E-training

"Welcome to the K Controls e-training course designed to deliver useful "Pneumatic Valve Actuation" application information in small instalments."

To unsubscribe or to register a colleague to receive these documents Click here

Safety integrity levels (SIL 1 to 4) (IEC 61508/61511)

Risks in a process plant can be minimized but they can never be completely eliminated. They will depend on the nature of the processes, the degree of automation and the possible impact on the surrounding area. The functional safety of field instrumentation and associated control and monitoring systems must be optimized via a disciplined approach to fault identification, prevention and control.

What is a functional safety system?

At its simplest a functional safety system detects a potentially dangerous condition and causes corrective or preventative action to be taken.

Typically a system will comprise a sensor which provides information on the value of a variable, a processor which compares the value with a predetermined limit and initiates action and an actuator which either corrects the variable or performs an emergency function.

Apart from the reference to danger, this description could be applied equally to the process controls for the equipment performing its function. In the past it was regarded as essential that the safety function operated independently from the process function. The advent of microprocessors has enabled vast amounts of data to be collected and analysed in real time thus providing the possibility of sophisticated safety systems including such features as self-diagnosis. With many different parties involved in the specification, design, manufacture, installation, operation and maintenance of safety systems, the need for a standardised approach was recognised and IEC 61508 is the result.

What is IEC 61508?

IEC 61508 is the international standard for electrical, electronic and programmable electronic safety related systems. It sets out the requirements for ensuring that systems are designed, implemented, operated and maintained to provide the required safety integrity level (SIL). Four SILs are defined according to the risks involved in the system application, with SIL4 being used to protect against the highest risks. The standard specifies a process that can be followed by all links in the supply chain so that information about the system can be communicated using common terminology and system parameters.

The standard is in seven parts:

IEC 61508-1, General requirements
IEC 61508-2, Requirements for E/E/PE safety-related systems
IEC 61508-3, Software requirements
IEC 61508-4, Definitions and abbreviations
IEC 61508-5, Examples and methods for the determination of safety integrity levels
IEC 61508-6, Guidelines on the application of IEC 61508-2 and IEC 61508-3
IEC 61508-7, Overview of techniques and measures

E-training

K Controls designs and manufactures valve networking monitoring and control products:

Switchboxes
Control Monitors
Position Transmitters
Corrosion resistant
ATEX certified – gas + dust
High and low temperatures
IP68 for submersion
Low powered solenoids
Remote I/O compatible
AS-interface®
DeviceNet™
PROFIBUS® PA
FOUNDATION™ FIELDBUS
4-20mA + HART®
Wireless solutions
Linear or rotary adaptation

K Controls can also supply your positioner requirements

IEC 61508 has been adopted in the UK as BS EN 61508, with the "EN" indicating adoption also by the European electro technical standardisation organisation CENELEC. Other standards are being produced for the application of the 61508 approach to particular sectors. Sector specific standards related to IEC 61508 include:

IEC 61511	Process industries
IEC 61513	Nuclear power plants
IEC 62061	Machinery sector
IEC 61800-5-2	Power drive systems.

BS IEC 61511: 2003 Functional safety - Safety instrumented systems for the process industry sector

Safety instrumented systems - do they meet minimum standards and performance levels?

SIS's have been used for many years to perform safety instrumented functions in chemical, petro-chemical and gas plants as well as in non-nuclear power generation. But in order for instrumentation to be effectively used for safety instrumented functions, it is essential that the instrumentation achieves certain minimum standards and performance levels.

To reach these standards, new BS IEC 61511:2003 Functional safety - Safety instrumented systems for the process industry sector should be utilised. The standard addresses the application of SISs for the process industries, and requires a process hazard and risk assessment to be carried out to enable the specification for SISs to be derived. The SIS includes all components and subsystems necessary to carry out the safety instrumented function from sensor(s) to final element(s).

The standard is intended to lead to a high level of consistency in underlying principles, terminology and information within the process industries. This should have both safety and economic benefits.

The standard comes in three parts:

Part 1: Framework, definitions, system, hardware and software requirements gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. It has been developed as a process sector implementation of IEC 61508.

Part 2: Guidelines for the application of BS IEC 61511-1, which will give guidance on how to comply with Part 1.

Part 3: Guidance for the determination of the required safety integrity levels provides information on the underlying concepts of risk, the relationship of risk to safety integrity, the determination of tolerable risk, and the number of different methods that enable the safety integrity for the safety instrumented functions to be determined.

E-training

K Controls designs and manufactures valve networking monitoring and control products:

Switchboxes
Control Monitors
Position Transmitters
Corrosion resistant
ATEX certified – gas + dust
High and low temperatures
IP68 for submersion
Low powered solenoids
Remote I/O compatible
AS-interface®
DeviceNet™
PROFIBUS® PA
FOUNDATION™ FIELDBUS
4-20mA + HART®
Wireless solutions
Linear or rotary adaptation

K Controls can also supply your positioner requirements

It is strongly recommended that attention is paid to the BS EN 61508 series on Functional safety of electrical/electronic/programmable electronic safety-related systems as BS IEC 61511 sits within the framework of BS EN 61508.

Safety integrity levels (SIL)

Both the BS EN 61508 and BS IEC 61511 standards divide systems and risk reducing measures into four safety levels, these ranging from SIL 1 (indicating a low risk) to SIL 4 (indicating an extreme risk).

Definition of Systems risk

Extent of damage (S)

S1 = Injury of a person, insignificant environmental damage

S2 = Severe, irreversible injury of one or more persons, death of a person, severe or temporary environmental damage.

S3 = Death of several persons, severe, permanent environmental damage

S4 = Death of a large number of persons

Presence of a hazardous area (A)

A1 = Seldom to often

A2 = frequently to continuously

Avoidance of danger (G)

G1 = Possible under certain circumstances

G2 = practically impossible

Probability of an undesired situation arising (W)

W1 = Very slight

W2 = Slight

W3 = Relatively high

These different risk parameters can then be graphed to arrive at a SIL level.

Example: S2 + A1+G1+W3 = SIL 1

Risk reducing measures

The values SIL 1 to SIL 4 are derived from this process of risk analysis. The greater the risk, the more important it is to implement reliable risk reduction measures and, consequently, greater use must be made of highly reliable components.

System risk reduction

The reliability of a safety system can be measured using the following parameters;

PFD = Probability of failure on demand (for low demand mode of operation)

E-training

K Controls designs and manufactures valve networking monitoring and control products:

Switchboxes
Control Monitors
Position Transmitters
Corrosion resistant
ATEX certified – gas + dust
High and low temperatures
IP68 for submersion
Low powered solenoids
Remote I/O compatible
AS-interface®
DeviceNet™
PROFIBUS® PA
FOUNDATION™ FIELDBUS
4-20mA + HART®
Wireless solutions
Linear or rotary adaptation

K Controls can also supply your positioner requirements

The PFD for the complete system is derived from the values of the individual components.
As field mounted sensors and actuators are exposed to greater environmental stresses the risk associated with these components is relatively high.

For systems operating in high demand or continuous mode of operation the probability of failure on demand (PFD) is replaced with probability of a dangerous failure per hour (PFH)

Allocation of total system PFD:

35% for sensor system and signal path to PLC
50% for actuation system and signal path from PLC
15% for the PLC

SFF = Safe failure fraction

Failures in a safety system can be dived into:

SD = Safe detected failures
SU = Safe un-detected failures
DD = Dangerous detected failures
DU = Dangerous undetected failures

The SFF = SD + SU as a proportion of the total of all failures

HFT = Hardware Fault Tolerance

This is the maximum number of hardware faults which will not lead to a dangerous failure.
If HFT = 0 it means that a single fault can cause a dangerous failure.

Example: If a component has an SFF in the range 60 to 90% and an HFT of 0 it would be defined as SIL 2. If the HFT was 1 this would increase to SIL 3.

T proof = the time interval between functional viability tests of the entire system including its mechanical components.

The shorter the test interval the greater the probability that the safety system will function in the correct manner.

As an example a Namur proximity switch that K Controls offers in the 007 Switchbox has an SFF of greater than 68% and a PFD of 4.82E-05
(4.82×10^{-5}).

T proof = 1 year. This enables it to be used in a SIL 2 environment.

E-training

K Controls designs and manufactures valve networking monitoring and control products:

Switchboxes
Control Monitors
Position Transmitters
Corrosion resistant
ATEX certified – gas + dust
High and low temperatures
IP68 for submersion
Low powered solenoids
Remote I/O compatible
AS-interface®
DeviceNet™
PROFIBUS® PA
FOUNDATION™ FIELDBUS
4-20mA + HART®
Wireless solutions
Linear or rotary adaptation

K Controls can also supply your positioner requirements

If you have any questions or comments, would like a colleague to receive this information or you would like the latest list of training documents, please use the contact details below:

K Controls Ltd
2 Crown Way
Crown Business Centre
Horton Road
West Drayton UB7 8HZ
United Kingdom

Phone:
+44 (0)1895 449601

Fax:
+44 (0)207 990 8111

E-mail:
sales@k-controls.co.uk

Web:
www.k-controls.co.uk

Blog:
www.k-controls.info

Visit us:
View a map

The PFD of the system PFD_{sys} is the sum of sensor subsystem PFDs, logic subsystem PFD_L and final element subsystem PFD_{FE}

$$PFD_{sys} = PFD_s + PFD_L + PFD_{FE}$$

Or for continuous of high demand systems

$$PFH_{sys} = PFH_s + PFH_L + PFH_{FE}$$

This summary is only a brief overview; please refer to the standards for more detailed information.

Further reading

Book details - Safety Integrity Level Selection - Systematic Methods Including Layer of Protection Analysis :

http://www.isa.org/Template.cfm?Section=Books&Template=/Ecommerce/ProductDisplay.cfm&ProductID=4517

Article : Buses in safety instrumented systems:

http://www.isa.org/Content/ContentGroups/InTech2/Departments/Safety1/20049/Buses_in_safety_instrumented_systems.htm