements.

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 and program types:

- Application program
  Program specific to the user application containing, in general, logic sequences, permissives, limits and expressions that control the input, output, calculations, and decisions necessary to meet the SIS functional requirements
- Embedded software
  Software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user. Embedded software is also referred to as firmware or system software. See full variability language
- Utility software
  Software tools for the creation, modification, and documentation of application programs. These software tools are not required for the operation of the SIS

Software functional safety assessment
The process of investigating and arriving at a judgement on the functional safety achieved by the SIS.

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 (SIL)
One of four possible discrete levels for specifying the safety integrity of software in a SIF.

Software support tool
Tools which can be used either on-line, or off-line and that directly, or indirectly contribute to the development, testing and verification of executable software code. Refer also to T rating.

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
When no fault tolerance is implemented, safe failures result in the initiation of the safety action regardless of the process condition. A spurious trip may be safe with regard to a given safety function but may be dangerous with regard to another safety function. Spurious trips may also have detrimental effects on the production availability of the process.

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.

System
Set of devices, which interact according to a specification. Note a person can be part of a system.

Systematic capability measure
(Expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of a device meets the requirements of the specified SIL, in respect of the specified safety function, when the device is applied in accordance with the instructions specified in the device safety manual.

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.

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 SIF on demand for demand mode of operation or the average frequency of a dangerous failure for 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.

Tolerable risk
Level of risk which is accepted in a given context, based on the current values of society.

Trip
The action of a trip system to prevent a plant fault condition from developing into a hazardous event. Usually operator action is required to rest 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 system 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

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. Some failures are undetected by diagnostic test but are detected by a proof test (depending of diagnostic coverage), other failures are undetected by a proof test (depending of the proof test coverage), others failures can remain undetected until revealed by a real process demand.

Utility software
Software tools used for the creation, modification, and documentation of application programs; not required for the operation of the SIS, refer also to ‘T rating’.

V

Validation
Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled and for demonstrating that the SIF(s) and SIS after installation meet the SRS in all respects.

Verification
The activity of demonstrating for each phase of the relevant SIS 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.

Voting
Specific configuration of devices 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.

ABB FSM Technical Authority
Howard Road
Eaton Socon
St Neots
Cambridgeshire
PE19 8EU
United Kingdom
Phone: +44 (0)1480 475321
E-Mail: oilandgas@gb.abb.com

abb.com/oilandgas