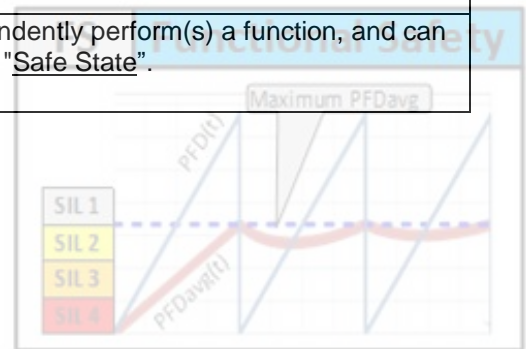
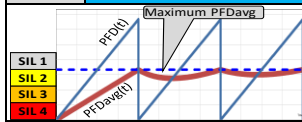


Functional Safety Glossary

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

A	
Analogue signal	A signal type that can handle the measurement of a process variable.
Annunciation Failure Rate	<p>Failure that DOES NOT directly impact safety but DOES impact the ability to detect a future fault (such as a fault in a diagnostic circuit) and that is not detected by internal diagnostics.</p> <p>In other words, failure that has NO IMPACT in safety, the related SIF will perform properly on demand, BUT when this kind of failure happens "Fault Detection capabilities" (Diagnostics) WILL NOT work.</p> <p>NOTE: "Annunciation UnDetected Failure Rate" should be included as part of the "Safe Failure" rate, according to IEC-61508. This failure rate WILL NOT affect system reliability or safety, and it should not be included in "Spurious Trip Rate" calculations.</p>
Average Probability in Time	See "Continuous Probability in Time".
Average Probability of Dangerous Failure on Demand (PFDavg)	<p>Continuous probability calculated from the "Probability of Dangerous Failure on Demand" (PFD) in a period of time.</p> <p>Interpretation: Index to compare "Unreliability" of "Safety Instrumented Functions" (SIF).</p>
B	
Beta Factor (β , or β_D)	See "Common Cause Failure (CCF) factor (β)", and "Common Cause Detected Failure factor (β_D)"
Boolean signal	A type of signal that can have two(2) states only. These ones can be: One(1)/Zero(0), True/False, On/Off, Running/Stop, Safe/Normal, High/Low, etc.
C	
Certification	Process in which several tests and/or revisions are applied/done to a SIS, SIF or Device of a SIF, in order to verify and confirm that it was designed, assembled and installed as indicated in the SRS ("Safety Requirements Specification") document and it complies with the standards IEC-61508 and/or IEC-61511.
Channel	Element or a group of elements that independently perform(s) a function, and can set the whole group in the "Normal State" o "Safe State".





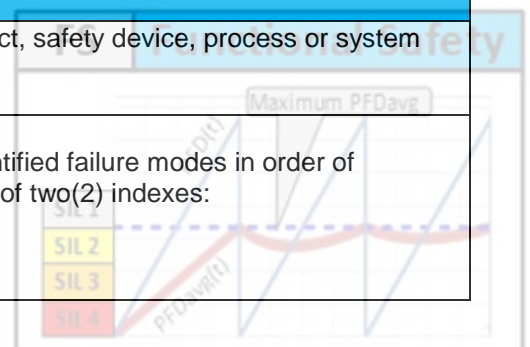
<p>Command signal, INTERLOCK</p>	<p>The Interlock command signal is applied to a single (or more) “TARGET signal(s)”, and it can be in the NORMAL or SAFE state. In SAFE state, there has been “A Demand” of the INTERLOCK function.</p> <p>When the Interlock command signal is in the NORMAL state, the INTERLOCK has no effect on the associated “SIF Output Signals”.</p> <p>When the Interlock command signal is in the SAFE state, “A Demand” of the INTERLOCK function has occurred, next when any of the associated “SIF Output Signals” report a transition from the NORMAL to the SAFE state, then the INTERLOCK forces such “SIF Output Signal” to be in the SAFE state, superseding the associated “Safety Logic”. I.E., the “SIF Output Signal” remains in the SAFE state, regardless the “Safety Logic” result that will occur later.</p> <p>When the Interlock command signal changes back to NORMAL state, then the INTERLOCK allows the “Safety Logic” to determine the “SIF Output Signal” state.</p>
<p>Command signal, Manual RESET</p>	<p>In NORMAL operation, the “Safety Logic” sets its “TARGET signal(s)” in NORMAL state.</p> <p>When “A Demand” occurs, the “Safety Logic” sets its “TARGET signal(s)” in SAFE state.</p> <p>When the operation condition returns to NORMAL, and the “Safety Logic” sets back its output to NORMAL state, its “TARGET signal(s)” remains in SAFE state if a “Reset Logic” was implemented for such “TARGET signal(s)”.</p> <p>The purpose of the manual RESET command is to disable temporarily the “Reset Logic” to allow the related “Safety Logic” output to pass to the “TARGET signal(s)”, in order to set it(them) to the NORMAL state, if the “Safety Logic” output is already in NORMAL state.</p> <p>The manual RESET command signal is normally in the “De-Energized” state. When the manual RESET is applied, the manual RESET command signal is changed temporarily to the “Energized” state.</p>
<p>Command, Self-RESET</p>	<p>See “Command, Automatic RESET”.</p>
<p>Command, Self-Resetting</p>	<p>See “Command, Automatic RESET”.</p>
<p>Command, Automatic RESET</p>	<p>When the Automatic “RESET command” is included as part of a “Reset Logic”, and the related “Safety Logic” result changes its output back to the NORMAL state and it remains in that state, then the related “SIF Output Signals” change to the NORMAL state, without user interaction.</p>
<p>Common Cause Detected Failure factor (β_D)</p>	<p>Of those failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere).</p> <p>Interpretation: 0% means that the Detected Failures (β_D) common causes do not exist.</p>
<p>Common Cause Failure (CCF)</p>	<p>Failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure.</p> <p>-- OR --</p> <p>Common Cause Failure (CCF) causing multiple failures from a single shared cause. The multiple failures may occur simultaneous or over a period of time;</p> <p>Interpretation: Failure that can appear due to a single cause when several safety channels are working in parallel.</p> <p>Common Cause Failure (CCF) applies for the Safety Channel Architecture XooN, when (X<N) ONLY. In any other case CCF is not considered.</p>

<p>Common Cause Failure (CCF) factor (β)</p>	<p>The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere).</p> <p>Interpretation: 0% means that the Undetected Failures (I_{bu}) common causes do not exist.</p>
<p>Common Mode Failure</p>	<p>See " Common Cause Failure".</p> <p>Common Mode Failures (CMF) are a particular case of CCF in which multiple equipment items fail in the same mode.</p>
<p>Component Type "A"</p>	<p>An element can be regarded as type A if, for the components required to achieve the safety function:</p> <ol style="list-style-type: none"> the failure modes of all constituent components are well defined; and the behaviour of the element under fault conditions can be completely determined; and there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.
<p>Component Type "B"</p>	<p>An element shall be regarded as type B if, for the components required to achieve the safety function:</p> <ol style="list-style-type: none"> the failure mode of at least one constituent component is not well defined; or the behaviour of the element under fault conditions cannot be completely determined; or there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures. <p>NOTE : This means that if at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.</p>
<p>Console</p>	<p>See "Control Console"</p>
<p>Console Operator</p>	<p>Operator that sits down in front of the "Control Console" to monitor and execute command through the Console to operate a plant.</p>
<p>Continuous Probability in Time</p>	<p>Probability of an even to occur within a "Sample Space", and within a period of time. See "Probability".</p>
<p>Control Console</p>	<p>A collection of one or more workstations and associated equipment such as printers, communications devices and panel/mimic/push/switch buttons used by a "Console Operator" to interact with the plant control system and to perform plant operation functions.</p>
<p>Criticality (C)</p>	<p>Index that is used in FMECA study to rank identified failure modes. It is calculated from:</p> <ol style="list-style-type: none"> Failure rate of the component associated to the identified failure mode, Failure mode ratio associated to each failure mode among all identified failure modes of the same safety device complement, Conditional probability of a failure mode in an operation condition, among all identified operation conditions for the same failure mode, and Mission time of the related component.
<p>Criticality (C) number</p>	<p>Refer to IEC-60812-2006 Combination of the severity of an effect and the frequency of its occurrence or other attributes of a failure mode as a measure of the need for addressing and mitigation.</p> <p>"Criticality" (C) can be calculated by a qualitative or quantitative approach. Qualitative approach, refer to section 5.3.4.1 Quantitative approach, refer to section 5.3.4.</p>

D	
<p>Dangerous Diagnostic Coverage (DC_D)</p>	<p>Fraction of "Dangerous Failures" (I_D) detected by automatic on-line diagnostic tests. The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures. Value in the range [0 - 100]%</p>
<p>Dangerous Failure Rate (λ_D)</p>	<p>Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:</p> <p>a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or</p> <p>b) decreases the probability that the safety function operates correctly when required.</p> <p>-- OR --</p> <p>Failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state.</p> <p>NOTE: Whether or not the potential is realized may depend on the channel architecture of the system; in systems with multiple channels to improve safety, a dangerous hardware failure is less likely to lead to the overall hazardous or fail-to-function state.</p> <p>Interpretation: When a "Dangerous Failure" occurs, this one prevents the SAFETY FUNCTION to perform its Duty. In other words, when a HAZARD occurs, SIF CANNOT perform its automatic protection function and the "Final Safety Element" (FSE) will remain in the NORMAL state. The EUC is UNPROTECTED.</p>
<p>Demand</p>	<p>Any time a SIF changes the "Final Safety Element(s)" from the NORMAL to the SAFE state, a "Demand" has occurred.</p>
<p>Demand mode</p>	<p>See "Mode of Operation"</p>
<p>Demand Mode, Continuous</p>	<p>Continuous Demand mode where the safety function retains the EUC in a safe state as part of normal operation.</p>
<p>Demand Mode, High</p>	<p>High Demand mode where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.</p>
<p>Demand Mode, Low</p>	<p>Low Demand mode where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.</p>

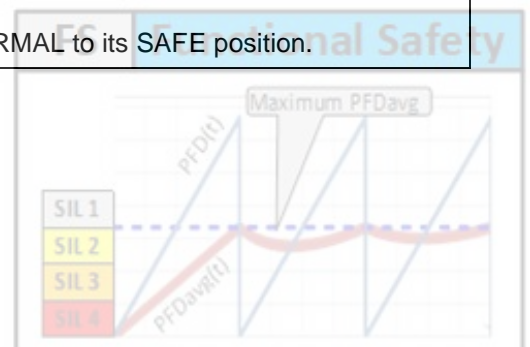


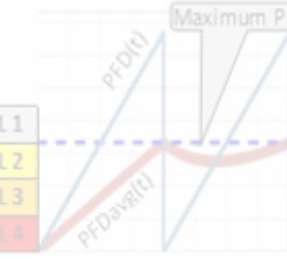
<p>Detected Failure</p> <p>Safe Detected Failure Rate (λ_{SD})</p> <p>Dangerous Detected Failure Rate (λ_{DD})</p>	<p>In relation to hardware, detected by an automatic diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation.</p> <p><u>EXAMPLE</u> These adjectives are used in detected fault and detected failure. A dangerous failure detected by diagnostic test is a revealed failure and can be considered a safe failure only if effective measures, automatic or manual, are taken.</p> <p>In relation to hardware failures and software faults, detected by the diagnostic tests or through normal operation.</p> <p>NOTE: in practice, the above first definition SHALL NOT include proof tests, operator intervention. ONLY automatic diagnostic test shall apply.</p> <p>Interpretation : Failure that can be “Detected” by an automatic diagnostic test, and this test implementation is capable to notify both a Safety/Control system and Operator. The <u>automatic diagnostic test</u> execution frequency MUST BE higher than a “Proof Test” execution frequency.</p>
Device Type "A"	See "Component Type 'A' "
Device Type "B"	See "Component Type 'B' "
Diagnostics, electronic device	<p>Automated test (or tests) that an electronic device executes at a pre-defined frequency in order to identify, reveal or detect own faults, or other devices' faults that are connected to it.</p> <p>Implementation or installation that takes advantage of “Diagnostics” (Fault detection capabilities) of an electronic device can communicate the results of “Diagnostics” to other devices, or systems (SIS, DCS). Typical instrument protocols or methodologies to communicate the “Diagnostic” results are HART, FieldBus, Profibus, NAMUR NE 43, “NAMUR sensor” (EN-60947-5-6:2000 and IEC-60947-5-6:1999).</p> <p>Implementation or installation that DOES NOT take advantage of “Diagnostics” (Fault detection capabilities) of an electronic device CANNOT communicate the results of “Diagnostics” to other devices, or systems (SIS, DCS).</p>
Digital signal	See “Boolean Signal”.
Discrete signal	See “Boolean Signal”.
E	
Element Type "A"	See "Component Type 'A' "
Element Type "B"	See "Component Type 'B' "
Equipment under control	Machine, equipment or process plant used for manufacturing, process, transportation, medical, or other activities.
F	
Failure Modes and Effects Analysis (FMEA)	It is a methodology to identify ways a product, safety device, process or system can fail. Refer to IEC-60812.
Failure Modes, Effects and Criticality Analysis (FMECA)	<p>FMECA is an extension of FMEA.</p> <p>In addition to FMEA, FMECA ranks the identified failure modes in order of importance, according to calculation of one of two(2) indexes:</p> <ol style="list-style-type: none"> “Risk Priority Number” (RPN) or Criticality (C).



FUNCTIONAL SAFETY GLOSSARY

<p>Failure Modes, Effects and Diagnostic Analysis (FMEDA)</p>	<p>A FMEDA is a systematic detailed procedure that is an extension of the classic FMEA procedure, which purpose is to calculate the failure rates of a safety device or group of safety devices.</p> <p>This technique was first developed for electronic devices and recently extended to mechanical and electro-mechanical devices.</p> <p>A FMEDA assessment of a hardware device or arrangement (group of devices) provides the required failure data (or Reliability data) needed for “SIL verification”, “SIL Certification” or to calculate the device contribution in a “Safety Instrumented Function” (SIF) when the SIF’s SIL rating is calculated.</p>
<p>Failure Rate (λ)</p>	<p>Reliability parameter [$\lambda(t)$] of an entity (single components or systems) such that “$\lambda(t).dt$” is the probability of failure of this entity within [t, t+dt] assuming that it has not failed during [0, t].</p> <p>Interpretation: Average frequency of failure (Probability), or chance of a single Component, Element or System to fail within a period of time.</p>
<p>Failure Rate, Dangerous Detected (λ_{DD}, or LdDD)</p>	<p>See “Detected Failure”, “Dangerous Detected Failure Rate”.</p>
<p>Failure Rate, Dangerous UnDetected (λ_{DU}, or LdDU)</p>	<p>See “UnDetected Failure”, “Dangerous UnDetected Failure Rate”.</p>
<p>Failure Rate, Safe Detected (λ_{SD}, or LdSD)</p>	<p>See “Detected Failure”, “Safe Detected Failure Rate”.</p>
<p>Failure Rate, Safe UnDetected (λ_{SU}, or LdSU)</p>	<p>See “UnDetected Failure”, “Safe UnDetected Failure Rate”.</p>
<p>Fault</p>	<p>Abnormal condition that may cause a reduction in, or loss of, the capability of a functional unit to perform a required function.</p>
<p>Fault Detection Capabilities</p>	<p>See “Diagnostics, electronic device”.</p>
<p>Fault Tolerance</p>	<p>Ability of a functional unit to continue to perform a required function in the presence of faults or errors.</p>
<p>Field Operator</p>	<p>Operator that is normally at the plant field to monitor and to execute action directly over the plant equipment or instruments.</p>
<p>Final Safety Element (FE or FSE)</p>	<p>Last Device or "Safety Channel Architecture" (SCA) in the "Main Safety Loop Series" (MSLS) which executes in fact the safety action to protect the plant or system against an identified Hazard.</p> <p>It is normally a valve (+actuator) that has to be Opened/Closed, a motor that has to be set in the On/Off state, etc., to complete the execution of the safety action.</p> <p>It can be in the NORMAL or SAFE state, in order to move the related plant/equipment to the NORMAL or SAFE state, respectively.</p>
<p>Full Valve Stroke Test (FVST)</p>	<p>See “Stroke Test”.</p> <p>In a FVST, the valve is stroked from its NORMAL to its SAFE position.</p>



<p>Functional Safety Management (FSM)</p> 	<p>The Functional Safety Management (FSM) is the management activity that prepares and follows up the execution of the “Safety Plan”.</p> <p>The Safety Plan or Functional Safety Management (FSM) Plan is a key document in any IEC 61508 / ISO 26262 development project. It specifies how functional safety will be ensured throughout the entire development project and in production.</p> <p>The Safety Plan must identify all roles and responsibilities that apply to the development process. The Safety plan shall list various techniques and measures that will be implemented as part of the project under development to ensure that the targeted SIL is achieved.</p> <p>The deliverable of this task is the <u>draft Safety Plan</u> that the Customer must subsequently refine and implement in the project under development.</p>
--	---

G

<p>Graphic User Interface (GUI)</p>	<p>See “Human Machine Interface” (HMI)</p>
--	--

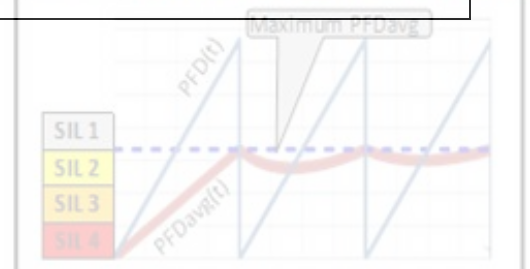
H

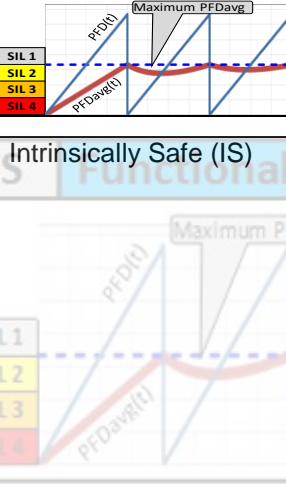
<p>Hardware Fault Tolerance</p>	<p>Hardware fault tolerance is the ability of a component or subsystem to continue to be able to undertake the required safety instrumented function in the presence of one or more dangerous faults in hardware. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring.</p>
--	--

<p>Hardware Fault Tolerance (HFT), or Hardware Fault Tolerance degree</p>	<p>Ability of a functional unit to continue to perform a required function in the presence of faults or errors.</p> <p>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. A hardware fault tolerance of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring</p> <p>Normally the “Hardware Fault Tolerance Degree” is associated to the “Safety Channel Architecture” (SCA) XooN, where “Hardware Fault Tolerance” (HFT) is equal to “N-X”, or in other words, the number of safety channels that can be in failure condition, but the SCA can still perform the required safety.</p> <p><u>Examples:</u></p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>SCA</th> <th>Voting</th> <th>Hardware Fault Tolerance (HFT)</th> <th>Redundancy (1)</th> </tr> </thead> <tbody> <tr><td>1oo1</td><td>1</td><td>0</td><td>0</td></tr> <tr><td>1oo2</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>2oo2</td><td>2</td><td>0</td><td>0</td></tr> <tr><td>1oo3</td><td>1</td><td>2</td><td>2</td></tr> <tr><td>2oo3</td><td>2</td><td>1</td><td>1</td></tr> <tr><td>3oo3</td><td>3</td><td>0</td><td>0</td></tr> <tr><td>2oo4</td><td>2</td><td>2</td><td>1</td></tr> <tr><td>1oo2D</td><td>2</td><td>1</td><td>1</td></tr> <tr><td>2oo3D</td><td>3</td><td>1</td><td>1</td></tr> </tbody> </table> <p>Note 1: see “Redundancy”</p>	SCA	Voting	Hardware Fault Tolerance (HFT)	Redundancy (1)	1oo1	1	0	0	1oo2	1	1	1	2oo2	2	0	0	1oo3	1	2	2	2oo3	2	1	1	3oo3	3	0	0	2oo4	2	2	1	1oo2D	2	1	1	2oo3D	3	1	1
SCA	Voting	Hardware Fault Tolerance (HFT)	Redundancy (1)																																						
1oo1	1	0	0																																						
1oo2	1	1	1																																						
2oo2	2	0	0																																						
1oo3	1	2	2																																						
2oo3	2	1	1																																						
3oo3	3	0	0																																						
2oo4	2	2	1																																						
1oo2D	2	1	1																																						
2oo3D	3	1	1																																						

<p>Harm</p>	<p>Physical injury or damage to the health of people or damage to property or the environment.</p>
--------------------	--

HART	Highway Addressable Remote Transducer) is a hybrid analogue+digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy 4–20 mA analogue instrumentation current loops, sharing the pair of wires used by the analog only host systems.
Hazard	Potential source of harm.
Hazard and Operability Study (HAZOP)	It is a structured and systematic examination of a complex planned or existing process or operation in order to identify and evaluate problems that may represent risks to personnel or equipment. The intention of performing a HAZOP is to review the design to pick up design and engineering issues that may otherwise not have been found. The HAZOP technique was initially developed to analyse chemical process systems, but has later been extended to other types of systems and also to complex operations such as nuclear power plant operation and to use software to record the deviation and consequence. A HAZOP is a qualitative technique based on guidewords and is carried out by a multi-disciplinary team (HAZOP team) during a set of meetings.
Hazard and Operability Study REPORT (HAZOP Report)	The HAZOP Report is a key document pertaining to the safety of the plant. It is crucial that the benefit of this expert study is easily accessible and comprehensible for future reference in case the need arises to alter the plant or its operating conditions. Normally, the HAZOP report includes the list and description of all identified "Safety Instrumented functions" (SIFs).
Hazard DETECTION CONDITION	After a Hazards occurs (Hazard OCCURRENCE) the process plant physical conditions to allow instrumentation to detect the hazard may not be in place yet. Some time is required to allow the Hazard to develop a physical condition that allow instrumentation to detect it. A Hazard reached the DETECTION CONDITION when the instrumentation in fact is able to detect such Hazard.
Hazard Identification Study (HAZID), or Hazard Analysis	It is used as the first step in a process used to assess risk. The result of a hazard analysis is the identification of different type of hazards.
Hazard OCCURRENCE	Time at the process operation when an even occurs that declares the initiation of a HAZARD.
Human Machine Interface (HMI)	Also known as an HMI. An HMI is a software application that presents information to an operator or user about the state of a process, and to accept and implement the operators control instructions. Typically, information is displayed in a graphic format (Graphical User Interface or GUI). An HMI is often a part of a SCADA (Supervisory Control and Data Acquisition) system, or a DCS (Distributed Control system).
I	
Initiator	See "Sensor", "Process variable". First Device or "Safety Channel Architecture" (SCA) in the "Main Safety Loop Series" (MSLS) which executes the measurement of the process variable that identifies the Hazard for the plant or system has to be protected from.



<p>Intrinsically Safe (IS)</p> 	<p>It is a protection technique for safe operation of electrical equipment in hazardous areas by limiting the energy, electrical and thermal, available for ignition.</p> <p>In signal and control circuits that can operate with low currents and voltages, the intrinsic safety approach simplifies circuits and reduces installation cost over other protection methods. Areas with dangerous concentrations of flammable gases or dust are found in applications such as petrochemical refineries and mines.</p> <p>As a discipline, it is an application of inherent safety in instrumentation. High-power circuits such as electric motors or lighting cannot use intrinsic safety methods for protection.</p>
--	--

L

<p>Logic Solver</p>	<p>It is a device, part of a SIS that can execute the “Safety Logic” (many “TRIP criteria”, “Voting Logics” and “SIF Decision Logics”). Nowadays the “Logic Solver” could be part of a module in the DCS (PCS), or an independent module based on electrical, electronic, mechanical, pneumatic or hydraulic technology. Sometimes a hybrid “Logic Solver” can be used.</p>
----------------------------	---

M

<p>Main Safety Loop Series (MSLS)</p>	<p>Sequence in Series of "Safety Channel Architectures" (SCA) that constitute a Safety Loop, or SIF, from the Sensor(s) (or Initiator(s)) to the Final Safety Element(s) [FE(s)].</p>
--	---

<p>MAINTENANCE times</p>	<p>The SIF MAINTENANCE times are: MTTR, TD, MRT, TI, SIf and time constraints. These times have a direct impact on the MAINTENANCE effort to keep the SIF installation in good shape. The following table shows typical “MAINTENANCE times” requirement for a project:</p>
---------------------------------	--

#	Description	Abbre.	Default	Constraint	Remark
1	Proof Test Period	TI	6 months	≥ 4 months	Initiators
				≥ 4 months	SOVs
				≥ 6 months	Safety valves
2	Service Life	SIf	24 months	≥ 12 months	
3	Mean Time To Restoration	MTTR	72 hours	≥ 24 hours	
4	Proof Test Duration	TD	4 hours	≥ 1 hour	
5	Mean Repair Time	MRT	24 hours	≥ 8 hours	

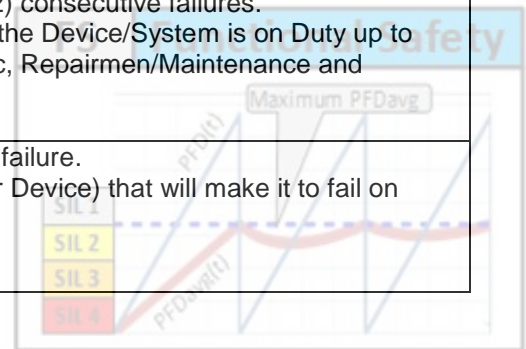
<p>Maximum Allowed Response Time (MART)</p>	<p>See “Safety Response Time” (SRT).</p>
--	--

<p>Mean Repair Time (MRT)</p>	<p>See "Mean Restoration Time" (MRT).</p>
--------------------------------------	---

<p>Mean Restoration Time (MRT)</p>	<p>Expected overall repair time MRT encompasses the times (b), (c) and (d) of the times for MTTR.</p>
---	---

<p>Mean Time Between Failures (MTBF)</p>	<p>Mean time between the occurrence of two(2) consecutive failures. This time includes the operation time since the Device/System is on Duty up to when the failure occurrence, next diagnostic, Repairmen/Maintenance and commissioning to be on Duty again.</p>
---	---

<p>Mean Time To Dangerous Failure (MTTF_D)</p>	<p>Expectation of the mean time to dangerous failure. Mean Time to a failure of the SIS (or SIF, or Device) that will make it to fail on demand.</p>
---	--



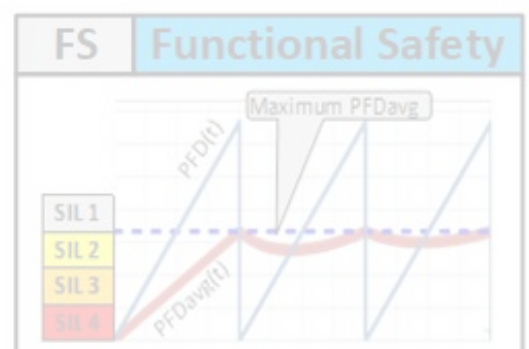
Mean Time To Failure (MTTF)	Mean time since the Device/System is on Duty up to the occurrence of a failure.
Mean Time To Failure Spuriously (MTTF _{spuriously} , or MTTFs)	The mean time to a failure of the SIS (or SIF, or Device) which results in a spurious or false trip of the process or equipment under control (EUC)
Mean Time To Repair (MTTR)	See "Mean Time To Restoration" (MTTR).
Mean Time to Restoration (MTTR)	Expected time to achieve restoration MTTR encompasses: <ul style="list-style-type: none"> (a) the time to detect the failure, and (b) the time spent before starting the repair, (c) the effective time to repair, and (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

NAMUR	User Association of Automation Technology in Process Industries (NAMUR) (German: Interessengemeinschaft Automatisierungstechnik der Prozessindustrie), established in 1949, is an international association for users of automation technology in the process industries with its headquarters in Leverkusen, Germany. The association represents the interests of, and supports the experience exchange among over, 140 member companies and with other associations and organizations. Work results are published in the form of NAMUR recommendations and worksheets and submitted to national and international standardization bodies as proposed standards. www.namur.de
NAMUR NE 43 (For Analogue signals)	The Namur NE 43 is a recommendation which gives a guideline (for Analogue signals) how a sensor fault can be indicated to a DCS or SIS by means of the 4-20mA signal. A sensor fault is signaled by extending the range of the 4-20mA signal. When the current is below 3,6 mA or above 21 mA this is interpreted as a sensor fault. In order to avoid false alarms.
NAMUR Sensor (For Boolean, Digital or Discrete signals)	(EN-60947-5-6:2000 and IEC-60947-5-6:1999) NAMUR format that is used for switching devices (Sensors or Sensors' interfaces) to communicate the two switch states via two different current levels. Typically, 2.1 mA for one State and 1.2 mA for the other State. Signal current value above 2.1 mA or below 1.2 mA indicates that a " <u>Detected Failure</u> " occurred.
Near miss	"near hit", "close call", or "nearly a collision" is an unplanned event that has the potential to cause, but DOES NOT actually result in human injury, environmental or equipment damage, or an interruption to normal operation.

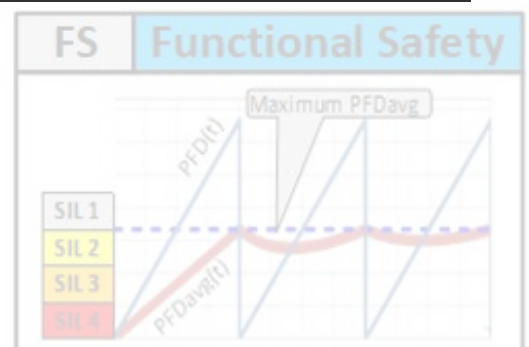


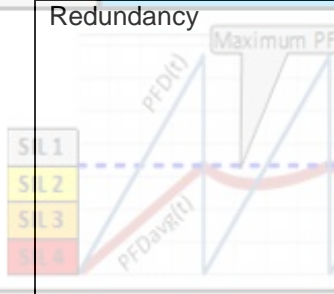
No Effect Failure Rate	<p>Failure of a component of a SIF device that IS NOT part of the safety function, so it has NO EFFECT in the required safety.</p> <p>In other words, failure that DOES NOT prevent a “Target System” to perform its automatic protection function and DOES NOT initiate “Spurious Trip”.</p> <p><u>For example:</u> Failure of a digital display of a transmitter in the field.</p> <p>NOTE: “No Effect Failure Rate” should be included as part of the “Safe Failure” rate, according to IEC-61508. Nevertheless, this failure rate WILL NOT affect system reliability or safety, and it SHOULD NOT be included in “SIL” and “Spurious Trip Rate” calculations.</p>
NORMAL state	It is the value, position, mode or condition of a signal or safety equipment while the plant is in NORMAL operation mode.
O	
Out Of Service (OOS)	An Equipment or SIF device is set in the “Out Of Service” condition when it is shutdown and set out of normal operation, in order to allow to apply MAINTENANCE activities for a time longer than MTTR (Mean Time to Restoration).
P	
Partial Valve Stroke Test (PVST)	See “Stroke Test”. In a PVST, the valve is stroked from its NORMAL position up to an intermediate position between the NORMAL and SAFE position. The valve never reaches the SAFE position.
PE-based	Programable Electronic based system. CPU based system.
Periodical Test	See "Proof Test" and reference in IEC 61508-4, sec.385, NOTE 1.
Probability	<p>Probability of an event to occur, or to do not occur, within a "Sample Space". In probability theory, the "Sample Space" of an experiment or random trial is the set of all possible outcomes or results of that experiment. Probability is an index which value is in the range [0 to 1]. If the issue of interest is the chance of an event to occur, a probability value of:</p> <ul style="list-style-type: none"> 1.0 = indicates that the event will occur for sure. near to 1.0 indicates that the event has a big chance to occur. near to 0.0 indicates that the event has a small chance to occur. 0.0 = indicates that the event still not occur for sure.



<p>Probability of Dangerous Failure on Demand (PFD)</p>	<p>From a safety point of view, the important issue is to design a safety system taking care of the required uncertainty for the system to do not respond on demand. this uncertainty shall be considered from each device within the safety system.</p> <p>From the "Failure Model", it is clear that this uncertainty is represented mainly by the "Dangerous Undetected failure rate" (λ_{DU}).</p> <p>The other failure rates in the "Failure Model" are not directly considered, because:</p> <ol style="list-style-type: none"> 1) If a Safe Failure occur, the safety system will go to the SAFE state. 2) If a "Dangerous Detected failure" occurs, it is known that the safety system has a failure, and maintenance activities shall be requested on time to fix such failure. <p>Nevertheless, other factors are important when the safety system is designed, and when it is on Duty, like:</p> <ol style="list-style-type: none"> a) Maintenance considerations. b) Proof test effectiveness (E_t) of each device in the safety system. c) Common cause failure (CCF) of devices that are organized in parallel safety channels. d) Additional diagnostic capabilities in "Safety Channel Architectures" of type XoonN(D). <p>Since probability is a mathematical index in the range [0 to 1], and "Safety" is a continuous issue in "time", the PFD is a punctual probability function of time, which starts when safety is on Duty the first time, and it is based on the an adjusted "Failure Rate" after applying the previous considerations.</p>
<p>Process Safety Time (PST)</p>	<p>It is the maximum time bound that is available for a Safety Implementation (SIF or IPF), from the time the HAZARD occurs, up to the completion of the final safety action, to avoid the development of such HAZARD into an ACCIDENT or Harm.</p>
<p>Process Variable</p>	<p>See "Sensor", "Initiator".</p> <p>The plant variable (pressure, temperature, level, flow, concentration, etc.) that is important to monitor, in order to determine if the process plant is in the desired operation condition, or is an unsafe condition to trip the execution of safety actions.</p>
<p>Proof Test</p>	<p>Periodic test performed to detect dangerous hidden failures in an element (component, device) of a safety related system so that, if it is necessary, a repair can restore the system to an "as new" condition or as close as practical to that condition.</p> <p>NOTE 1 The effectiveness of the proof test will be dependent both on failure coverage and repair effectiveness. In practice detecting 100 % of the hidden dangerous failures is not easily achieved for other than low-complexity E/E/PE safety-related systems. This should be the target. As a minimum, all the safety functions which are executed are checked according to the E/E/EP system safety requirements specification. If separate channels are used, these tests are done for each channel separately. For complex elements, an analysis may need to be performed in order to demonstrate that the probability of hidden dangerous failure not detected by proof tests is negligible over the whole life duration of the E/E/EP safety related system.</p> <p>NOTE 2 A proof test needs some time to be achieved. During this time the E/E/PE safety related system may be inhibited partially or completely. The proof test duration can be neglected only if the part of the E/E/PE safety related system under test remains available in case of a demand for operation or if the EUC is shut down during the test.</p> <p>NOTE 3 During a proof test, the E/E/PE safety related system may be partly or completely unavailable to respond to a demand for operation. The MTTR can be neglected for SIL calculations only if the EUC is shut down during repair or if other risk measures are put in place with equivalent effectiveness.</p>

Proof Test Coverage (PTC)	<p>See "Proof Test Effectiveness" (Et).</p> <p>Faults in the safety system that are not detected by either diagnostic tests or proof tests may be found by other methods arising from events such as a hazardous event requiring operation of the safety function or during an overhaul of the equipment. If the faults are not detected by such methods it should be assumed that the faults will remain for the life of the equipment.</p> <p>Consider a normal proof test period of T1 where the fraction of faults detected when a proof test is performed is designated as PTC (proof test coverage) and the fraction of the faults not detected when a proof test is performed is designated as (1-PTC). These latter faults which are not detected at the proof test will only be revealed when a demand is made on the safety related system at demand period T2. Therefore, the proof test period (T1) and the demand period (T2) govern the effective down time.</p>
Proof Test duration (TD)	<p>Amount of time to dedicate for the Proof Test execution. Normally it is indicated in hours [h].</p> <p>This is the time that is properly dedicated to the Proof Test, starting at the moment the device is disconnected from the safety loop, up to the time the device is connected again to the safety loop.</p> <p>Value in range [0 , 24] hours</p> <p>The time for preparation before and after the Proof Test execution is not considered in TD.</p> <p>If the Device under proof testing is located in the SIF's MSLS, such SIF is out of service during the TD time, and its PFD value is 1.0 (no protection). PFDavg shall increase accordingly.</p>
Proof Test Effectiveness (Et)	<p>(See also "Proof Test").</p> <p>See also "Proof Test Coverage" (PTC).</p> <p>Portion of the "Dangerous Undetected Failures" (λ_{DU}) revealed by Proof Testing, without applying maintenance to the device of interest.</p> <p>The Proof Test Effectiveness (Et) is computed for a single Device by using its "Dangerous Undetected failure rate, revealed by Operation intervention or a proof test" (λ_{DU-P}) divided by the "Dangerous Undetected Failures" (λ_{DU}).</p> <p>Value in the range [0 - 100]%</p>
Proof Test Period	<p>Frequency in days, week, months, or years in which a "Proof Test" is performed.</p>
Pulse signal	<p>In signal processing, the term pulse has the following meanings: A rapid, transient change in the amplitude of a signal from a baseline value to a higher or lower value, followed by a rapid return to the baseline value.</p> <p>In process control, it is a Boolean signal that alternate the two(2) states [1/0, True/False, etc.] in time, following a pre-defined pattern and/or frequency range.</p> <p>Example: Flow Turbine type meter, Compressor/Machine speed, etc.</p>
Punctual Probability	<p>See "Probability".</p>



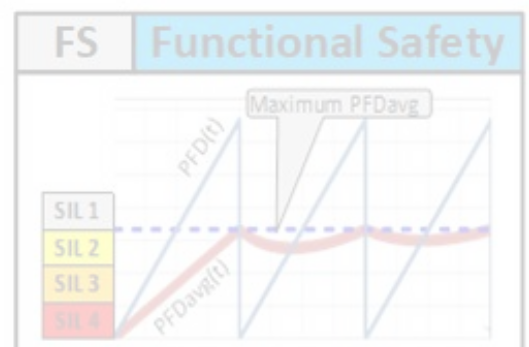
R	Functional Safety																																										
<p>Redundancy</p> 	<p>The existence of more than one means for performing a required function or for representing information.</p> <p><u>Example 1:</u> Duplicated functional components and the addition of parity bits are both instances of redundancy.</p> <p>Redundancy is used primarily to improve reliability (probability of functioning properly over a given period of time) or availability (probability of functioning at given instant). It may also be used in order to minimize spurious actions through architectures such as 2oo3.</p> <p><u>Example 2:</u></p>																																										
		<table border="1" style="margin-left: auto; margin-right: auto;"> <thead> <tr> <th>SCA</th> <th>Voting</th> <th>Hardware Fault Tolerance, HFT (1)</th> <th>Redundancy</th> </tr> </thead> <tbody> <tr><td>1oo1</td><td>1</td><td>0</td><td>0</td></tr> <tr><td>1oo2</td><td>1</td><td>1</td><td>1</td></tr> <tr><td>2oo2</td><td>2</td><td>0</td><td>0</td></tr> <tr><td>1oo3</td><td>1</td><td>2</td><td>2</td></tr> <tr><td>2oo3</td><td>2</td><td>1</td><td>1</td></tr> <tr><td>3oo3</td><td>3</td><td>0</td><td>0</td></tr> <tr><td>2oo4</td><td>2</td><td>2</td><td>1 (Note 2)</td></tr> <tr><td>1oo2D</td><td>2</td><td>1</td><td>1</td></tr> <tr><td>2oo3D</td><td>3</td><td>1</td><td>1</td></tr> </tbody> </table>	SCA	Voting	Hardware Fault Tolerance, HFT (1)	Redundancy	1oo1	1	0	0	1oo2	1	1	1	2oo2	2	0	0	1oo3	1	2	2	2oo3	2	1	1	3oo3	3	0	0	2oo4	2	2	1 (Note 2)	1oo2D	2	1	1	2oo3D	3	1	1	
SCA	Voting	Hardware Fault Tolerance, HFT (1)	Redundancy																																								
1oo1	1	0	0																																								
1oo2	1	1	1																																								
2oo2	2	0	0																																								
1oo3	1	2	2																																								
2oo3	2	1	1																																								
3oo3	3	0	0																																								
2oo4	2	2	1 (Note 2)																																								
1oo2D	2	1	1																																								
2oo3D	3	1	1																																								
		<p>Note 1: see “Hardware Fault Tolerance”</p> <p>Note 2: “Fault Tolerance” is not a measure of “Redundancy”. In the “2oo4” SCA let’s say four(4) safety channels (or safety devices) are used: A, B, C, and D. To achieve the required safety the “2oo4” SCA shall evaluate the following combinations: AB, AC, AD, BC, BD, CD.</p> <p>If one(1) channel (or device) fails, let’s say “A”, then “2oo4” redundancy is “3”, because three(3) combinations will not work, but the other three(3) will achieve required safety: AB, AC, AD, BC, BD, CD.</p> <p>If two(2) channels (or devices) fail, let’s say “A” and “B”, then “2oo4” redundancy is “1”, because five(5) combinations will not work, but the remaining one will achieve required safety: AB, AC, AD, BC, BD, CD.</p>																																									
	Reliability Block Diagram (RBD)	A “Reliability Block Diagram” (RBD) is a diagrammatic method for showing how components or Devices individual interaction and reliability contributes to the success or failure of a complex system. RBD is also known as a dependence diagram (DD).																																									
	Replace period	See "Service Life"																																									
	Reset Function	<p>The purpose of a “Reset Function” is to keep a machine, equipment or process plant in the SAFE condition, after it was performed a transition from the NORMAL to the SAFE state. After such transition, the “Reset Function” is activated.</p> <p>In other words, the “Reset Function” is activated after a SIF demand.</p> <p>Once the machine, equipment or process plant comes back to the NORMAL state, a “RESET command” must be executed to make the “Reset Function” to abandon the “Activated” condition, and to allow the “Safety Logic” output to determine the NORMAL or SAFE state.</p> <p>The “Reset Function” can be implemented as a “Reset Logic” in the “Logic Solver”, or as a mechanical device in the field, located at the “Trip device”/“Final Safety Element”, or both.</p> <p>Refer to “Reset Logic” or “Mechanical Reset” for further details.</p>																																									

<p>Reset Logic</p>	<p>The “Reset Logic” is implemented in a “Logic Solver, and it applies to a “TARGET signal(s)”.</p> <p>The “Reset Logic” starts to work after a transition of the “Safety Logic” output from the NORMAL to the SAFE state. At this time, the purpose of the “Reset Logic” is to keep the related “TARGET signal” in the SAFE state, superseding the “Safety Logic” output. I.E., the “TARGET signal” remains in the SAFE state, regardless the “Safety Logic” output state value.</p> <p>Once the “Safety Logic” output changes back to NORMAL state, and remains in that state, a “Reset Command” action is required on the “Reset Logic” to disable it, in order to allow the “Safety Logic” output to determine the “TARGET signal” state again.</p> <p>See “Command Automatic RESET” or “Command signal Manual RESET”, the one that apply in the implementation.</p>
<p>Reset, Mechanical</p>	<p>The “Reset Function” can be implemented as a mechanical device in the field, located at the “Trip device”, “Final Safety Element”, or both.</p> <p>The Mechanical “Reset Function” starts to work, after a transition of the related “Trip device”/“Final Safety Element” from the NORMAL to the SAFE state.</p> <p>At this time, the purpose of a Mechanical Reset is to keep the “Trip device”/ “Final Safety Element” in the SAFE state, regardless the related “SIF Output Signal” state changes that will occur later.</p> <p>Once the state of all the related “SIF Output Signals” change back to NORMAL state, and such NORMA state remains, it is required that the Field Operator executes a Manual “Reset Command” at the “Trip device”/“Final Safety Element”.</p> <p>This command disables the Mechanical Reset action, in order to allow the “Trip device”/“Final Safety Element” to change to the NORMAL state, and to let the “SIF Output Signal” to determine the “Trip device”/“Final Safety Element” state.</p>
<p>Risk Priority Number (RPN)</p>	<p>Index that is used in FMECA study to rank identified failure modes. It is calculated from:</p> <ol style="list-style-type: none"> a) Failure mode Severity, b) Probability of occurrence of a failure mode for a predetermined or stated time period, or an estimate of the chance a failure mode will occur, and c) Detection index, i.e. an estimate of the chance to identify and eliminate the failure before the system is affected.
<p>Risk Reduction Factor (RRF)</p>	<p>Risk reduction that is required by the machine, equipment or process plant “Safety Instrumented System” (SIS) to ensure the related Hazard risk can be reduced up to the Tolerable Risk.</p> <p>Not only SIS can be applied to reduce risk, also other safety technologies, design changes to reduce risk, or other physical risk reduction measures can be applied.</p>
S	
<p>SAFE condition</p>	<p>Plant condition next to a shutdown request, in which the possibility of any harm occurrence is eliminated, after applying safety actions to set all equipment (Final Safety Elements) in the SAFE state.</p>
<p>Safe Diagnostic Coverage (DCs)</p>	<p>Fraction of "Safe Failures" (λ_s) detected by automatic on-line diagnostic tests. The fraction of safe failures is computed by using the safe failure rates associated with the detected safe failures divided by the total rate of safe failures. Value in the range [0 - 100]%</p>
<p>Safe Failure Fraction (SFF)</p>	<p>Property of a safety related element that is defined by the ratio of the average failure rates of safe (λ_s) plus dangerous detected failures (λ_{DD}) and safe plus dangerous failures ($\lambda_s + \lambda_{D}$).</p>

<p>Safe Failure Rate (λ_s)</p> 	<p>Failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:</p> <p>a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or</p> <p>b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state.</p> <p>-- OR --</p> <p>Failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state.</p> <p>NOTE 1 : Whether or not the potential is realized may depend on the channel architecture of the system.</p> <p>NOTE 2 : Other names used for safe failure are nuisance failure, spurious trip failure, false trip failure or fail-to-safe failure.</p> <p>NOTE: This second definition includes many failures that DO NOT cause a false trip under any circumstances and is quite different from the definition practitioners need to calculate the false trip probability. Using this definition, all failure modes that ARE NOT dangerous are called “Safe.” For example: No Effect” of “Annunciation” failures. These failures MUST NOT be included in the SIL verification calculations.</p> <p>Interpretation: When a “Safe Failure” occurs, the SAFETY FUNCTION moves the “Final Safety Element” (FSE) from NORMAL to SAFE state.</p>
SAFE state	It is the value, position, mode or condition of a signal or safety equipment while the plant is in the safe shutdown mode after execution of safety actions.
Safety Architecture	See “Safety Channel Architecture”
Safety Channel Architecture (SCA)	<p>See “Voting Logic”.</p> <p>Connection skeme including decision logic in which several devices are organized to provide safety states transmission within the SIF's 'MAIN Safety Loop SERIES" (MSLS).</p> <p>The SCA are indicated by a term of the form "XooN", it means:</p> <p>A) Logic of N inputs, where output is set on SAFE state when X inputs are in SAFE state.</p> <p>B) Logic that will fail on demand when (N - X + 1) input devices fail due to "Dangerous Undetected Failures".</p> <p>NOTE 1: N is always greater than, or equal to X.</p> <p>NOTE 2: N is always greater than, or equal to X.</p>



<p>Safety design maximum SIL limit (SDmaxSIL)</p>	<p>Break line between SIL ratings to guarantee that the safety design SIL rating will remain after implementation, considering some amount of possible deviations.</p> <p>Design Case: if a PFDavg value is 9.95E-03, it is equivalent to SIL 3 rating according the IEC 61508 standard. But this value is very near to the PFDavg range equivalent to SIL 2 rating. Minor deviations during implementation phase can make this safety loop to move to SIL 2 rating.</p> <p>The SDmaxSIL is defined as a percentage in the range of [0 - 100]% of the PFDavg range for SIL definition, in order to have some safety calculation margining during design phase.</p> <p>EXAMPLE: as indicated in the IEC 61508 standard, the PFDavg range for SIL 3 rating is [1.0E-04 to 1.0E-03]. If the SDmaxSIL value is established as 90%, then 90% of the PFDavg range for SIL 3 is: Margin High = (1.0E-03 - 1.0E-04) x (100% - 90%) = 9.0E-05 Margin LOW = (1.0E-04 - 1.0E-05) x (100% - 90%) = 9.0E-06 then adding this "Margin" to the PFDavg range for SIL 3 rating it is possible to establish a new range for SIL 3 rating design as follows: [9.1E-04 to 9.1E-05]</p>
<p>Safety Instrumented Function (SIF)</p>	<p>SIF is a safety function implemented in a "Safety Instrumented System" (SIS), which purpose is to avoid a machine or process plant to be operated under conditions that will result in a harm of personal safety, environment or the machine/process plant itself. When a SIF is performing its safety function, it is in the "On Duty" condition.</p> <p>More precisely, a SIF defines which the "SIF Input Signal(s)" is (are) that trips (trip) an action(s) (or Command(s)) to be sent through the "SIF Output Signal(s)" to set the "Final Safety Element(s)" in a SAFE state, in order to move the related plant or equipment into a SAFE condition.</p> <p>In NORMAL operation condition, the "Final Safety Elements" are in the NORMAL state.</p> <p>The SIFs are identified in a HAZOP, and they are recorded in a HAZOP report.</p>
<p>Safety Instrumented System (SIS)</p>	<p>It is an instrumented system used to implement one or more safety instrumented functions (SIFs), which are expected to set a plant or equipment to its SAFE condition, prior to any hazard happens. A SIS is composed of any combination of sensor (s), logic solver (s), and final safety elements(s).</p>



FUNCTIONAL SAFETY GLOSSARY

Safety Integrity Level (SIL)

Discrete level (one out of a possible four(4)), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest.

In practice the “Safety Integrity Levels” are defined as follows:

“Safety Integrity Level” (SIL)	Where to implement SIF
SIL 4	Implement in SIS
SIL 3	
SIL 2	
SIL 1	
SIL a	Implement in DCS or SIS (project decision)
SIL 0	No additional safety considerations are required for the identified HAZARD. No implementation is required

Safety Logic

It is a predefined logic which contains the rules of making actions on “Safety Output Signals”, based on the of “Safety Input Signal” states. The “Safety Logic” can be executed by a “Logic Solver”, or by the same “Safety Input Signal” measuring device.
When a “Logic Solver” is used, it can contain many “TRIP criteria”, “Voting Logics”, “Safety Logics”, Reset functions, Interlock functions, Permissive functions and basic logic operations.

Safety Output Signal

See “SIF Output Signal”.

Safety Related System

See "Safety Instrumented System".

Safety Response Time (or SRT)

It is the maximum allowed “Safety Instrumented Function” (SIF or IPF) response time to avoid the development of a HAZARD into a Harm or ACCIDENT.
This time goes from the time the HAZARD reaches the DETECTION CONDITION (Instrument can detect), up to the completion of the final safety action.
SRT is established to guarantee that a SIF/IPF will achieve its duty, regardless any deviation or degradation from the safety design and implementation, or due to normal instruments tear and wear.
In case of no clear project requirement, SIF design must comply: $SRT \leq (50\% \text{ of PST})$.

Safety Scenario

Operation condition that is identified during a HAZOP, which can cause an accident or operability problem, due to a failure or operation mistake in the Equipment Under Control (EUC), or due to a failure in the E/E/PE safety-related system.

Safety shutdown mode

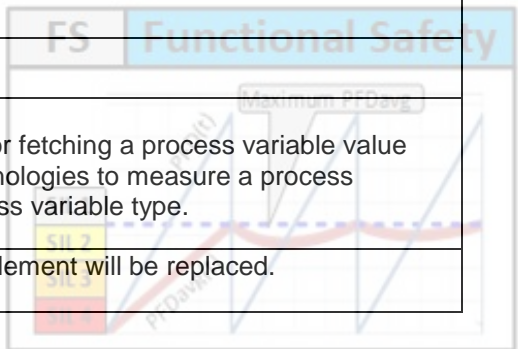
See: “Safe condition”

Sensor

See "Initiator", "Process variable".
Device used for measurement, monitoring, or fetching a process variable value continuously. There are many different technologies to measure a process variable, and also for measuring each process variable type.

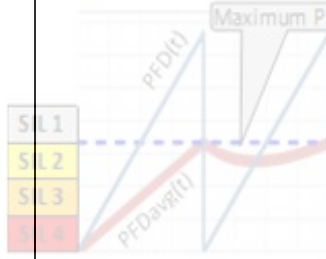
Service Life (SLf)

Period of time when a component of SIF's Element will be replaced.



<p>SIF Decision Logic</p>	<p>Logic configured in a “Logic Solver” which determine the “SIF output signal” states based on “SIF input signal” states. All SIFs are included in the "SIF decision logic".</p> <p>From the SIL verification and PFD calculation point of view, "SIF decision logic" is a concept out of scope. A SIS handle many SIFs, and SIL/PFD are concepts to handle for each SIF, not for all SIFs in SIS.</p> <p>For the scope of this "Tool", "SIF decision Logic" shall be the same as the "Voting Logic".</p>
<p>SIF Input Signal</p>	<p>It is the signal that provides information about current condition of a process variable, plant or equipment to a “Logic Solver” (part of a SIS). It can be of the Analogue or Boolean type.</p>
<p>SIF Output Signal</p>	<p>It is the output signal of “Logic Solver”, part of a SIS, that will be sent to trip device in the plant or equipment, in order to set a final safety element in its NORMAL or SAFE state, which in conjunction with other ones, will move the plant/equipment operation to the SAFE condition.</p> <p>Normally a “SIF Output Signal” is a digital signal.</p>
<p>Signal</p>	<p>It is an indication, such as a gesture, colored light, electric current or electromagnetic field, which serves as a means of communication from one place to another one.</p>
<p>Soft Reset</p>	<p>Manual RESET command signal (see “Command signal, Manual RESET”) that is implemented in the ICSS HMI.</p>
<p>Spurious Trip</p>	<p>Refers to the shutdown of the process for reasons not associated with a problem in the process that the SIF is designed to protect (e.g., the trip resulted due to a hardware fault, software fault, transient, ground plane interference, etc.). Other terms used include nuisance trip and false shutdown.</p>
<p>Spurious Trip Rate</p>	<p>The expected rate (number of trips per unit time) at which a trip of the SIF can occur for reasons not associated with a problem in the process that the SIF is designed to protect (e.g., the trip resulted due to a hardware fault, software fault, electrical fault, transient, ground plane interference, etc.). Other terms used include nuisance trip rate and false shutdown rate.</p>
<p>SRS, Conceptual SRS</p>	<p>“<u>Safety Requirements Specification</u>” (SRS) document that is prepared during project detail design phase.</p> <p>It MAY NOT include the final selected devices information for SIF implementation, as well as verified information from VENDOR.</p> <p>BUT, it shall include the clear requirements for specifying SIF’s devices, how devices will be connected, which “Diagnostics” are required inside each device or as part of a configuration in the “Logic Solver” (or other systems), DCS-SIS communication, SIF HMI in DCS, etc.</p>
<p>SRS, Process Safety SRS</p>	<p>See “Conceptual SRS”.</p>
<p>SRS, Detailed Design SRS</p>	<p>“<u>Safety Requirements Specification</u>” (SRS) document that is prepared at the end of project detail design, or end of SIS FAT.</p> <p>It shall include the final SIF design/installation information and all the information missing or pending for verification in the “<u>Conceptual SRS</u>”.</p>
<p>SRS, Safety Requirements Specification</p>	<p>Specification containing the safety requirements for just one, or ALL, “Safety Instrumented Functions” (SIFs) that have to be performed by the “Safety Instrumented System” (SIS). In a project, it shall include: the associated target safety integrity levels, target Spurious Trip Rate, target Safety Time, Interlock/Reset procedures, interface logic with external systems, etc.</p>

T	
Stroke test	Proof test where a safety valve is stroked fully or partially from its NORMAL to its SAFE position, in order to verify that it is in good condition to perform its safety function when it is required.
Transmitter	Device that read the process variable value from the Sensor, next amplify/normalize/convert the process variable value to a standard communication protocol and sends that value (or SIF Input Signal) to the “Trip criterion”. Nowadays some communication protocols also send “Sensor/Transmitter” configuration and statuses information. Sometimes the “Sensor” and the “Transmitter” are contained in the same device. Example of this is a nowadays pressure transmitter.
Trip criterion	Logic to apply to one[1] (or more) “SIF input signal(s)” to determine if such value (or group of values) is (are) in the NORMAL or in the TRIP state. The simpler “TRIP criterion” consists in comparing an analogue SIF input signal value against its fix “Trip value” or “Trip setting”, to check if one value is greater or lesser than the other one.
Trip device	This device can be a Solenoid Valve (SOV), a relay, a “Smart Position Transmitter” (SmPosT), etc. The “Trip device” can be in the NORMAL or SAFE state. According to the “SIF Output Signal” nature that is connected to the “Trip Device”, its function in the SAFE state is one of the following: a) To interrupt the mechanism that makes the “Final Safety Element” to remain in its NORMAL state, next the “Final Safety Element” moves up to its SAFE state. This is equivalent to the “De-Energize to TRIP” philosophy. b) To start a mechanism that moves the “Final Safety Element” from its NORMAL state up to its SAFE state. This is equivalent to the “Energize to TRIP” philosophy. The “Trip device” in the NORMAL does the opposite as indicated above, making the plant/equipment to be in the NORMAL state.
Trip logic	See “Trip criterion”.
Trip setting	Value in which an analogue signal value, input of a SIF, shall be above or below to change such signal from the NORMAL state to the TRIP state.
Trip setting logic	See “Trip criterion”.
TRIP state	It is the value, position, mode or condition of a “SIF input signal” when such signal abandons the “NORMAL state”. This change is detected by a “Trip criterion”. When a “SIF input signal” is in the TRIP state, the “Voting Logic” will decide to change the “SIF output signal” to the SAFE state or not.
Trip value	See "Trip setting".
Type A element (SIF's Device)	“Non-Complex” SIF device. An element can be regarded as type A if, for the components required to achieve the safety function a) the failure modes of all constituent components are well defined; and b) the behaviour of the element under fault conditions can be completely determined; and c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.

<p>Type B element (SIF's Device)</p> 	<p>“Complex” SIF device (typically using microcontrollers or programmable logic). An element shall be regarded as type B if, for the components required to achieve the safety function,</p> <p>a) the failure mode of at least one constituent component is not well defined; or</p> <p>b) the behaviour of the element under fault conditions cannot be completely determined; or</p> <p>c) there is insufficient dependable failure data to support claims for rates of failure for detected and undetected dangerous failures (see 7.4.9.3 to 7.4.9.5).</p> <p>NOTE This means that if at least one of the components of an element itself satisfies the conditions for a type B element then that element will be regarded as type B rather than type A.</p>
--	--

U

<p>UnDetected Failure</p> <p>Safe Undetected Failure Rate (λ_{SU})</p> <p>Dangerous Undetected Failure Rate (λ_{DU})</p>	<p>In relation to hardware, UnDetected by the diagnostic tests, proof tests, operator intervention (for example physical inspection and manual tests), or through normal operation.</p> <p>EXAMPLE These adjectives are used in undetected fault and undetected failure.</p> <p>In relation to hardware and software faults not found by the diagnostic tests or during normal operation.</p> <p>NOTE This term deviates from the definition in IEC 61508-4 to reflect differences in process sector terminology.</p> <p>NOTE: in practice the above first definition SHALL NOT include automatic diagnostic test. ONLY proof tests and operator intervention shall apply.</p> <p>Interpretation: Failure that CANNOT be “Detected” by an automatic diagnostic test. Notification capability DOES NOT exist. BUT, it can be “Detected” by:</p> <ul style="list-style-type: none"> - Operator intervention (for example physical inspection and manual tests), or - Proof tests, or -- Normal operation observation. - By applying Maintenance.
--	--

V

<p>Voting logic</p>	<p>It is a logic to be applied to “Trip criterion” outputs, and/or more “SIF Input Signals”, in order to determine if their condition is in the NORMAL or in the TRIP state.</p> <p>This information is provided next to a “Logic Solver” which decides to trip (set in the SAFE state) or not the related plant/unit/equipment.</p> <p>From the SIL determination and PFD calculation point of view, the "Voting Logic" is a particular SCA that is applied to the "SIF input signals" only.</p> <p>See “Safety Channel Architecture”.</p>
---------------------	---

