DETERMINATION OF SAFETY REQUIREMENTS FOR SAFETY-RELATED PROTECTION AND CONTROL SYSTEMS - IEC 61508

Simon J Brown
Technology Division, Health & Safety Executive,
Bootle, Merseyside L20 3QZ, UK

The methodology for the determination of safety requirements of safety-related systems adopted by the international standard IEC 61508, Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems is reviewed. The process of determining overall safety requirements from a hazard & risk analysis and how this leads to a safety requirements specification (in terms of safety functions and associated safety integrity levels) is described. The concept of the 'process safety time' and how it relates to requirements for the diagnostic test interval of the safety-related system is explained.

INTRODUCTION

Whilst hazards, whenever possible, should be eliminated using the principles of inherent safety, there are many applications where this is not practical and where it is necessary to put in place arrangements to reduce risks associated with chemical processes to tolerable levels. Often, safety-related systems based on electrical, electronic or programmable electronic (E/E/PE) technology are used to effect such risk reduction (for example, emergency shut down systems and fire / gas detection systems). The aim of IEC 61508[1] is to ensure that the safety integrity of such E/E/PE safety-related systems is adequate to achieve functional safety. This is achieved by first determining the safety requirements for the E/E/PE safety-related systems using a systematic risk based approach. This takes into account the hazards and risks associated with the process and process control system, together with any contributions to overall safety provided by other technology safety-related systems and risk reduction facilities. To be effective, it is important that this activity takes place at a very early stage in the design of the arrangements necessary to ensure the safety of the process and it will often form part of the intial process hazard analysis. It is therefore important that those involved with this activity are familiar with the concept of safety functions in the context of IEC 61508.

OVERALL SAFETY REQUIREMENTS

HAZARD & RISK ANALYSIS

One of the first steps in the IEC 61508 methodology is to undertake an analysis to determine the hazards and risks associated with the so-called 'equipment under control' (EUC) and the EUC control system. This is termed the 'EUC risk'. In chemical process applications this is the risk associated with the process and process control system. At this stage, no account is taken of any safety-related systems or other risk reduction measures. The aim is, for each hazard, to assess the nature and extent of the 'unmitigated' risk in terms of consequence and frequency of the hazardous event. This is typically undertaken using the fault tree analysis technique. It should be noted that IEC 61508 places a lower limit on the dangerous failure rate that can be claimed for the EUC control system of 10^{-5} dangerous failures per hour, unless the control system is itself designed according to the requirements of the standard. This is to prevent unrealistic claims being made for the risk reduction of a control system in order to ease the requirement on the safety-related system.

TOLERABLE RISK

The next stage is, for each hazard, to determine the tolerable risk, again in terms of consequence and frequency. IEC 61508 does not give any specific guidance as to what might be regarded as a tolerable risk, but general advice is given in IEC 61508-5 on how tolerable risk might be determined using the 'ALARP' (as low as is reasonably practicable) model. Also, a discussion document which addresses this matter has recently been published by the Health & Safety Executive[2]. In practice, the tolerable risk will depend on many factors (for example, severity of injury, the number of people exposed to danger, the frequency at which a person or people are exposed to danger and the duration of the exposure). Important factors will be the perception and views of those exposed to the hazardous event. In arriving at what constitutes a tolerable risk for a specific application, a number of inputs are considered. These include:

— guidelines from the appropriate safety regulatory authority;

— discussions and agreements with the different parties involved in the application;

— industry standards and guidelines;

— international discussions and agreements – the role of national and international standards are becoming increasingly important in arriving at tolerable risk criteria for specific applications;

— the best independent industrial, expert and scientific advice from advisory bodies;

— legal requirements – both general and those directly relevant to the specific application;

— individual and societal concerns.

RISK REDUCTION

Where the EUC risk associated with any of the hazards exceeds the tolerable risk, then it is necessary to put in place measures to reduce the risk to at least the tolerable level. This can be achieved by reducing either the frequency of the hazardous event, or the consequences associated with the hazardous event or by reducing both the frequency and consequence of the hazardous event (see Figure 1). The measures employed to bring about the required risk reduction can comprise safety-related systems using E/E/PE or other technologies (for example, mechanical pressure relief systems), or external risk reduction facilities (such as fire walls, bunds, etc.). The measures employed to effect the necessary risk reduction are sometimes referred to as layers of protection. In some applications it may be possible to obtain the necessary risk reduction from a single layer of protection (e.g. a pressure relief valve). However, particularly when higher levels of risk reduction are required, there are benefits to be gained by employing a number of different measures (sometimes referred to as layers of protection) to protect against any one hazard, particularly if the layers are independent so that a failure in any one layer does not promote a failure in another. This both eases the safety integrity requirements of any one layer and provides protection against the failure of any one layer. IEC 61508 refers to the process of sharing risk reduction between different layers of protection as 'allocation'. This is sometimes referred to as 'layer of protection analysis'[3]. The concept of allocating risk reduction to different types of protection is illustrated in Figure 2.

SAFETY FUNCTIONS & SAFETY INTEGRITY

The requirements for each layer of protection, in terms of the functional action required, and the probability with which the action will be successfully carried out, are together referred to in IEC 61508 as a 'safety function'. It is vital that the necessary risk reduction for each hazard is accurately captured in the specification of the safety functions. In general, safety functions are specified in terms of both the functional requirement and the safety integrity requirement to achieve the required risk reduction. The first stage in the development of a specification for a safety function is the determination of the functional requirements and safety integrity requirement. The functional requirement is a precise description of the action required to achieve the necessary risk reduction. The safety integrity requirement is is a measure of the likelihood that the required function will be successfully carried out. These requirements are, in principle, determined before the safety functions are allocated to the various types of safety related system or risk reduction facilities. The safety integrity requirement of a safety function is determined by the risk reduction which is effected by the safety function and may be derived using either quantitative or qualitative techniques. Having determined the safety integrity requirements for the safety functions, they are then allocated to the E/E/PES safety-related systems, other technology safety related systems and external risk reduction facilities in such a way that the required risk reduction is achieved for each hazard. This process results in target performance measures for all the types of safety-related system and risk reduction facilities used. However, IEC 61508 only specifies requirements for E/E/PE safety-related systems and it is therefore assumed that techniques for the implementation of other technology safety-related systems and external risk reduction facilities (to achieve the safety integrity requirements which have been allocated to those systems) are available elsewhere. For those safety functions which are allocated to E/E/PES safety-related systems, the standard defines 4 safety integrity levels (SILs). This approach allows the grading, according to the required risk reduction, of the measures and techniques recommended by the standard for the avoidance and control of systematic faults. Also, IEC 61508 defines a range of target failure probabilities for each SIL, see Table 1. These form the targets for the quantified reliability requirements of the safety functions. There are 2 basic types of safety functions - those which operate 'on demand' and those which operate continuously.

LOW DEMAND MODE SAFETY FUNCTIONS

An example of an 'on demand' safety function is a trip which operates to take some action, for example, closing a feed valve, when some process variable, for example, pressure in a vessel, exceeds some set limit. The target failure measure for a demand mode safety function is the probability of failure on demand (PFD). A demand mode safety function typically provides the required risk reduction by reducing the frequency of a hazardous event whist maintaining the same consequence. In such circumstances the required risk reduction can readily be quantified:

Risk in the absence of the safety function, $R_{np} = F_{np} . C$ (1)

Tolerable risk, $R_t = F_t . C$ (2)

where F_{np} = frequency of the hazardous event with no protective safety function in place
F_t = tolerable frequency of the hazardous event
C = consequence associated with the hazardous event

therefore:

Required risk reduction factor, $\Delta R = R_{np} / R_t = F_{np} / F_t$ (3)

For a demand mode safety function:

$F_p = PFD \, . \, F_{np}$ (4)

where F_p = frequency of the hazardous event with the safety function in place
PFD = probability of failure on demand of the safety function

therefore the PFD required to achieve the necessary risk reduction is given by:

$PFD = F_t / F_{np} = 1 / \Delta R$ (5)

The SIL of the safety function is determined according to Table 1.

On this basis, the ranges of target failure probabilities relating to each SIL can also be related to ranges of risk reduction factors, see Table 2.

In other situations a demand mode safety function may reduce the consequence of a hazardous event. An example of such a safety function is a water deluge which operates to reduce the consequences (fire and explosion) associated with a leak of some flammable liquid or gas. IEC 61508 does not provide any explicit methodology for the determination of the safety integrity level of the safety function in such circumstances. One possible approach results from the consideration that tolerable risk is a measure of risk which takes account of both the consequence and likelihood of a hazardous event. In this situation, the risk reduction effected by the safety function is given by:

Risk reduction = F_m / F_u

where F_m = tolerable frequency of the mitigated hazardous event
F_u = tolerable frequency of the unmitigated hazardous event

The risk reduction factor can then be mapped to a SIL according to Table 2.

IEC 61508 regards safety functions having a demand rate of less than one per year and no greater than twice the proof test frequency as operating in the ‘low demand mode’, and the target failure measure for such safety functions is determined according to the PFD requirements of Table 1. If the demand rate exceeds 1 per year, or is greater than twice the proof test frequency, then the safety function is regarded as operating in the ‘high demand / continuous mode’ and the target failure measure for the safety function is defined in terms of the probability of dangerous failure per hour, according to Table 3.

HIGH DEMAND / CONTINUOUS MODE SAFETY FUNCTIONS

An example of a truly continuous mode safety function would be a temperature control loop which is required to maintain temperature at all times below some upper limit. Examples of such safety functions are rare in process applications, where safety functions typically operate

as ‘trips’ on demand. However, as outlined above, IEC 61508 also treats demand mode safety functions which operate with a demand rate greater than 1 per year, or greater than twice the proof test frequency as operating in the ‘high demand / continuous mode’. The concept of risk reduction is of limited value in determining the safety integrity requirements of such safety functions. Instead, the target failure measure may be determined directly by the tolerable frequency of the hazardous event which is being mitigated by the safety function. This is expressed in terms of the probability of dangerous failure per unit time, T (e.g. dangerous failures per hour). This is equivalent to the dangerous failure rate (λ) of the safety function provided that $\lambda T << 1$. Again, IEC 61508 defines 4 levels of safety integrity for safety functions implemented in E/E/PE safety-related systems, see Table 3.

Process Safety Time

Where a continuous / high demand safety function relies on a single channel system (that is, a system having no redundancy), then IEC 61508 requires that the diagnostic tests within the E/E/PE safety-related system are able to detect faults quickly enough to allow action to be taken to achieve a safe state (e.g. shut-down of the process) before any fault in the process or the process control system could lead to a hazardous event. The process safety time is defined by IEC 61508 as the period of time between a failure occurring in the EUC or the EUC control system and the hazardous event if the safety function is not performed.

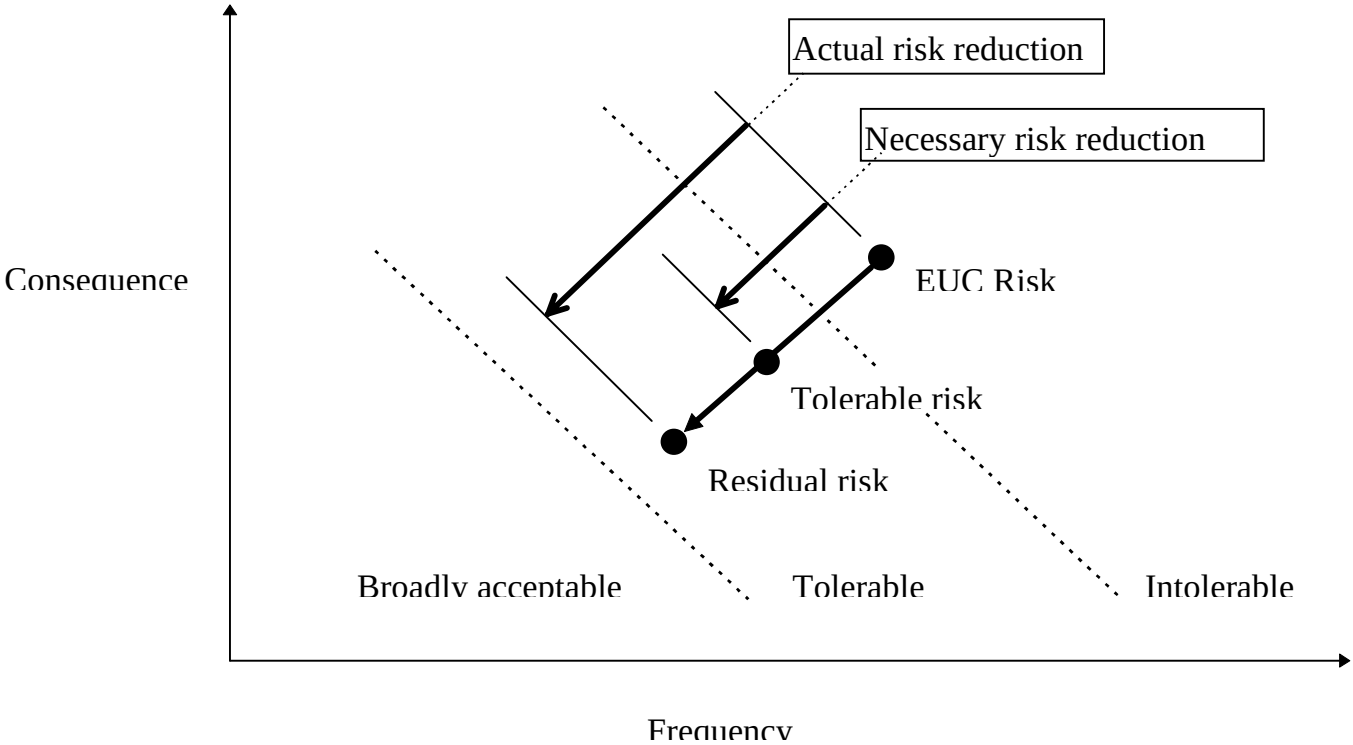
CONCLUSIONS

The effective application of IEC 61508 requires a fundamental understanding of the process and process control system and the associated hazards and risks in order to derive the safety requirements for E/E/PE safety-related systems. The methodology requires that the risk reduction provided by safety-related systems or protection measures of other technologies is taken into account and that safety functions allocated to E/E/PE safety-related systems are specified in terms of both functionality and safety integrity levels. IEC 61508 requires that the safety integrity level of a safety function be determined by the risk reduction required to achieve tolerable risk. The risk reduction may be achieved by either the reduction in frequency of the hazardous event, or by a reduction in the consequence, or a combination of both. Safety functions may operate in the low demand mode (typical for a protection system) or in the high demand / continuous mode. In the case of the latter, knowledge of the process safety time is necessary in order to allow the effective application of fault detection diagnostics.

REFERENCES

1. IEC 61508 - Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems, IEC, Geneva, 1998
2. Health & Safety Executive, 1999, Reducing Risks Protecting People (Discussion document)
3. Center for Chemical Process Safety of the American Institute of Chemical Engineering, guidelines for the Safe Automation of Chemical Process, ISBN 0-8969-0554-1, 1993

Figure 1 Risk terminology



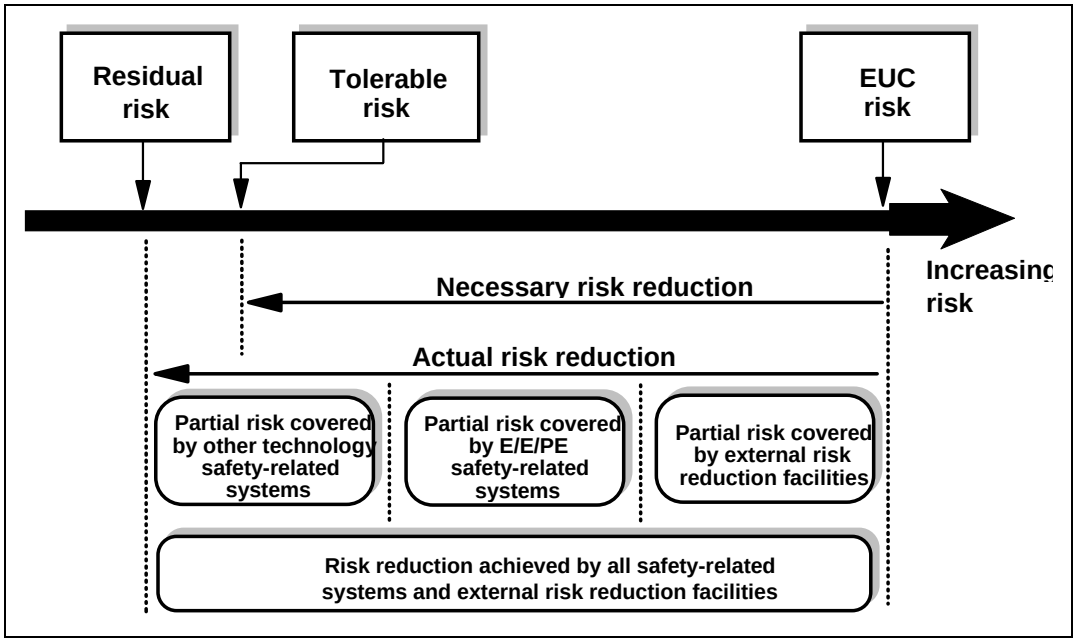


Figure 2 Risk reduction concepts

Safety Integrity Level of the Safety Function	Probability of Failure on demand (PFD) of the Safety Function
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Table 1 Target Failure Measures for Demand Mode Safety Functions

Safety Integrity Level of the Safety Function	Risk Reduction Factors
4	$\geq 10^{4}$ to $< 10^{5}$
3	$\geq 10^{3}$ to $< 10^{4}$
2	$\geq 10^{2}$ to $< 10^{3}$
1	≥ 10 to $< 10^{2}$

Table 2 Risk Reduction Factors of Safety Functions

Safety Integrity Level of the Safety Function	Probability of Dangerous Failure per hour
4	$\geq 10^{-9}$ to $< 10^{-10}$
3	$\geq 10^{-7}$ to $< 10^{-9}$
2	$\geq 10^{-6}$ to $< 10^{-7}$
1	$\geq 10^{-5}$ to $< 10^{-6}$

Table 3 Target Failure Measures for Continuous / High Demand Safety Functions