Journal of KONBiN 1 (13) 2010
ISSN 1895-8281

DOI 10.2478/v10040-008-0155-y

THE OPERATION MODES OF E/E/PE SYSTEM AND THEIR INFLUENCE ON DETERMINING AND VERIFYING THE SAFETY INTEGRITY LEVEL

RODZAJE PRACY SYSTEMU E/E/PE I ICH WPŁYW NA OKREŚLANIE I WERYFIKACJĘ POZIOMU NIENARUSZALNOŚCI BEZPIECZEŃSTWA

Tomasz Barnert[1], Kazimierz T. Kosmowski[2], Marcin Śliwiński[3]

Gdansk University of Technology, G. Narutowicza 11/12, 80-952 Gdańsk
e-mails: (1) t.barnert@ely.pg.gda.pl, (2) k.kosmowski@ely.pg.gda.pl, (3) m.sliwinski@ely.pg.gda.pl

Abstract. *The standard PN-EN 61508 introduces some probabilistic criteria for the E/E/PE systems that can operate in different modes of operation, which are related to the safety integrity level (SIL). For the control and protection systems, operating in a low demand mode, the criterion is the average probability of dangerous failure on demand PFD_{avg}. In case of systems working in a continuous mode of operation or high demand, the criterion is probability of dangerous failure per hour PFH. In practice, the E/E/PE systems implement many safety-related functions (SRFs), which have different requirements for high and low demands. Thus, there is the problem with choosing proper probabilistic criterion for determining required SIL for a safety-related function to be implemented by these systems as well as in the process of quantitative verification of SIL for considered architectures.*

Keywords*: functional safety, safety integrity level, safety-related system, modes of operation*

Streszczenie: *Norma PN-EN 61508 wprowadza kryteria probabilistyczne dotyczące wyróżnionych rodzajów pracy systemów E/E/PE, które związane są z poziomami nienaruszalności bezpieczeństwa SIL. Dla systemów sterowania i zabezpieczeń, pracujących w trybie rzadkiego przywołania do działania, kryterium tym jest przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie PFD_{avg}. W przypadku systemów realizujących funkcje bezpieczeństwa w sposób ciągły lub w trybie częstego przywołania do działania, kryterium tym jest prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę PFH. W praktyce spotyka się systemy E/E/PE, w których zaimplementowane są różne funkcje bezpieczeństwa, realizowane w zarówno w trybie częstego przywołania do działania lub ciągły, jak i trybie rzadkiego przywołania do działania. Istnieje więc problem wyboru kryterium probabilistycznego w celu określenia wymaganego poziomu nienaruszalności SIL funkcji związanej z bezpieczeństwem do zrealizowania przez te systemy, jak i w procesie ilościowej probabilistycznej weryfikacji SIL tych systemów o rozważanych strukturach.*

Słowa kluczowe*: bezpieczeństwo funkcjonalne, poziom nienaruszalności bezpieczeństwa, rodzaje pracy systemu*

1. Introduction

The functional safety can be considered as a part of general safety, which depends on a proper response of the control and/or protection systems. The concept of functional safety was formulated in (IEC 61508, 1998; IEC 61511, 2000; IEC 62061, 2004) and is applied to the design and operation of the safety-related electric, electronic and programmable electronic (E/E/PE) systems. These E/E/PE systems perform specified function(s) to ensure that the risk is maintained at acceptable level. Two different requirements should be satisfied to ensure the functional safety:

- the requirements imposed on the performance of safety-related functions,
- the safety integrity requirements (the probability that given safety-related function is performed in satisfactory way within specified time).

The requirements for safety functions are to be determined based on identification and analyses of hazards, while the safety integrity requirements are result of the risk analysis and assessment.

Taking into account a process of the safety integrity level determination, the type of safety-related system and the demand mode of its operation should be considered carefully. The low demand mode is usually found in the process industry systems, but frequent or continuous one appears in machinery or transportation systems. The choice of proper method of determining SIL is associated with demand mode. Considering low demand mode the methodology based on qualitative or semi-qualitative information might be used (e.g. the risk graph method). In case of frequent or continuous mode operation the quantitative method is recommended. An example of such method is the failure mode, effect and criticality analysis (FMECA).

2. The safety integrity level and probabilistic criteria

A main term related to the functional safety concept is the *safety integrity*. It is understood as the probability that given safety-related system will satisfactorily perform required safety related function (SRF) under all stated conditions within a given period of time.

The safety integrity requirements are specified by the *safety integrity level* (SIL), which is a discrete level (1÷4). It is related to given safety function to be allocated using the E/E/PE system. The safety integrity level of 4 (SIL4) is the highest level, and it is difficult and expensive to implement, i.e. it usually requires sophisticated and complex architecture of the E/E/PE safety-related system.

The interval probabilistic criteria for the safety-related functions to be implemented using E/E/PE systems are presented in Table 1.

Table 1. Probabilistic criteria for safety functions to be allocated using E/E/PE systems

SIL	PFD_{avg}	PFH [h^{-1}]
4	[10^{-5}, 10^{-4})	[10^{-9}, 10^{-8})
3	[10^{-4}, 10^{-3})	[10^{-8}, 10^{-7})
2	[10^{-3}, 10^{-2})	[10^{-7}, 10^{-6})
1	[10^{-2}, 10^{-1})	[10^{-6}, 10^{-5})

For consecutive SILs two probabilistic criteria are defined in IEC 61508, namely:

- the average probability of failure to perform the safety-related function on demand (PFD_{avg}) for the system operating in a low demand mode,
- the probability of a dangerous failure per hour PFH (the frequency) for the system operating in a high demand or continuous mode of operation.

3. Modes of operation of the E/E/PE safety-related systems

As it was mentioned the normative document IEC 61508 distinguishes two modes of operation, which can be associated with safety-related function: low demand mode of operation and high demand or continuous mode of operation. There is a significant difference between both of them. The safety-related function which operates in the low demand mode is only performed when it is required. It means that the safety-related system should not have the influence on equipment under control (EUC) until the demand for safety function occurs. In case of continuous mode the safety-related system continuously controls the EUC. In this situation the dangerous failure of safety-related system can lead directly to the hazardous event (IEC Functional.., 2010).

Thus, mentioned above modes of operation are used to describe given safety function to be carried out by the E/E/PE safety-related system. A low demand mode of operation is defined for the situation when the frequency of demands for operation of given safety-related system is no greater than one per year and no greater than twice the proof test frequency. High demand or continuous mode appears when the frequency of demands for operation of a safety-related system is greater than one per year or greater than twice the proof test frequency. It should be mentioned that the new revised version of IEC 61508:2010 gives a new description for continuous mode of operation as a state where the safety function retains the equipment under control in a safe state as part of normal operation.

4. Categorization of E/E/PE safety-related systems

The E/E/PE systems working in low demand mode of operation are mainly used in the process industry, like petrochemical and mining (safety instrumented systems SIS) (CCPS: Guidelines.., 2000). They are related to requirements presented in IEC 61511 standard. The high demand and continuous demand modes of operation systems are usually used in the machinery safety-related electronic control systems

as well as in transportation (e.g. anti-lock braking system ABS, railway protection and communication systems, as described in EN 50129 standard).
Single E/E/PE safety-related system can attend to one or more different safety functions simultaneously. Those safety functions can operate in different modes of operations: low, high or continuous (Fig. 1).

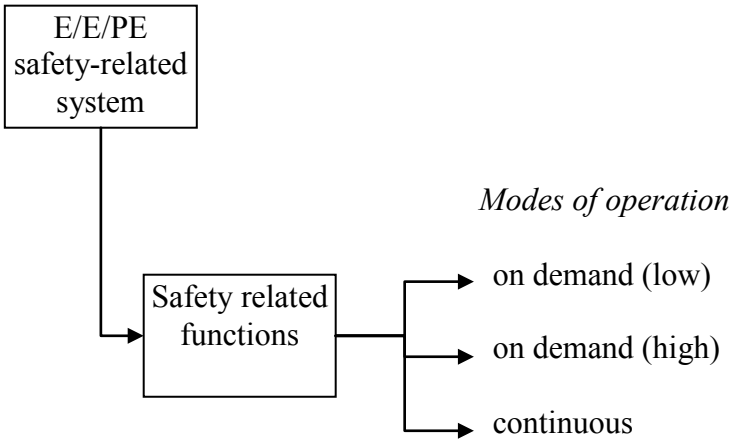

Fig. 1 Modes of operation of the E/E/PE safety-related systems

During the process of determining the safety integrity level, the mode of operation has a significant influence on its results. Having the knowledge about the mode in which the safety function will be operating, the proper method of SIL determination can be chosen.
A coherent method which can be used for both, the low as well high or continuous mode of operation, is quantitative one. This method usually results in proper SIL level, because the risk model is based on construction of a specific model for each hazardous event. This kind of method requires good knowledge, skilled analyst as well as considerable time to carry out. The examples of quantitative methods used in the process of determining required SIL are FMECA (failures, modes and effects criticality analysis) or FTA (fault tree analysis). Special care should be taken with another quantitative method - the LOPA (layers of protection analysis), because is not suitable for functions that operate in continuous mode.
Another method widely used for determining SIL is the risk graph. This method can be qualitative or semi-quantitative. It is easier to perform than quantitative one. The risk parameters descriptions can include some numeric values that are used for calibrating the risk graph. The risk graph method usually results in higher requirements for the safety integrity level (SIL) than SIL derived from the quantitative method. Despite this, this method is extensively used in the process and offshore industry. The risk graph methodology is usually used for the low demand operation mode of safety-related function.

According to IEC 61508 and IEC 61511 the functional safety validation should be performed in terms of requirements for overall safety functions and overall safety integrity requirements. In particular, PFD_{avg} or PFH value has to be verified in the probabilistic modeling process for the architectures considered of given E/E/PE safety-related system taking into account the interval probabilistic criterion for determined previously SIL.
Taking into account a method of minimal cut sets, the probability of failure to perform the design function on demand can be evaluated based on following formula:

$$PFD(t) \approx \sum_{j=1}^{n} Q_j(t) \approx \sum_{j=1}^{n} \prod_{i \in K_j} q_i(t) \tag{1}$$

where: K_j – j-th minimal cut set (MCS), $Q_i(t)$ - probability of j-th minimal cut set; n – the number of MCS, $q_i(t)$ - probability of failure in performing the design function by i-th – subsystem or element.

The average probability of failure to perform the design function on demand for given system is calculated, assuming that all subsystems are tested with the same test interval T_I, as follows

$$PFD_{avg} = \frac{1}{T_I} \int_0^{T_I} PFD(t)dt \tag{2}$$

The probability per hour (the frequency) of a dangerous failure can be evaluated based on formula as below (Barnert & Sliwinski, 2007, Barnert, et al., 2008a, Barnert, et al., 2008b)

$$PFH \approx \frac{\sum_{j=1}^{n}(1-\sum_{\substack{i=1 \\ i\neq j}}^{n} Q_j(t))(\sum_{j \in K_j} \frac{Q_j(t)}{q_i(t)}(1-q_i(t))\lambda_i)}{1-\sum_{j=1}^{n}\prod_{i \in K_j} q_i(t)} \tag{3}$$

where: λ_i is the dangerous failure rate of i-th subsystem.

For different E/E/PE architectures, the PFD_{avg} and PFH can be determined using formulas from normative documents (IEC 61508, IEC 61511 & IEC 62061) or based on the method of minimal cut sets, i.e. formulas (2) and (3). Obtained values of PFD_{avg} and PFH according these formulas for different configurations of subsystems and selecting those (bold type numbers) resulting in SIL3 for the system (SYS) are presented in Table 2.

Table 2. Results of PFD_{avg} and PFH obtained for different configurations (koon) of subsystems

	Sensor	CM communitation module	Safety PLC	Actuator
$PFD_{avg1oo1}$	8.78E-03	1.36E-03	2.39E-03	4.39E-03
PFH_{1oo1}	2.00E-07	3.10E-08	5.46E-08	1.00E-07
$PFD_{avg1oo2}$	2.76E-04	2.96E-05	**5.53E-05**	1.13E-04
PFH_{1oo2}	5.63E-08	4.24E-09	**8.56E-09**	1.96E-08
$PFD_{avg\ 2oo3}$	**4.77E-04**	**3.45E-05**	7.03E-05	**1.63E-04**
PFH_{2oo3}	**5.25E-08**	**5.89E-09**	1.37E-08	**2.67E-08**
SIL_{sub}	3	4	4	3
$PFD_{avg\ SYS}$	**7.30E-04**			
PFH_{SYS}	**9.365E-08**			
SIL_{SYS}	**3**			

In conventional approach the probabilistic model for given complex protection system (E/E/PE) is being developed on the basis of models for subsystems: the sensors (S), communication module (CM) programmable logic controllers (PLC) and actuators (A). The relevant formulas for two cases of probabilistic modeling considered are given below:

For the probability of system failure on demand:

$$PFD_{avgSYS} \cong PFD_{avgS} + PFD_{avgCM} + PFD_{avgPLC} + PFD_{avgA} \tag{4}$$

where: PFD_{avgSYS} – average probability of failure on demand of the E/E/PE safety-related system; PFD_{avgS} – average probability of failure on demand for the sensor subsystem; PFD_{avgPLC} – average probability of failure on demand for the programmable logic controller; PFD_{avgA} – average probability of failure on demand for the actuator subsystem.

For dangerous failure of the system in high or continuous mode of operation the formula is as follows:

$$PFH_{SYS} \cong PFH_{S} + PFH_{CM} + PFH_{PLC} + PFH_{A} \tag{5}$$

where: PFH_{SYS} – the probability of dangerous failure per hour of the E/E/PE safety-related system; PFH_{S} – the probability of dangerous failure per hour for the sensor subsystem; PFH_{PLC} – the probability of dangerous failure per hour for the

programmable logic controller; PFH_A – the probability of dangerous failure per hour for the actuator subsystem.

The E/E/PE safety-related system can implement many different safety functions, which operate in different modes of operations. An example of E/E/PE safety-related system with the low demand mode of operation safety function is presented in Figure 2.

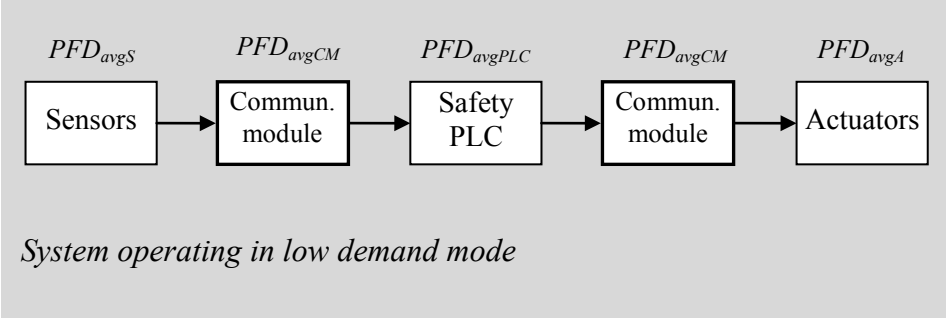

Fig. 2 Safety-related system with subsystems operating in low demand mode

In this case, the verification process of SIL uses the average probability of failure on demand of the E/E/PE safety-related system, calculated from formula (4).
Another example of E/E/PE safety-related system, which implements the high demand or continuous mode of operation safety function, is presented on Figure 3.

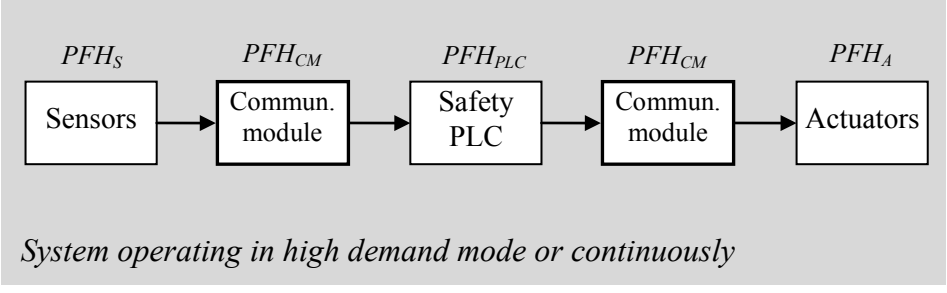

Fig. 3 Safety-related system with components operating in high demand mode or continuously

In the verification process of SIL, the probability of dangerous failure per hour *PFH* is calculated according to formula (5).

The last example shows that there are situations when the components of E/E/PE safety-related system, which implements the low demand mode of operation safety

function, can work also in continuous mode. In this case, the communication module subsystem is working in continuous mode of operation (Fig. 4).

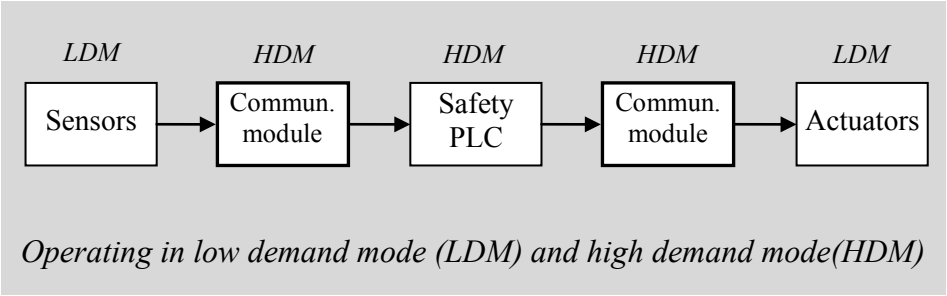

Fig. 4 Safety-related system with components working in continuous mode of operation

In presented situation, during the verification process of SIL the formulas (4) and (5) can not be obviously used, because of different meaning of PFD_{avg} and PFH. The solution would be the determination of the PFD_{avg} and PFH values for the subsystems. Then, the appropriate SIL might be determined for consecutive subsystems. The final step could be to apply a qualitative method for reducing the block diagram to obtain the safety integrity level SIL for the entire system.

5. Conclusion

The IEC 61508 distinguishes two operation modes of the E/E/PE systems implementing the safety-related functions, i.e. the low demand mode (LDM) of operation and high demand or continuous mode of operation (HDM). The E/E/PE safety-related system can implement several different safety functions, which can operate in different modes of operations. Assumed operation mode of the safety-related system has influence on the choice of proper method for SIL determination and probabilistic results obtained. In case of frequent or continuous mode of operation (HDM) the quantitative method of probabilistic modeling is suggested, e.g. FMECA or FTA. In case of low demand mode of operation, both the qualitative and semi-quantitative are useful.

During the process of SIL verification of the E/E/PE system with implementing different safety-related functions and modes of operation, the values of PFD_{avg} for low demand mode of operation or PFH for high demand or continuous mode of operation should be respectively determined, as it is suggested in IEC 62508. However, there are situations when E/E/PE safety-related system operates e.g. mainly in low demand mode, but some of its components/subsystems operate in continuous mode. This situation can be met in distributed control and protection systems, e.g. undersea gas pipelines (Kosmowski, et al., 2006). In such cases the SIL can be assigned for consecutive subsystems and resulting SIL determined for

the entire system using the qualitative method. It is simplest approach with some theoretical and practical limitations.

Further research effort is needed to deal systematically with the issues outlined in this article to work out a coherent methodology for applying it without doubts in practice of functional safety analysis and management. The discussions and consultations among the functional safety expert have been already initiated (IEC Functional..., 2010) to explain basic conceptual issues and propose practical solutions, also with regard to a new version of the standard IEC 61508:2010.

Acknowledgement *The authors wish to thank the Ministry for Science and Higher Education in Warsaw for supporting the research and the Central Laboratory for Labour Protection (CIOP-PIB) for co-operation in preparing the research programme concerning the safety management of hazardous systems including functional safety aspects.*

References

1. Barnert T., Sliwinski M.: Methods *for verification safety integrity level in control and protection systems*. Functional Safety Management in Critical Systems, Jurata, Gdansk 2007.
2. Barnert T., Kosmowski K.T., Sliwinski M.: *Security aspects in verification of the safety integrity level of distributed control and protection systems*. Journal of KONBIN, p. 150-176, Air Force Institute of Technology, KONBIN 2008, Wrocław. Warsaw 2008 .
3. Barnert, T., Kosmowski, K.T., Sliwinski, M.: *Determining and verifying the safety integrity level of the control and protection systems under uncertainty*. Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2008, Valencia, London 2008.
4. CCPS: *Guidelines for Chemical Process Quantitative Risk Analysis*. Center for Chemical Process Safety of the American Institute of Chemical Engineers. New York 2000.
5. IEC 61508: *Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety related systems*. Parts 1-7. International Electrotechnical Commission (IEC) 1998.
6. IEC 61511: *Functional safety: Safety instrumented systems for the process industry sector*. Parts 1-3. International Electrotechnical Commission (IEC) 2000.

7. IEC 62061: *Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems*. International Electrotechnical Commission (IEC) 2004.
8. IEC Functional Safety Zone: "Key concepts", http://www.iec.ch/zone/fsafety/concepts.htm. 2010
9. Kosmowski, K.T., Sliwinski, M., Barnert T.: *Functional safety and security assessment of the control and protection systems.* Taylor & Francis Group, European Safety & Reliability Conference, ESREL 2006. Estoril. London 2006.

Tomasz Barnert M.Sc., received MSc. in 2005 from Gdansk University of Technology (GUT). From 2006 researcher and since 2008 assistant at Faculty of Electrical and Control Engineering, GUT. Specialization: information technologies, distributed computer networks, functional safety and security of distributed control and protection systems.

Kazimierz Kosmowski Prof., received PhD. in 1981 and D.Sc. in 2003 from Gdansk University of Technology (GUT). Since 2006 the manager of Division of Control Eng. at Faculty of Electrical and Control Eng. and since 2007 a vice-chairman of Polish Safety and Reliability Association (PSRA). Specialization: reliability and safety of technical systems, human reliability, functional safety of the programmable control and protection systems.

Marcin Śliwiński PhD., received PhD. in 2006 from Gdansk University of Technology (GUT). From 2001 researcher and since 2006 lecturer at Faculty of Electrical and Control Engineering. Specialization: information technologies, distributed computer networks, expert systems, functional safety of the programmable control and protection systems, probabilistic modelling of technical systems.