Soft Computing Method for Determining the Safety of Technological System by IEC 61508

Ormos[*], L., Ajtonyi[**], I.

[*]College of Nyíregyháza, Technical and Agricultural Faculty,
Department 'Electrotechnics and Automation', Nyíregyháta, POB.166,
4401-Hungary

[**]University of Miskolc, Institute of Electrical Engineering,
Department of Automation, Miskolc-Egyetemváros, 3515-Hungary

Abstract: safety functions were originally performed in different hardware from the process control functions. This was a natural feature because all control systems were discrete single function devices. It was not really inconvenient for instrument designs to achieve the separation and extra features needed for the safety shutdown devices. There is a temptation nowadays to combine safety and control in the same equipment. The question is how to determine the safety measure of a technological system? The two basic methods are the quantitative method and the qualitative method where the quantitative method is based on numeric historical data, and the qualitative one uses linguistical historical data. This paper makes a comparision of these methods and introduces a solution of qualitative method based on soft computing method.

Keywords: safety measure, safety instrumentation, safety integrity level, catastrophe theory

1 Safety and shutdown systems

There have been some steadily developing trends in the last ten years which have moved the subject of so-called *functional safety* from a specialized domain of a few engineers into the broader engineering and manufacturing fields (Macdonalds,2004).

The term *functional safety* is a concept directed at the functioning of the safety device or safety system itself. It describes the aspect of safety that is associated with the functioning of any device or system that is intended to provide safety. A short description of functional safety is the following: "*Functional safety is that part of the overall safety of a plant that depends on the correct functioning of its safety related systems."*(from IEC 61508 part 4.).

1.1 Hazard and risk analysis

It seems, specification errors contribute a large proportion of safety system failures. Recognizing and understanding the safety problem to be solved is the first essential step in avoiding this problem. The foundation for any system application is a thorough understanding of the problem to be solved. The process industry seems to have reached consensus on the use of a top down methodology and is generally known as the hazard study method (Jamshidi,1996).

Safety functions were originally performed in different hardware from the process control functions. This was a natural feature because all control systems were discrete single function devices. It was not really inconvenient for instrument design to achieve the separation and extra features needed for the safety shutdown devices. Only with the advent of DCS and PLC controllers did engineers have to pay attention to the question of combining safety and control in the same systems. All standards and guidelines clearly recommend the separation of the control and safety functions. The diagram in Figure 1.1 (Macdonald, 2004, p. 41) shows the separation of safety control from process control.

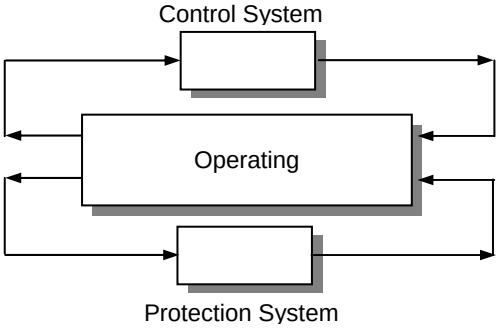

Figure 1. Separation of safety controls from process controls

1.2 Risk reduction and classification

The problem of risk classification is that risk does not come in convenient units like volts or kilograms. There is no universal scale of risk. The method of calculation is generally consisted and it is possible to arrive at a reasonable scale of values for a given industry. As a result IEC have suggested using a system of risk classification that is adaptable for most safety situations.

The risk reduction factor *RRF* can be computed by the expression (1):

$$RRF = \frac{Fnp}{Ft},$$

where *Fnp* is given by demands/year.

The safety availability *SA* is

$$SA = \frac{(RRF - 1)}{RRF} \quad 100[\%].$$

The probability of failure on demand PFD_{avg} is computed by equation (4.92):

$$PFD_{avg} = \frac{1}{RRF} = \frac{Ft}{Fnp} = \Delta R \ ,$$

and the protected risk frequency *Fp* is

$$\boldsymbol{Fp = Fnp\ PFD_{avg}} \ ,$$

where the target value of *Fp* is the tolerable risk frequency *Ft*. The alternative name of *PFD* is fractional dead-time. Its meaning is the fraction of time that safety system is dead.

1.3 Safety integrity level (SIL)

The question is, how to decide when to use a safety instrumented system *SIS*, and how good must it be. It depends on the amount of risk reduction required after the other devices have been taken into account. The measure of the amount of risk reduction provided by a safety system is the *safety integrity*.

In order to get a scale of performance safety practitioners have adopt the concept of safety integrity levels *SIL*s. The SILs are derived from earlier concepts of grading or classification of safety systems. The SIL table provides a class of safety integrity to meet a range of PFD_{avg} values. Hence the performance level of safety instrumentation needed to meet the SIL is divided into categories shown in Table 1 (Macdonald, 2004). There are some choices about how to the SIL is

Safety integrity level	Low demand mode of operation (average probability of failure to perform its design function on demand)
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. Safety integrity level by IEC61508

determined. Basically there is a choice between using real numbers (quantitative method) and some variations on fuzzy logic (qualitative methods).

1.4 Determining the safety integrity

The most important tasks in the SRS development is to specify the safety integrity of each SIS functions. This needs to be done fairly early in the development stages to see that the proposed solutions are realistic, achievable and of course affordable. The cost of the SIS will rise steeply with the SIL values even if a logic solver is used that meets SIL 3 the cost of sensors and actuators and engineering work will still be influenced strongly by the SIL rating.

The reason for diversity in methods of determining SILs is probably due to the difficulties of arriving at reliable and credible estimates of risk in the wide variety of situation faced in industries. Whilst a quantitative risk assessment is desirable it may be worthless if the available data on fault rates is minimal or subject to huge tolerances. Qualitative methods allow persons to use an element of judgement and experience in the assessment of risk without having to come up with numeral values that are difficult to justify.

One advantage of the SIL concept is that provides a 10:1 performance band for risk reduction and for SIS in each safety integrity level. Hence the classification of the safety system can be matched to a broad classification of the risk and the whole system is able to accept a reasonable tolerance band for estimates of risks and risk reduction.

1.5 Quantitative method for determining safety integrity level

The quantitative method is used to assist in development of the SRS and the defining of the SIL by historical data. The steps of quantitative method are:

- evaluation of hazard event rate without protection, definition of target risk frequency, and record of all details under phase 4 of the SLC;
- addition of external and non-SIS protection and evaluation of effect on risk frequency;
- proposition of an SIS risk reduction measure which reduces the hazard event rate and hence the risk frequency;
- conclusion of a practical risk reduction factor for the SIS consistent with being below the target risk frequency;
- conversion of the risk reduction factor to an SIL value for the SIS;
- draft the SRS with a reference to the calculation sheet and risk reduction model;
- finalization SIS detail SRS.

2 Qualitative methods for determining safety integrity level

The qualitative method is a very attractive alternative for arriving at SILs because it avoids the need to place actual quantitative figures on the hazard demand rates, risk frequency and the consequences.

2.1 Qualitative method by IEC 61508

Since in many cases the used figures are very approximate it is perhaps more realistic to use an approximate description. The following diagram in Figure 2 will show the risk parameter chart (Macdonald,2004).

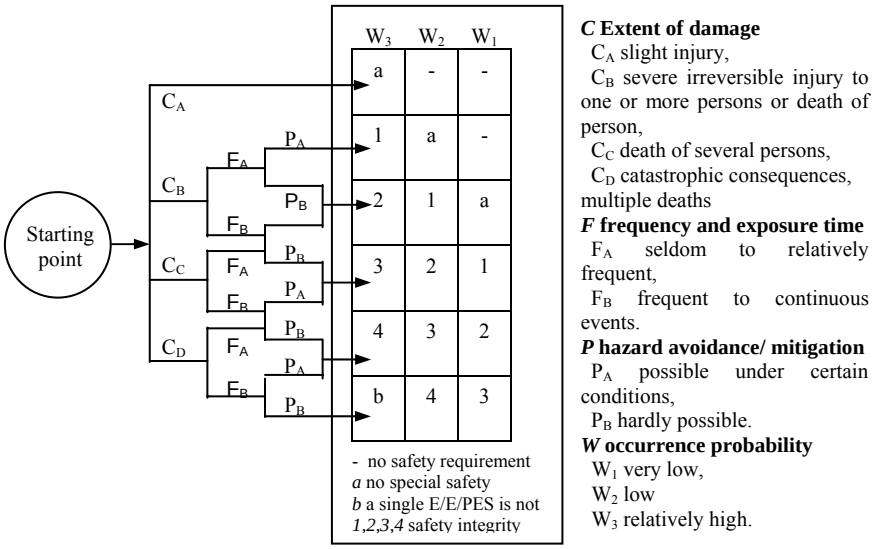

Figure 2. Risk parameters charts based on IEC 61508

In practice the process industries there are separate versions for three categories of hazard:

- harm to persons,
- harm to environment,
- loss of assets (production and equipment losses/repair costs).

All three versions of the risk graph can have the same basic layout but for environment and asset loss the parameter *F*, for exposure, is considered to be permanent and can be left out of the diagram.

For a full determination of SIL requirements each safety function should be evaluated for the three categories of hazard and the SIL target rating must be set to meet the highest value found from the three categories.

IEC 61511 has generated a very useful version of the factors affecting the parameters *C, F, P* and *W* shown in Table 2. It must be cleared that for each application it is the responsibility of individual companies or safety departments to establish their own agreed parameters for the risk graph they wish to use. In particular it is important to note the interpretation of the term *W* as being based on the assumption that no SIS is present.

***C* Consequence** average number of fatalities likely to result from the hazard. It is determined by calculating the average numbers in the exposed area when the area is occupied taking into account the vulnerability to the hazardous event.
***F* Occupancy** probability that the exposed area is occupied. It is determined by calculating the fraction of time the area is occupied.
***P* Probability of avoiding the hazard** the probability that exposed persons are able to avoid the hazard if the protection system fails on demand. This depends on there being independent methods of alerting the exposed persons to the hazard and manual methods of preventing the hazard or methods of escape.
***W* Demand rate** the number of times per year that the hazardous event would occur if no SIS was fitted. This can be determined by considering all failures which can lead to one hazard and estimating the overall rate of occurrence.

Table 2. Parameter description table from IEC 61511

2.2 The safety layer matrix method for SIL determination

Another qualitative method described by IEC standards is called safety layer matrix method which is described in Annex E of IEC 61508. The same principles have been included in the ISA standard S84.01 Annex A.3.1, and in the recently issued IEC 61511-3 in annex along with the risk graph. IEC states some basic requirements for safety layers before the logic of the matrix diagram can be used:

- independent SIS and non-SIS risk reduction facilities,
- each risk reduction facility is to be an independent protection layer,
- each protection layer reduces the SIL by 1,
- only one SIS is used.

The method then determines the SIL for the SIS by applying the situation to a severity matrix chart such as the one shown in Figure 3. It seems even easier than the risk matrix but it depends on a calibrated scale of severity and the correct identification of valid protection layer. Obviously it must be sure that each safety layer has a suitable integrity to qualify as a protection layer.

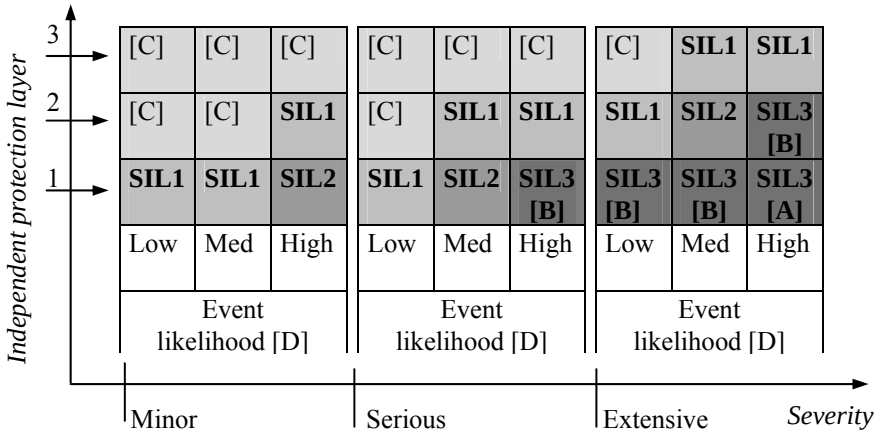

Figure 3. Hazardous event severity matrix (after Macdonald,2004 p.133)

2.3 Thom's catastrophe theory as tool for qualitative method

The events affected on SIL value form a set of conditions and occur moving to other catastrophe layer described by functions (Poston and Stewart, 1985) (Madarasz,2004). Typical feature of switch catastrophes is the separation which means the continuous changing will be modified to sudden changing when any environmental condition has changed. Special form of switch catastrophe is the *conditional catastrophe* when functions are directed or switched to different catastrophe surfaces by *control variables*, i.e. the conditional variables.

The catastrophe surface is a peak catastrophe shown in Figure 4. As it seems control variables affect on the functions of processes, and the direction of changing is influenced by the control variable. The SIL determination is based on the rules of conditional catastrophes.

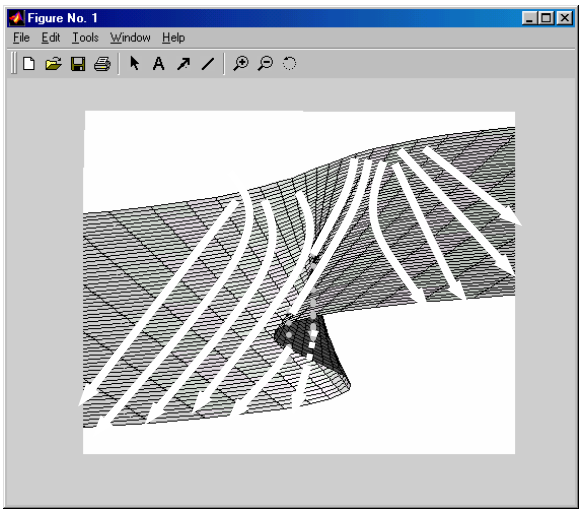

Figure 4. The conditional catastrophe

2.4 The determination of safety integrity by qualitative method

In this work a qualitative method has carried out for single channel safety control. The goal of this method is to determine the value of *safety integrity level* in accordance with the number of applied *independent protection layers* in SIS by a knowledge base without the application of any historical data base. Soft computing applied for SIS is based on the hazardous event severity matrix in Figure 3 proposed by standard IEC 61508 part 5 and standard IEC 61511-3.

The principal method to determine the number of IPLs is a special event of Thom's catastrophe theory, the conditional catastrophe described in Chapter 4. In this case, the number of needed independent protection layers depend on the severity of hazardous events and the number of independent protection layers. The environmental condition is the event likelihood, and the output is the SIL value.

2.5 Fuzzy system to determine the value of SIL

The determination of SIL by soft computing method is based on the application of fuzzy logic together Thom's conditional catastrophe theory. Functions having continuity are operated by variables featured the SIL of specified processes. When any conditions change then safety features will change, and the SIL will have got new value.

The fuzzy system for risk graph method has four inputs described in Table 2 and the output is the value of SIL. Three inputs *C*, *F*, and *P* are variables and *W* is the condition. The function for SIL is shown in Figure 5.

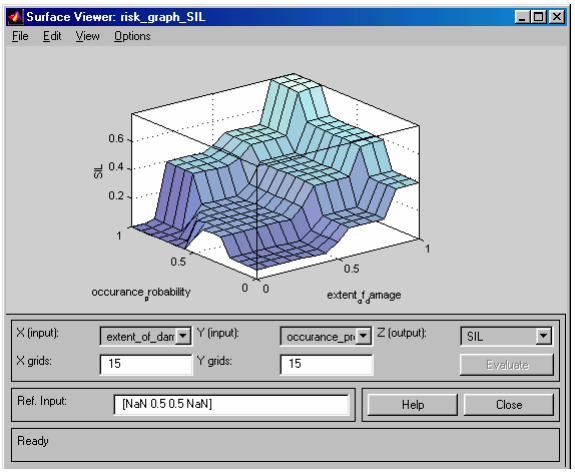

Figure 5. Function for determining the SIL by the risk graph method

The fuzzy system for the severity matrix method has two linguistic input variables the severity and the event likelihood, and one numeric variable the number of independent protection layers which is not determined by analytical function but consists of discrete values. The original output is the value of SIL. The relationship between the *Severity* and the *IPL*, and the *SIL* influenced by the condition *Event-likelihood* is shown in Figure 3. Determination of SIL value by fuzzy logic system based on the severity matrix can be seen in Figure 6.

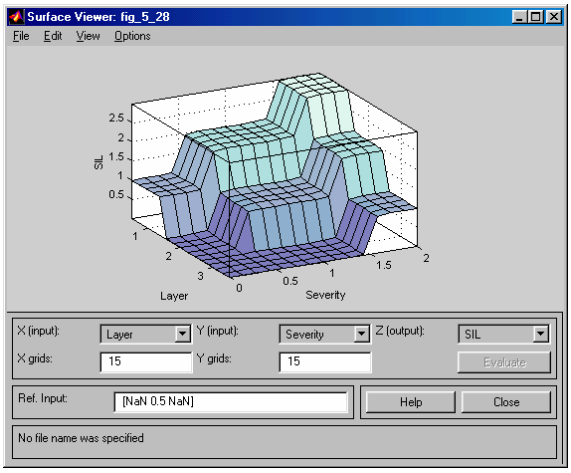

Figure 6. Function for determining the SIL by the severity matrix

Conclusions

The quantitative method requires a lot of historical data about the system operation and its safety features. All the historical data have to be quantitative ones for the computation described in Session 1.2 where the SIL is determined by the value of average probability of failure on demand PFD_{avg} from Table 1.

The qualitative method for determining the SIL has the following features

1. The qualitative method requires professional experience.
2. The qualitative method does not require the collection of historical data.
3. The qualitative method can take into consideration information which might not be quantified.
4. The qualitative method carries out information from information.

References

[1] Macdonald, D.: Practical Industrial Safety, Risk Assesment and Shutdown Systems, An imprint of Elsevier, Linacre House, Jordan Hill, Oxford OX2 8DP, 200 Wheeler Road, Burlington, MA 01803, 2004.

[2] Madarász, L.: Informačné technológie a ich aplikácie v zložitých systémoch (Information technologies and their application for large-scale systems.) University Press, elfa, TU Košice, 2004.

[3] Jamshidi, M.: Large-Scale systems: Modeling, Control, and Fuzzy Logic, Prentice Hall PTR, Upper Saddl River, New Jersey 07458, 1996.

[3] Poston, T.-J. Stewart: Katasztrófaelmélet és alkalmazásai, Műszaki Könyvkiadó, Budapest, 1985.