

---

**ROWAN HOUSE** LTD

6 Hurst Green Precinct  
Off Woodbury Road  
Halesowen  
West Midlands  
B62 9RH  
Tel. 0121 422 3311

South Wales Office:  
Tel. 01656 745187

North West Office  
Tel. 0151 355 3588

**IEC 61508 and IEC 61511  
Safety Critical Instrumentation  
Glossary of terms**

**IMPORTANT:** This glossary of terms is intended as a quick guide to terminology and in some cases the explanation has been abridged. Thus the explanations for the terminology are not formal definitions.

**DISCLAIMER:** Rowan House Ltd accept no liability whatsoever for the use or interpretation of this glossary of terms. Users may only use this document at their own risk.

### INTRODUCTION

IEC61511 is the guidance for the process industry for the implementation of the master standard IEC61508. It is referred to in the USA as "S84" which is an abbreviation of the ANSI/ISA standard S84.01. Two-thirds of IEC61511 refers you to the relevant sections of IEC61508 so these standards are implemented together and never separately. The master standard, IEC61508, is a European norm.

Clive de Salis at Rowan House was the first Chair of the UK's 61508 Association and during the giving of talks and presentations around the country soon found that parts of the standard were misunderstood. We hope you find this quick glossary of terms helpful.

**Audit:**

A systematic examination to determine if all of the aspects of the safety system are being realised, thus ensuring that the loss-control objectives of the Company are achieved. The audit should be by independent persons working with those responsible for the system.

**As Low As Reasonable Practical. (ALARP):**

A term applied to the reduction of risk by taking measures to reduce risk to persons (between intolerable and negligible levels) until the cost of further measures is grossly disproportionate to the benefits they would deliver. This value is termed the tolerable value of risk.

**Common Mode Failures:**

A common mode failure is the result of an event or events, which, because of dependencies, causes a coincidence of failure states of components in two or more channels of a redundancy system, leading to the defined system failing to perform its intended function on demand.

**Demand (D):**

A plant abnormal condition which requires a SIF or other device to take appropriate action to prevent a hazardous event.

**Demand Rate:**

The frequency at which a SIF is required to perform its protective function. The demand may be continuous, (usually more often than once per year), when the availability of the SIF is directly a function of its failure to danger rate. Other wise it is a function of its reliability and testing.

**Diagnostic Coverage (Dc):**

Diagnostics provided to monitor, at frequent intervals, the operating condition of a device to identify if a fail to danger state exists. The amount of coverage is a function of the monitoring design.

**Diversity:**

Different means of achieving a safety function with minimum common mode, e.g. Low Pressure with Flame Monitor to measure for burner 'flame out' problems.

**E/E/PE:**

Electrical / Electronic/Programmable Electronic devices based on Electrical and/or Electronic and/or Programmable Electronic technology.

**E/E/EPs:**

A system based on one or more E/E/EP devices connected to Input and Output devices.

**Emergency Shutdown System (ESD):**

A system, usually implemented as an independent system from the plant control system. For high safety integrity levels it is normal to avoid software based systems.

**Equipment Under Control (EUC):**

Equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities.

**Fail Safe:**

A design property of an item or system which, on failure places the monitored unit into a safe state.

**Failure:**

The termination of the ability of a system hardware element to perform its designed function. (Note: hardware can fail but software can only have faults.)

**Fault Tree:**

A logic diagram showing which fault modes of sub-items or external events, or combinations thereof, result in a given fault mode of the item.

**Functional Safety:**

The ability of a safety related system to carry out the actions necessary to bring the plant to a safe state.

**Fractional Dead Time (FDT):**

Average probability of being in a failed state and is related to the proof test interval. (See also PFDavg).

**Fail to danger detected (Fdd):**

The failure rate to danger of the component/sub-system/system that is revealed by any diagnostics.

**Fail to danger undetected (Fdu):**

The failure rate to danger of the component/sub-system/system that is un-revealed by any diagnostics. This typically refers to automated diagnostics and the failure is only discovered when the item is being proof-tested.

**Fail to safe (Fs):**

The failure rate to safe of the component/sub-system/system that is revealed, usually by placing the plant into its safe state. (spurious trip rate)

**Hardware Fault Tolerance (HFT):**

The ability of a component/sub-system/system to continue to carry out its design function with different failure levels. The level of HFT required of a SIF is a function of its Safe Failure Fraction, and its required SIL.

**Hazard and Operability study (HazOp):**

Hazard and Operability study. This involving a small team of competent personnel checking

through the plant Piping and Instrument Drawings (P&ID) and other related information in a systematic manner against a checklist of guide words. The results of HazOp review is an identification of the hazards, risks and existing risk reducers. The results of the HazOp are then used to determine the requirement for a SIF and its SIL.

**HAZAN:**

A methodology for identifying hazards.

**Harm:**

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

**Hazard:**

A physical situation with the potential to cause Injury / death to personnel and / or environment damage and / or damage to equipment.

**Hazardous Situation:**

Circumstance in which a person (or environment) is exposed to hazard(s)

**Hazardous Event:**

Event causing actual damage, or danger, generally as a result of failure - of control, or of containment.

**Logic System:**

The part of the safety system that performs the appropriate safety function, excluding sensors and operated elements.

**Mean Time to Repair (MTTR):**

The time from a diagnostic alarm and/or proof test failure to restore the item to normal operation.

**Proof Test:**

A test performed in a defined manner, to detect un-revealed failures in the safety system so that the system can be restored to "as new" or as close as practical. The proof test may be conducted at different intervals for each sub-system, be on-line and only test part of that sub-system = test coverage, (Tc). When testing does not achieve a 100% test of the SIF then a 100% test is required at some point in its life. This is usually at the maintenance interval, (Tm).

**Protective System:**

An instrument protective system used in SIL 1 to SIL 4 applications. [See Safety Integrity Level].

**PFDavg:**

Average probability of failure on demand of a safety-related protection system.

**'Proven in use'**

Documented evidence of reliability that shows that the component/sub-system/system is suitable for use in a SIL rated SIF

**Risk:**

A combination of the probability of occurrence of harm and the severity of the harm.

**Residual risk:**

The risk remaining after protective measures have been taken.

**Risk Reduction Factor (RRF):**

The inverse of PFDavg.

**Safety Function (SF):**

The function to be implemented by an E/E/PE safety related system, other technology safety-related system or external risk reduction facilities, which is intended to achieve or maintain a safe state for the plant, in respect to a specific hazardous event.

**Safe Failure Fraction (SFF):**

That fraction of all failures associated with a component/ sub-system/system that are either self-revealing, (usually placing the plant into a safe state). Alternatively, are identified by diagnostics.  $SFF = (F_{dd} + F_s) / (F_{dd} + F_s + F_{du})$

**Safety Integrity:**

Probability of a safety-related system performing the required safety functions under all the stated conditions, within a stated period of time.

**Safety Integrity Level (SIL):**

1 to 4 discrete levels defining the probability of failure (required reliability) of the safety system to perform its design function under stated conditions.

**Safety Instrumented Function (SIF):**

The safety function (see SF above), the basic instrument loop and its philosophy of operation.

**Safety Instrumented System (SIS):**

A term not used by IEC 61508, but today generally used as a synonym for the term safety-related system containing a single SIF or multiple SIFs in a shutdown system.

**Safety-Related System (SRS):**

A designated system that both -

Implements the required safety functions necessary to achieve or maintain a safe state for a plant; and contributes on its own or with other safety-related systems/ risk reducers the necessary risk reduction, to acceptable levels, of risk of -

- serious harm / death to personnel, or environmental damage,

- or to meet legal requirements.

It may also be used to prevent significant damage to equipment that could result in major financial costs and loss of customers.

**Tolerable Hazard Rate (THR):**

THR is expressed as events per year. THR may be used for determining the target integrity of an SIF.

**Tolerable risk:**

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