An Introduction to AD Safety Systems Terminology and Definitions

Functional Safety Management

Functional Safety Management is the term used to describe the overall safety of a plant or process. It sits above the safety and design of individual components or pieces of equipment and focuses on how they are integrated together to construct a plant or process. It assesses whether the system or equipment is designed to operate correctly in response to its inputs, including the safe management of likely operator errors, hardware failures and wider environmental changes. The standards which govern it are BS EN 61508 and IEC 61511; these are now the universal standard by which the Health and Safety Executive measures safety systems. As part of Functional Safety Management, there are a number of regulations and formal assessment methods used. It is important to remember that compliance of a whole system is required, not a certificate for each individual component.

HAZOP – Hazard and Operability Study

- A methodology for identifying and dealing with potential problems in industrial processes, particularly those which could cause a hazardous situation or a severe impairment of the process. It applies to existing or planned processes, provided design specifications and information are available.
- Comprises a committee of all involved in the operation, design and construction of the process. There is a Chair, who should be experienced but not involved in the process. Also a Secretary. The remainder of the committee can vary with roles such as designer, user/operator, constructor, maintainer etc being involved.
- The output is a structured report, giving a qualitative assessment of each part of the process. Typical headings would be:
  - Deviation, Cause of Deviation, Consequences, Existing layers of safety, possible action

DSEAR – Dangerous Substances and Explosive Atmosphere Regulations 2002

- Combination of 2 EU directives – ATEX 137 Safety of Workers in potentially explosive atmospheres and Chemical Agents Directive, brought together by the Health and Safety Executive (HSE) as DSEAR.
- HSE Approved Codes of Practice and Guidance (ACOP) gives a list of topics and provides the HSE interpretation of the requirements of DSEAR. It covers:
  - Dangerous Substances and Explosive Atmospheres
  - Design of plant, equipment and workplaces
  - Storage of dangerous substances
  - Control and mitigation measures
  - Safe maintenance, repair and cleaning procedures
- In addition, there is guidance for dust related explosive atmospheres: HSE Safe Handling of Combustible Dusts
- In Europe, they only have Explosive risks covered (“EAR”). Hence, a system installed by a European company in the UK may only cover “Explosive” and not have considered the “Dangerous” side – this needs to be considered and addressed.

SIL – Safety Integrity Level

- SIF describes the system; SIL describes the reliability required
- A SIL loop is an electronic safety system implemented to take over should there be a failure in the underlying process which would otherwise create an unacceptable level of risk. If the process itself is capable of meeting and dealing with all the levels of risk deemed adequate, there is no need for a SIL. With proper consideration of safety requirements at the early stages of plant design through the HAZOP process, it is unlikely that there would be a need for SIL loops in a normal AD Plant.
- SIL loops are rated as follows:
  - SIL 1 = a loop that reduces the risk of catastrophe on failure by > 10
  - SIL2 = > 10^2
If a SIL 3 or 4 loop is deemed appropriate, it raises questions about the suitability of design, construction and operation of the process in the first place.

The level of safety required over the life of a process can change due to increasingly tighter regulation. Hence, a system designed with a level of safety deemed acceptable at the time may not have the level of safety now deemed appropriate. It may, therefore, need a SIF with a much higher SIL rating than in the past.

Generally components of a system, such as plc, transmitter, valve, will have SIL certificates. However, these are of no value in the overall system. What is needed is the safety report specifying the operational parameters in which the item was tested. These reports, together with the design of the way in which the system is integrated and constructed, then provide the overall level of the total control process.

Other Standards, Definitions and Organisations

- HSE – Health and Safety Executive
- SIESO – Society of Industrial Emergency Services Officers
- COMAH – Control of Major Accidents and Hazards. Regulations. Sites are graded and the HSE is generally only interested in top-tier COMAH sites. AD Plants will generally be in the lower tiers
- BS EN 61508, also known as IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems. They require that the company/organisation makes a conscious decision on the level of tolerable risk for a system. There is no set value proscribed. If, however, a company has issued a COMAH report, then the fatal accident rate is specified in it. That same value must be used for the SIL assessment Industry bodies may give recommended levels
- UKAS – UK Accreditation Service. Covers the Certification of functional safety management, (valid internationally)
- ATEX – French standard for Europe – Atmosphere Explosif (EAR in DSEAR)

Hierarchy of Importance

1. UK Law – Health and Safety at Work act
2. UK Government Department regulations
3. EU Law – see “EN” on a standard etc.
4. HSE Guidance – Approved Code of Practice - ACOP
5. British Standards
6. International Standards
7. Industry Codes of Practice
8. Industry guidance/other guidance