IEC61508-COMPLIANT SAFETY SYSTEM

AKAI Hajime [*1]

The ProSafe-RS Safety System has been developed in compliance with the IEC61508 international functional safety standard and has been certified by a third-party certification body as conforming to the standard. This international standard is based on risk management concepts and is widely accepted across the process industry for plant safety. In this article, we will discuss the main points of IEC61508, the concept of risk management and the standard's requirements for safety systems.

INTRODUCTION

The recent variety of industrial and railway accidents happening right before our very eyes make us painfully aware that "safety" must be put first and foremost. "Safety first" is a concept accepted by everyone and there is no room for disagreement. However, the author feels that, in some cases, the concrete objectives of "safety first" are not actually clear, and the grasp of the hazards is insufficient.

With regard to industrial safety, the IEC61508, which is the international standard for safety systems, sets down a policy of deciding on quantitative goals for risk reduction and for realizing those goals using concrete means. This approach to safety has been slow to gain popularity in Japan compared with Europe and the United States, but it has been gaining a lot of attention as companies reflect on the industrial accidents and the like which have occurred over the past few years. This approach to safety, which has this standard as its background, bases its line of thinking on the idea that safety is "absence of intolerable risks," rather than the conventional idea of safety as being "a non-hazardous state." When we assume that there are no defects in a means for ensuring safety, we work to eliminate defects in that safety means, but this means that we ignore taking steps to prepare for the remote possibility of a defect occurring. Even if one safety means is adopted, there is no such thing as a perfect system, so thinking in terms of a hierarchical system of protection becomes inescapable: that is, one has to adopt another safety means outside of the first one to cover any remaining risks. If the second means still fails to provide a level of tolerable residual risks, then one must adopt yet another safety means, and so on. In this hierarchy, quantitative goals for the risk reduction of the safety means in each layer are clearly defined. In the safety systems discussed in this paper, the quantitative targets for contributing to risk reduction are specified and how to achieve those targets are the key technical points.

By way of a technical explanation, in the following pages, this paper focuses on describing the part of international safety standard IEC61508, used as the criterion of safety systems, which relates to risk management and the part in which realization of safety systems is specified.

RISK REDUCTION IN IEC61508

The title of IEC61508 is "Functional safety of electrical/electronic/programmable electronic safety-related systems" and the title of Japanese standard JIS C 0508 prepared by translating this international standard IEC61508 is the same as above, of course, in Japanese. This standard is applicable to any cases for achieving safety using an electrical circuit, electronic circuit, or a programmable electronic system (E/E/PES: Electrical/Electronic/Programmable Electronic System), as shown by its title. Process industries, machine manufacturing industries, traffic and transportation, medical equipment, etc., are introduced as the major industries it applies to. In 2003, IEC61511 (Functional safety: Safety Instrumented System for the process industry sector) was published under the umbrella of IEC61508 for process industries which employ this standard most frequently. "Safety Instrumented System" is applied to emergency shutdown systems and fire and gas protection systems in industrial plants.

*1 IA Systems Business Division, IA Business Headquarters

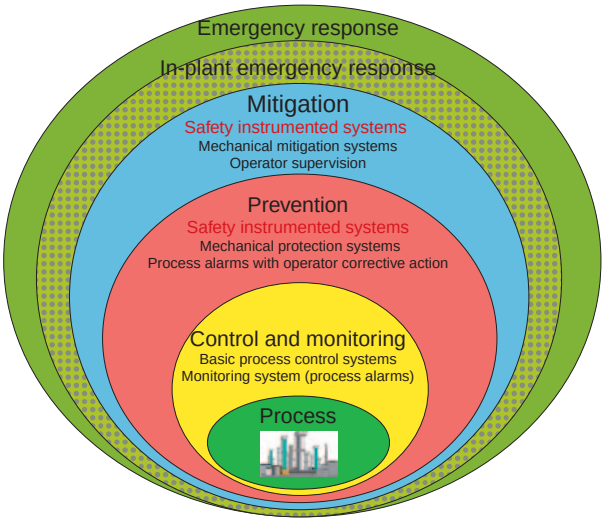

Figure 1 Hierarchical Plant Protection and Safety Instrumented System (SIS)

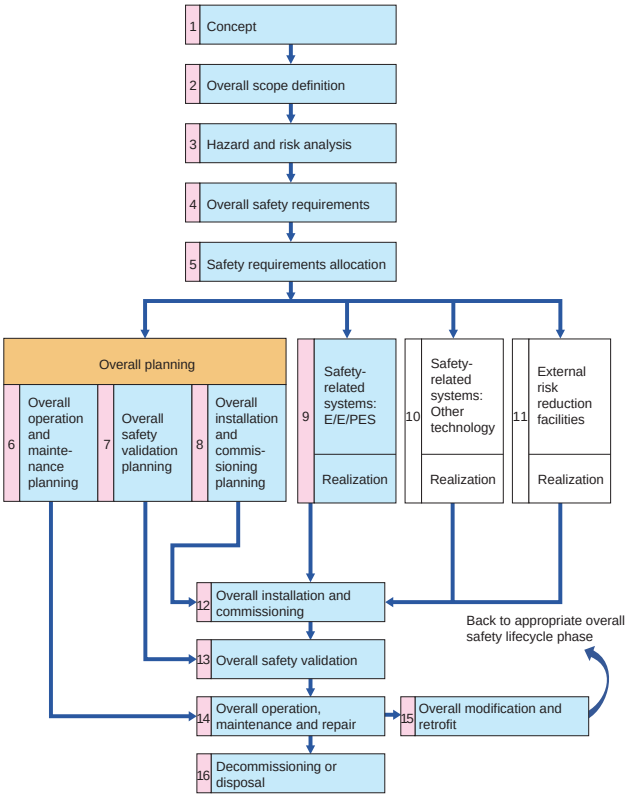

Figure 2 Safety Lifecycle

A safety instrumented system is composed of sensors to detect process abnormalities; logic solvers to conduct preset algorithms using information from sensors to start up actuators such as cut-off valves; and actuators. The safety systems described in this article are those that are positioned to this logic solver. Figure 1 shows the concept of hierarchical protection for achieving the "plant safety" and the positioning of safety instrumented systems. These contents are specified in IEC61511.

As described at the beginning of this paper, IEC61508 defines a quantitative index for risk reduction and specifies the management of safety related systems by lifecycles. In the following explanation of IEC61508, a description will be made by taking an example of applying the standard to process industries, that is, in the case of a safety instrumented system. Figure 2 shows the safety lifecycle in IEC61508. The very important positioning in IEC61508 is "Hazard and risk analysis," shown in the third box in this figure. This stage specifies the clarification of hazards and hazardous events generated in a plant and its control devices (DCS or the like). The specification requires carrying out risk assessment in the plant by taking into consideration methods for eliminating hazards, by assessing the ease with which hazardous events occur, and by clarifying possible damage caused by hazardous events. Means for risk analysis are not limited, and so several techniques are introduced in the standard such as a Hazard and Operability study (HAZOP study).

Next, risk reduction measures necessary for the hazardous events grasped in the above assessment are determined in the "overall safety requirements." As means for reducing risks, there are other safety-related systems (e.g. relief valves) and external risk reduction facilities in addition to the safety instrumented system, and safety functions requirements are specified for each of them. In the case of the safety instrumented system, for example, the specification includes closing a cut-off valve when any abnormality in the temperature, pressure or level of a certain position is detected. In addition, determining the safety integrity requirements is specified together with this safety functions requirements. The safety integrity requirement is a requested specification in which the extent of reducing risks in a plant is quantized. "Functional safety" which appears in the title of IEC61508 means the safety realized by the risk reduction means shown above.

While risk is represented by multiplying the size of the harm by the frequency of the occurrence of the harm, and the safety instrumented system serves to reduce the frequency of the occurrence of the harm. In this standard, the Safety Integrity Level (SIL) is introduced as a method for expressing the safety integrity requirement. The safety integrity level is classified into four levels (SIL1 to SIL4) as shown in Table 1. In IEC61508, the safety integrity level is handled by dividing it into a low demand mode (in short, the actuation demand occurs once a year or less) and a high demand/continuous mode, considering the frequency of actuation demand for safety-related systems. The safety instrumented system installed in plants is classified into the low demand mode. A measure for the safety integrity level in the low demand mode is Probability of Failure on Demand (PFD). PFD is the probability with which the safety instrumented system does not operate due to a failure when actuation of the system is requested. Thus, the smaller the probability, the higher the safety integrity level becomes.

If we look at the safety integrity level from the viewpoint of the safety integrity requirement: for example, specifying SIL3 as the safety integrity requirement for a safety instrumented system

Table 1 Safety Integrity Level (SIL)

Safety integrity level (SIL)	Low demand mode (PFD)
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 $< 10^{-1}$

to be introduced, means that the safety instrumented system is asked to reduce the frequency with which the original hazardous situation occurs, to 1/1000 or less, because PFD of SIL3 is 10^{-4} or above, and less than 10^{-3}. In other words, for example, by installing a safety instrumented system in a plant where no countermeasures are in place and a hazardous event may occur once every 10 years, it becomes possible to achieve an improvement to a reduction in this frequency to once or less in every 10,000 years.

With respect to determining the safety integrity level (SIL), the social "safety" index should be referred to. This is a subject outside the scope of the IEC standard. As described at the beginning of this paper, it is understood that the idea that safety is "a state in which risks are sufficiently small and well within the tolerable limit," greatly affects this determination. If we examine examples in European coutries, the annual mortality rate for a person due to accident is frequently targeted at 10^{-5} to 10^{-6}. Although the annual mortality rate due to traffic accidents in Japan is about 10^{-4}, the author himself aims for an even lower figure than this average value, and we should seek a rate lower than 10^{-4}, even for disasters due to other causes and regardless of business operation and residential environment. Considering these facts, this index in European countries makes sense.

This "overall safety requirements" also shows the relation to the control systems. Figure 1 indicates the positioning of the safety instrumented system in plant safety management. When a process which is the control object and a control system to control that process lead to any abnormality, the safety instrumented system serves to prevent the occurrence of a hazardous event. The safety instrumented system is also applied to Fire and Gas Protection Systems (F & G) to mitigate the effects of outbreaks of fire or the discharge of toxic gases. As described here, this is a concept whereby the safety of overall systems can be achieved only when the safety functions in each hierarchical layer fulfill their respective abilities.

Based on this concept, this standard is stating that the safety instrumented system must be separated from the control system. For example, this means that shared or common sensors must not be used for these two systems just because the same process variables are being observed. This is because if one sensor fails, then it is possible that both the control functions and the safety functions will be lost at the same time. In addition, it also states that requirements for actuation of the safety instrumented system must be estimated by deeming the safety integrity level of the control system to be less than SIL1. This means that, even if a more highly reliable control system is used, the requested safety integrity level for a safety instrumented system must not be lowered simply based on assumptions about the reliability of that system.

ACHIEVING A SAFETY INSTRUMENTED SYSTEM COMPLYING WITH STANDARD IEC61508

Concrete construction of the safety instrumented system is described in the box "Safety-related system: E/E/PES" in the lifecycle of IEC61508 (Figure 2). With respect to the design of the safety instrumented system meeting the safety integrity level, the standard requires a response to "random hardware failures" of the components used in equipment and preparation of preventive measures for "systematic failures" named in the standard, such as improper specification, design, and operation of equipment.

(1) Response to random hardware failures

Since Probability of Failure on Demand (PFD), which is the index of the safety integrity level (SIL), is the probability of equipment losing its ability to function due to a failure when its actuation request is generated, it can be understood to be the ratio of non-operation of the equipment. In the case of control systems, hardware failures are treated by classifying them into the part where failures can be detected through self-diagnosis and the part where failures cannot be detected through self-diagnosis. However, in safety instrumented systems, failures in each part are further classified whether each of them is a 'safe failure' (the output is conducted in the direction in which the plant is shut down or there is no impact) or a 'dangerous failure' (the output function to shut down the plant is lost). That is, failures are classified into detected safe failures, undetected safe failures, detected dangerous failures and undetected dangerous failures. Since the detected dangerous failures can be detected through self-diagnosis, the outputs can be lead to the safe area using another means. The problem is the treatment of undetected dangerous failures. Since this type of failure cannot be detected by self-diagnosis, it can be detected only by the operation test (proof test) carried out during regular inspections. For non-redundant equipment, PFD is expressed by the equation below when representing this proof test interval with T.

$$PFD = \lambda_{DU} T/2 \quad \cdots\cdots (1)$$

Recently available equipment is a microprocessor-applied product using digital integrated circuits, and the equipment realizes the required PFD by means of thorough high-level self-diagnosis. Something to be noted in particular, is the fact that there is no change in the input and output signals of safety instrumented systems in most cases in their operating environments. Accordingly, self-diagnosis circuits must be realized on the assumption that no change occurs in all signals normally.

Then, to what extent, is self-diagnosis required to be actually realized? Let's take a safety system complying with SIL3 as an example. The safety instrumented system is composed of sensors, a safety system (logic solver) and actuators as described earlier, and the overall system PFD (sys) is

expressed by equation (2) below.

PFD (sys) = PFD (sensor) + PFD (safety system) + PFD (actuator) ····· (2)

For the safety controller, PFD (safety system) is expected to be less than 15% of overall PFD in actual engineering. The remainder of PFD is allocated to those of sensor and actuator. That is, since PFD (sys) is less than 10^{-3} and more than or equal to 10^{-4} for SIL3, it becomes necessary that PFD (safety system) should be 1.5×10^{-4} or less. While for the proof test interval, there is a domestic Japanese plant which has been in continuous operation for four years, and there is an overseas example of operation without shutdown for further long periods. Therefore, a proof test for a short interval cannot be accepted. Consideration of a proof test interval of 10 years (assumed to be 100,000 hours for simplification) results in the conclusion that the undetected dangerous failure value is 3×10^{-9}/h (3 fit) or less using equation (1). Since 3 fit is a small value which is far below the failure rate of one component, it is known that the level cannot be achieved as long as the diagnosis coverage of approximately 100% is realized. This situation is clearly different from that of general highly reliable equipment in which safety is considered from a balance with economy.

(2) Response to systematic failures

Among responses to systematic failures, measures for software design are important. As for the software design, Part 3 of IEC61508 specifies that a description of specifications be given so that misunderstandings cannot occur, to carry out design corresponding to such a description as above using sufficiently managed design tools, to verify competent module levels and system levels planned in the pre-design stage, and to implement strict management including impact analysis in changing design, and shows a structure which can prevent systematic failures. This part of IEC61508 also specifies that the actual development and design processes are executed as specified and that these are to be verified by a third party.

The safety system “ProSafe-RS” recently developed by Yokogawa Electric Corporation is certified by the third party body TÜV that its responses to both random hardware failures and systematic failures described above comply with the standard IEC61508.

CONCLUSION

Safety is the top priority in all industries. Contrary to the conventional concept pointing to zero danger, that is, absolute safety, the safety management based on risks introduced here may be understood as bringing some compromise due to the words “tolerable risk.” However, it should be understood that grasping the hazards in a plant by implementing strict risk analysis requires concrete risk reduction means and this is a severer requirement. The concept of hierarchical protection does not tolerate any little mitigation for protection inside the absolute stronghold against hazards, even if there were to be such a stronghold. The concept also does not provide a basis for lowering the safety integrity level of a safety instrumented system simply because of high reliability in control devices. A safety instrumented system complying with the standard is certified by being provided with an eminent self-diagnosis function different from general equipment. It is predicted that safety instrumented systems which can contribute to the improvement of safety even more, as compared with the realization of conventional safety functions using relays, will come into even more widespread use in the future. ◆

REFERENCES

(1) IEC61508 First edition: Functional safety of electrical/electronic/programmable electronic safety-related systems

(2) Shimizu Kyuuji, Fukuda Takafumi, Mechanical safety engineering, Yokendo, 2000, 188p. in Japanese

(3) Sekiguchi Takashi, Satoh Yoshinobu, Machine safety, Functional safety practice manual, Nikkan Kogyo Shimbun, 2001, pp. 220-243 in Japanese

◆◆◆