The Method of Analysis of Safety Systems Dedicated to the Systems in Rail Vehicle

Adrian Gill
Poznan University of Technology, Poland

The detailed algorithm of SSARV(P) – Safety System Analysis of Rail Vehicles is presented in this paper. Particular steps of SSARV(P) take into account the selected rules of LOPA – Layer of Protection Analysis. SSARV(P) is an overall method of SSARV provided for conceptual phase of safety system. The essence of SSARV(P) is to evaluate the proposed safety system based on measures of hazard risk. The measure of hazard risk is determined using known risk models. This paper presents also a description of LOPA and its general algorithms. Basic information about the independent layers of protection are presented as well.
Keywords: safety systems, safety system analysis, Layer of Protection Analysis.

1. INTRODUCTION

The purpose of safety systems is to rationalise risk in the area of its operation in the way that for hazards identified in them, at least acceptable risk level is provided [18]. The number of measures of risk reduction operating in the framework of safety system, the types of such measures and the level of reliability of their operation, among others, decide about efficiency of realization of the purpose defined in such way. Reasonable selection of measures of risk reduction for occurring sources of hazard is an essential task from the perspective of arrangement of safety system. Normally, when the arrangement of safety system was not preceded by an adequate analysis of its operation, safety system contains excessive number of measures of risk reduction, which generates substantial investment costs and cost connected with its operational use.

For the analysis of operation of safety system, layer model of safety system (WMSB) can be applied. Figure 1 presents exemplary graphic interpretation of such a model.

The essence of layer model of safety system (WMSB) is division of safety system components into independent groups called *layers of protection*. Using definition of layer of protection presented by K. T. Kosmowski e.g. in paper [11] this term means applied components of safety systems, which facilitate risk reduction by preventing generation of sources of hazard, localising sources of hazard and reducing results of undesirable events.

Particular importance of layer model of safety system (WMSB) is emphasized by W. Głodek regarding description of protections of industrial (chemical) processes. Suitability of applications is highlighted, among others, by authors of papers [3, 4, 9-12, 14-17].

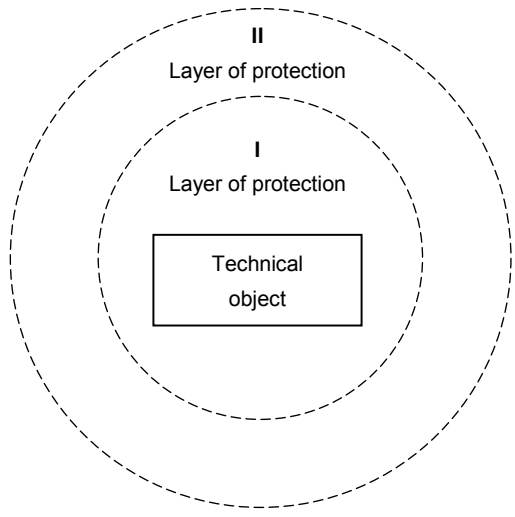

Fig. 1 Exemplary interpretation of layer model of safety system

Systematisation of analysis and substantial facilitation of risk assessment particularly working out scenarios of development of initiating undesirable events, are primary benefits stemming from application of layer model of safety system (WMSB) to analyse operation of safety systems [9].

2. LAYERS OF PROTECTION ANALYSIS – LOPA

2.1. PRELIMINARY REMARKS

LOPA (*Layers of Protection Analysis*) is a method of assessing operation of safety systems. LOPA concept– according to A. Szymanek [15] – is connected with so called defence in depth principle. This principle instructs to generate protection chains created from the following components: physical, technical, procedural, and organisational. Systems designed in such a way significantly improve safety level in areas where they realize their functions. Locating those systems in complex systems: Human – Technique – Environment yields particular advantages. Safety systems of multi-barrier topology have such characteristics that disturbing any barrier is detected on local level of system protection [16]. Thus, defence in depth concept is applied to control risk in industrial systems of process chemistry as well as in management of functional safety of appliances on the basis of rules of IEC61508 standard and sector rules of IEC61511 (for process industry) [16].

The basis of LOPA – with reference to defence in depth principle – is to identify links in the chain of object/system protections, which for the purposes of this procedure and other procedures of safety system analysis – are called IPL – *Independent Protection Layers*. IPL are the results of accepted procedure of safety system modelling particularly grouping measures of risk reduction including specified criteria (criteria applied in identification of IPL and description of exemplary IPL are presented in chapter 3). In other words Independent Protection Layers (IPL) are a certain functional structure, whose components comprise selected (classified in the scope of one layer) measures of hazard risk reduction. Independent Protection Layers (IPL) realize – through classified measures of risk reduction – specified safety functions. As a result, they enable operating sequences of development of undesirable events occurring in the area (object), for which safety system was dedicated.

In many papers about LOPA, it is assumed that the purpose of LOPA is to verify applied IPL to provide acceptable level of hazard risk activating in a form of undesirable events (ZN) in the area of analyses.

LOPA is also called semi-quantitive method of risk analysis (e.g. papers [4, 14]) or simplified method of risk analysis (e.g. papers [3, 12]). This stems from specific LOPA algorithm simplified in relation to known quantitative methods of hazard risk analysis. Authors of the method admit that LOPA is a rather preliminary stage of advanced quantitative risk analysis. It is a procedure usually applied after quality analysis [12].

2.2. DESCRIPTION OF LOPA

In LOPA procedure the analysis of only one pair of components of a specific relation cause–consequence is assumed, which is called event scenario. With reference to basic components taking part in risk management processes (sources of hazard (ŹZ), hazards (Z), undesirable events (ZN)), it is suggested to call the indicated relation: *relation* ZI – ZN (initiating event – undesirable event). Initiating event is a result of presence, state, characteristics of at least one source of hazard (ŹZ) occurring in the area of analysis. However, normally occurrence and certain synergy of several ŹZ are revealed as ZI. Named components of risk management processes (ŹZ, Z, ZN) are in cause and effect relations, called briefly chain *Ź Z– Z – Z N*. Thus, relation components ZI – ZN should be comprehended as links of *Ź Z– Z – Z N* chain. Selection of relation ZI – ZN can be made from relations or sequences of development of events identified in analyses preceding LOPA e.g. safety review or quality methods of risk analysis.

Record of transfer from ZI into ZN is presented in a form of sequences of event. Those sequences are worked out with inductive methods, which are also defined as bottom up method. This stems from the way of analysing possibilities of development of ZI against applied safety functions. Independent Protection Layers (IPL) map action (with success or failure) of safety function on ZI. Safety functions are taken by measures of hazard risk reduction classified into layers of protection. It is assumed that operation of IPL always happens according to two logical statuses: success (yes), failure (no). As a result of development of ZI, ZN

are created which end the sequence of event. In further phases of LOPA, sequence of event is selected which leads to event of the highest level of loss. It is recommended in this paper to call such sequence of event, as it was also called in paper [13] - representative sequence of events (RSZ). Applying principles of Event Tree Analysis (ETA) method is a suitable mode to work out sequence of development of ZI. The extent of influence of IPL on ZN can be defined also by applying ETA.

If risk level connected with certain RSZ is not acceptable, in safety system further measures of risk reduction, which support operation of existing layers or operate as another IPL (and can be analysed as another IPL in safety system model) are introduced in the safety system. Methodology of LOPA does not contain guidelines about selection of IPL which are adequate for identification of hazards. In the description of LOPA presented by the authors of paper [1] certain suggestion can be found about the form of safety system and thereby IPL which can occur in such system. Examples of layer models of safety system worked out on the basis of paper [1] are given by many authors. Figure 2 presents selected example of such model according to the author of paper [11].

Carrying out analysis, after selecting development scenario ZN, it should be defined what measures of risk reduction, which can operate as IPL, should be applied in safety system. Basic information regarding IPL is presented in chapter 3.

2.3. PROCEDURE ALGORITHMS OF LOPA

LOPA can be presented in a few steps. Among LOPA algorithms presented by various authors, e.g. papers [3, 4, 12, 13, 14] , no fundamental differences occur, they usually refer to the number of algorithm steps. Further – for comparison – selected exemplary LOPA algorithms are presented and described. According to e.g. the authors of paper [12] LOPA can be carried out in six steps. Algorithm steps presented below were worked out on the basis of paper [12]:

1. Identification of effects of undesirable events occurring in the area of analysis.
2. Selection of sequence of event leading to an accident.
3. Identification of ZI and defining frequency or probability of this event.
4. Identification of IPL and assessment of probability of failure on demand of each IPL
5. Hazard risk assessment connected with sequence of accidents.
6. Hazard risk estimation connected with sequence of accidents.

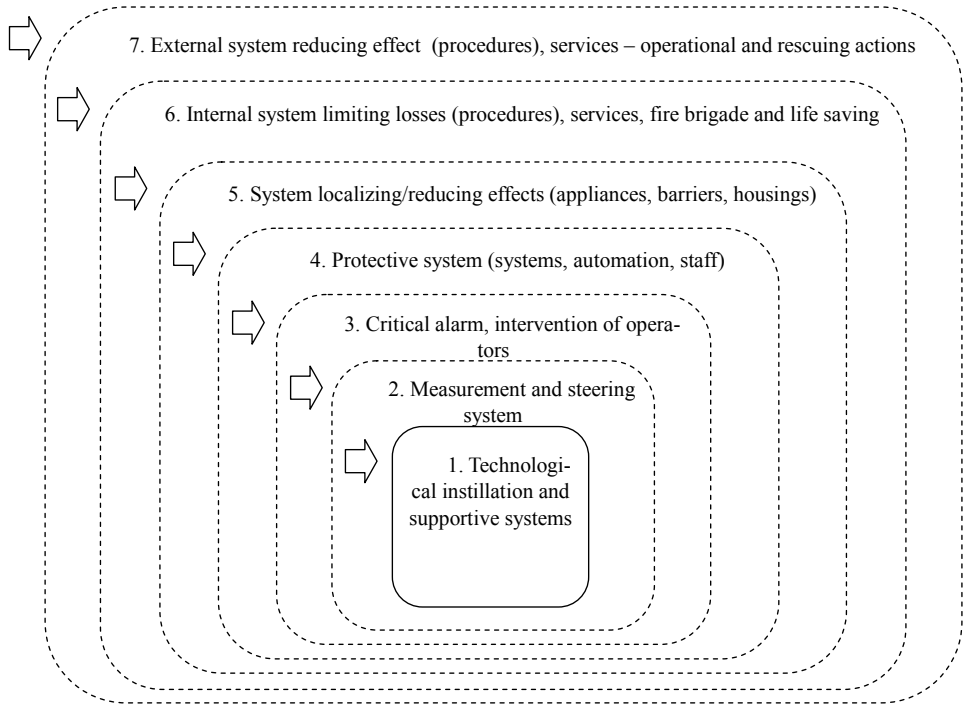

Fig. 2. Layers of protection of exemplary safety system. Study based on [11]

Occasionally – as the author of paper [14] suggests – in the registration phase (collecting) of method algorithm of documentation regarding analysed system is taken into account. This documentation includes documentation of risk identification, technical designs of safety system components, reports of safety inspection, design documentation of layers of protection, etc.

However, the authors of papers [13] recommend short LOPA algorithm consisting of three components:

1. Analysis of occurrence of a sequence of events leading to the most serious consequences or most probable sequence of events (called by the authors of paper [13] representative failure scenario (RZA)) without IPL.
2. Analysis of occurrence of a sequence of events leading to most serious consequences or most probable sequence of events with IPL.
3. Hazard risk estimation.

The authors of paper [17], following the algorithm presented by the authors of LOPA, defined the analysis algorithm below:

1. Selection of event initiating accident scenario (representative event scenario RSZ) and its cause.
2. Assessment of frequency of occurrence of initiating event in representative event scenario.
3. Identification of protection layers (IPL) and assessment of probability of their failure on demand (PFD).
4. Calculation of frequency of effects of initial events.
5. Hazard risk assessment pointed in RSZ as combination of frequency of initial events and measures of their effects.
6. Hazard risk estimation. Return to step 3 of the algorithm if it is necessary to reduce frequency of effects of initial event and reach acceptable risk level.
7. Continuation of analysis for all significant event scenarios.

2.4. THE MAIN ASSUMPTIONS AND METHOD ALGORITHM. ANALYSIS OF SAFETY SYSTEMS OF RAIL VEHICLES.

This paper presents extensive algorithm of SSARV(P) method – analysis of safety systems dedicated to rail vehicles. Individual method components take into account selected principles of already described LOPA method. SSARV(P) method is a version of general SSARV method, planned for conceptual phase of safety system. The essence of SSARV(P) is to estimate designed safety system made on the basis of accepted measure of risk. Measures of risk are defined using known risk models.

It was accepted that SSARV(P) method consists of three phases:

- creating the model of safety system,
- analysing the operation of layers of protection,
- estimating the level of residual risk.

Figure 3 presents diagrammatically the idea of SSARV(P) method and mention its phases. Figure 4 presents general algorithm of SSARV(P) method. The description of consecutive steps is presented below.

The main assumptions of the method:

- the level of risk identified in the area of analyses is not acceptable,
- safety system reacts to and affects sources of hazard in the area of analyses,
- safety system can be presented in a form of layer model,
- layers of protection are the results of accepted procedure of safety system modelling, particularly grouping measures of risk reduction taking into account certain criteria,
- grouping of measures of risk reduction is made according to safety functions realized by measures of hazard risk reduction,
- measure of risk reduction realizes or participates in realization of only one safety function,
- layer of protection realizes only one safety function,
- selection of measures of risk reduction for safety system is made from existing and known measures.

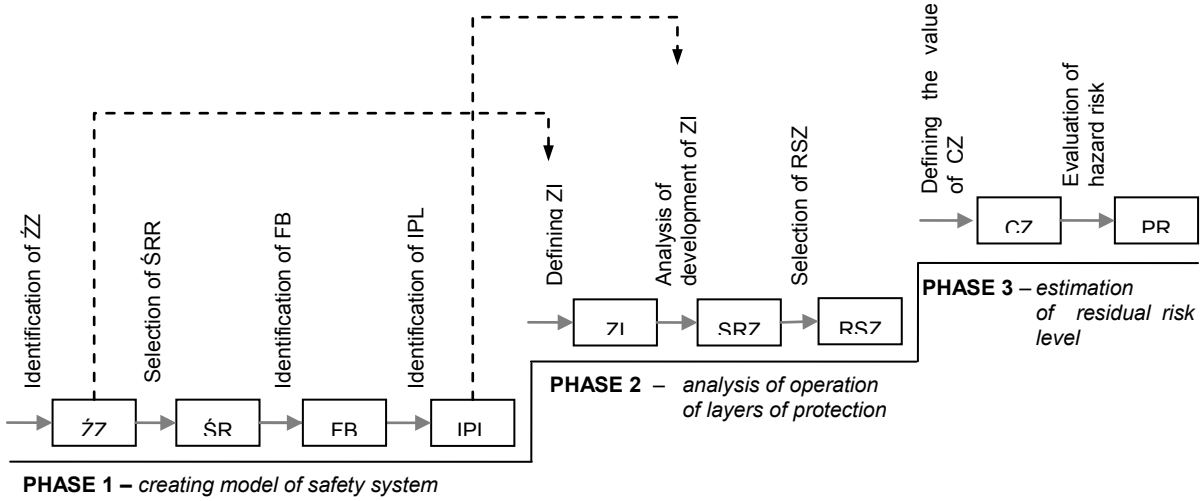

Fig. 3. Schematic diagram of individual phases of analysis method of safety system dedicated to rail vehicles – SSARV(P). Explanation of abbreviations is given in this article.

Step 1. Identification of sources of hazards (ŹZ)

It is suggested to use known methods for identification of sources of hazards e.g. check list method, check lists of sources of hazard in norms and standards referring to machine safety, safety overhaul, records of undesirable events, methods based on brain storming technique. Among others, papers [7, 10] present concept and formal procedures of identification of sources of hazards and identification of hazards using check lists of questions about occurrence of sources of hazards.

Step 2. Selection of measures of risk reduction (ŚRR)

This step consists in selection of measures of risk reduction, which will be applied in the safety system with reference to sources of hazards. Selection of those measures can be made using various modes. It was assumed in SSARV(P) method that selection of measures of risk reduction (ŚRR) is made on the basis of regulations referring to machine safety e.g. norms [2]. In this phase it is worth to mention in what safety function, selected measure of risk reduction can participate.

Step 3. Identification of safety function (FB)

Formalized procedures of identification of safety function on the basis of measures of risk reduction (ŚRR) have not been created. Any available information and characteristics of measures of risk reduction (ŚRR) are used for this purpose, especially, information about the mode of their operation and available technical knowledge referring to design of measures of risk reduction (ŚRR).

Step 4. Identification of independent protection layers (IPL)

Identification of independent protection layers (IPL) consists in defining (naming and marking) layers of the model according to accepted classification and classifying measures of hazard risk reduction used in the safety system for appropriate layers. The modes of realizing identification process of independent protection layers are presented in papers [6, 8]. One mode distinguishes – it is identification of independent protection layers on the basis of: a) existing safety system, b) classification of measures of risk reduction, c) known multi-layer models of safety systems, d) safety functions defined in e.g. study of results of another method of risk analysis, e) on the basis of safety regulations. Attention should be drawn to the fact that independent protection layers meet specified criteria (described in chapter 3). In SSARV(P) method it is suggested to apply the mode consisting in determining safety function (FB) on the basis of safety function (FB) which can realize measures of risk reduction (ŚRR).

Step 5. Defining initiating events (ZI)

Initiating event is a result of presence, state, characteristics of at least one source of hazard (ŹZ) occurring in the area of analysis. However, occurrence and specified synergy of several sources of hazard (ŹZ) can usually be considered

as initiating event (ZI). Defining initiating event consists in pointing and naming (marking) on the basis of source of hazard (ŹZ).

Step 6. Working out sequence of development of initiating events (SRZ)

It is recommended to apply principles of Event Tree Analysis (ETA). A substantial difference in LOPA procedure in comparison to ETA procedure is taking into account during creating sequence of events only material measures of hazard risk reduction e.g. automatically working components and/or systems alarms, physical systems reducing effects of undesirable event and omitting influence of external conditions such as meteorological conditions, wind velocity, atmospheric stability, occurrence of ignition sources, territorial layout of system components. Figure 5 presents exemplary course of sequence of events and schematic diagram of the second phase of SSARV(P) method.

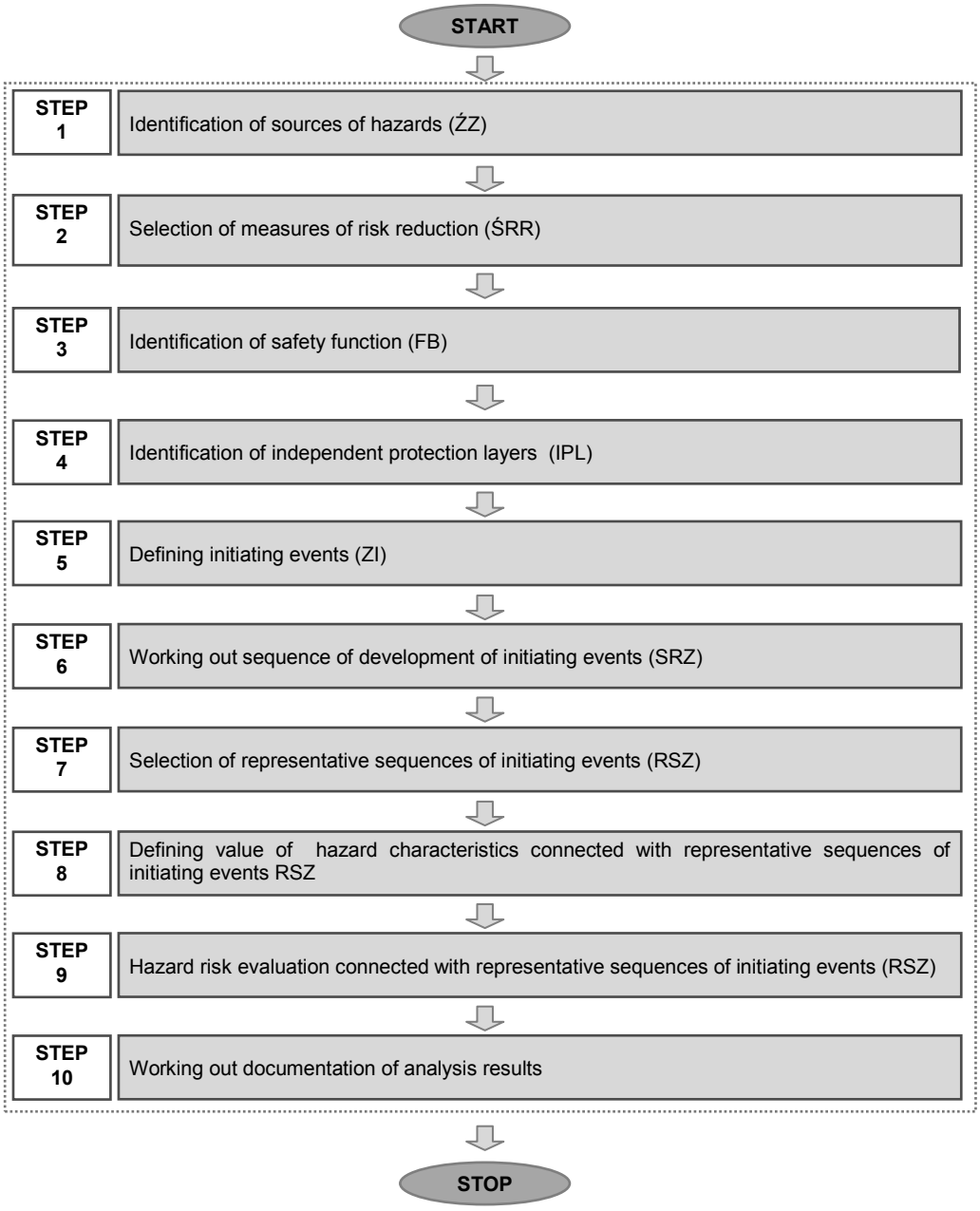

Fig. 4. General method algorithm, Safety System Analysis of Rail Vehicles – SSARV(P)

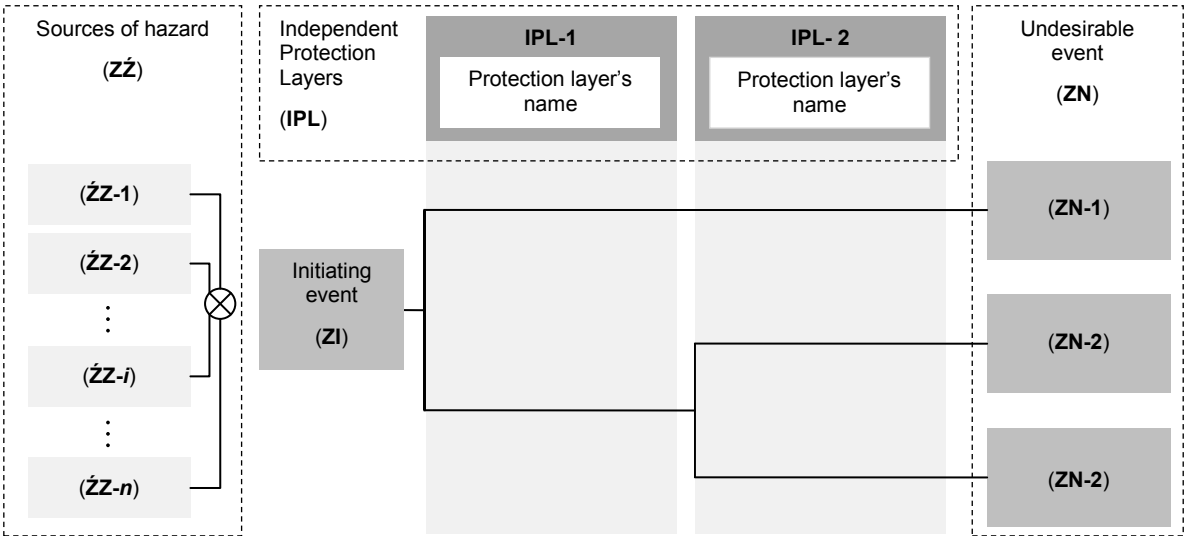

Fig. 5. Schematic diagram of analysis concept of layers of protection with SSARV(P) method – safety system analysis dedicated to rail vehicles

Step 7. Selection of representative sequences of development of initiating events (RSZ)

In the set of initiating events – undesirable events (ZN) ending sequence of development of initiating events (ZI) – there are events, which can be regarded as safety system's success, because after occurrence of initiating event, positive actions of the system started up, which caused that undesirable development of initiating event did not occur. There are also initial events, which should be regarded as safety system's failure, because after occurrence of initiating event, the actions of safety system ended with failure and damage or disaster happened. It is recommended that selection of representative sequences of events should be made on the basis of initiating events, which attest to failure of the operation of safety system.

Step 8. Defining value of hazard characteristics connected with representative sequences of initiating events (RSZ)

Hazard characteristic is a variable, whose values are used to define hazard risk component. Hazard characteristics include, among others: history of hazard activation in the area of analysis, probability of hazard activation, size of damage/loss generated in the area of analyses stemming from hazard activation, value of damage/loss stemming from hazard activation, size of exposures generated by sources of hazard.

Step 8-1. Defining the value of probability of hazard activation

Defining the value of probability of hazard activation is realized with procedure of quantitative analysis of sequence of events. This consists in defining probability of occurrence of undesirable events (ZN) through multiplying consecutive frequencies (or probability) of occurrence of initiating events (ZI) by probability of failure/success of independent protection layer (IPL) connected with specified tree's branch. For a branch referring to success (yes), success probability q_s is assumed and for a branch referring to failure (no) probability $q_n = 1 - q_{s\ is}$ is assumed. The sum of probabilities on each branching should equal 1, and the sum of probabilities of all undesirable events (ZN) (branches) should equal the value of frequency of occurrence of initiating events.

Step 8-2. Defining the measure of extent of losses connected with undesirable events (ZN)

Defining the measure of extent of losses connected with undesirable events (ZN) can be made using various modes. It is recommended to apply models of measures of risk used in known quantitative methods or quality-quantity methods to keep quantitative dimension of SSARV(P).

Step 9. Hazard risk evaluation connected with sequences of initiating events (RSZ)

It is verification (through evaluation, comparison) to which risk category/class (acceptable, tolerable, unacceptable) the risk, evaluated on the basis of selected (known) risk

model taking into account, among others, the value of hazard characteristics defined in step 8, belongs to. If the value belongs to risk class unacceptable, step 10 of the algorithm should be made – steering residual risk.

Step 10. Working out documentation of analysis results

The list of sequences of events leading to undesirable events (ZN) and recommendations about realization of procedures connected with steering residual risk, should be presented in this step. Generally, steering residual risk can be understood as purposeful interaction on analysis area – system, object, process – in the way that for hazards recognized in it, at least tolerable risk level is provided. In case of designing safety system, it is an adequate configuration of this system. It usually consists in implementing additional measures of risk reduction, however, amendment of efficiency of measures of risk reduction (ŚRR) is also a reasonable approach. Efficiency of measures of risk reduction (ŚRR) is expressed through e.g. probability of failure/success on demand.

3. GENERAL DESCRIPTION OF INDEPENDENT PROTECTION LAYERS (IPL)

The scope of independent protection layers (IPL) usually includes several reduction measures of hazard risk. In special case only one measure can create protection layer. It is accepted that each independent protection layer (IPL) can be considered as measure of hazard risk reduction, however, not each measure can be considered as independent protection layer (IPL). Examples of measures of risk reduction (ŚRR) which themselves perform function of independent protection layers (IPL) are presented e.g. in paper [17]. Normally, in the analysis of sequences of events in LOPA only material components of safety systems such as: automatic operation of components an/or systems, alarms, established action procedures, physical systems reducing effects of undesirable event are taken into account. Influence of external conditions such as meteorological conditions, wind velocity, atmospheric stability, occurrence of ignition sources, territorial layout of system components, are omitted. However, it is assumed that protection layers should meet the following criteria (own work on the basis of papers [1, 12]:

- speciality criterion: speciality is understood as orienting independent protection layer (IPL) to reduction of components of hazard risk connected with selected initiating event,
- efficiency criterion: efficiency is understood as ability to counteract hazard activation (when IPL acts according to its purpose) in case residual IPL fail,
- independence criterion: independence is understood as lack of proneness to influence of residual IPL and influence of initiating event,
- verifiability criterion: verifiability is understood as predicted in design proneness to control/estimation of extent of fulfilment of safety function by a layer.

Efficiency of operation of IPL is expressed by PFD (*Probability of Failure on Demand*) index, which is defined as probability that system (IPL) will not realize its function when it is required. In the analyses of operation of safety function, the fact that the area of system operation itself (process, object) is safe itself, is usually taken into account. In such case, for an object in the function of area of analysis, defining PFD should be possible. An object with certain PFD can be treated in further phases of the analysis as independent protection layer (IPL).

4. CONCLUSION

Analysis of operation of safety systems is a tool simplifying realization of risk rationalisation process in the areas where safety systems operate. Significance of this process is especially appreciated in process industry (chemical). With reference to areas of such industry operation, relatively the largest number of design procedures and appropriate application of safety systems can be indicated. This stems mostly from seriousness of identified hazards. Only one comprehensive method – Layer of Protection Analysis (LOPA), received formal conception. Operation of safety systems is usually based on multi-layer concept. This concept, among others, is used in LOPA recommending that analyses of operation of safety systems are carried out using multi-layer models of those systems. The essence of those models is a division of safety system components into independent groups called layers of protection. Acceptance of multi-layer model of measures of

hazard risk reduction systematised creation of such models and simplified risk estimation, especially working out scenarios of development of initiating undesirable events.

Such analyses have not been carried out yet with reference to safety systems dedicated to rail vehicles. This paper presents detailed algorithm of method of safety systems analysis dedicated to rail vehicles – SSARV (*Safety System Analysis of Rail Vehicles*). Individual method components include selected principles of LOPA method. The essence of SSARV is estimation of safety system operation as a whole, carried out on the basis of measures of risk. Measure of riskis defined on the basis of known risk models.

REFERENCES

[1] Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – part 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa. PN-EN 61508-5, 2010.

[2] Bezpieczeństwo maszyn. Ogólne zasady projektowania. Ocena ryzyka i zmniejszanie ryzyka. PN-EN ISO 12100, 2011.

[3] First K., *Scenario identification and evaluation for layers of protection analysis*, Journal of Loss Prevention in the Process Industries 23 (2010), pp. 705÷718. E-version: www.elsevier.com/locate/jlp.

[4] Freeman R., *Using Layer of Protection Analysis to Define Safety Integrity Level Requirements*, Process Safety Progress Vol.26, No.3. e-version: www.interscience.wiley.com.

[5] Gill A., Kadziński A., *System obsługiwania pojazdów szynowych jako element w warstwowym modelu ich systemów bezpieczeństwa*, Pojazdy Szynowe, 2006, no 4, pp. 31÷38.

[6] Gill A., Kadziński A., *Klasyfikacje środków redukcji ryzyka zagrożeń w warstwowych modelach systemów bezpieczeństwa w transporcie*, czasopismo Logistyka, no 4/2010, CD version.

[7] Gill A., Kadziński A., Kalinowski D., *Identyfikacja zagrożeń związanych z użytkowaniem drzwi podczas eksploatacji tramwajów typu 105Na*, Czasopismo AUTOBUSY – Technika, Eksploatacja, Systemy Transportowe, no 12/2011.

[8] Gill A., Kadziński A., *Idea identyfikacji warstw modeli systemów bezpieczeństwa obiektów w transporcie*, czasopismo Logistyka, no 3/2011, CD version.

[9] Głodek W., *Automatyka zabezpieczeniowa w przemyśle procesowym – przegląd unormowań*. Warsztaty SIPI61508, Gdynia, 28÷29 May 2003, e-version: http://www.sipi61508.com/ciks/pl.glodekw.pdf.

[10] Kadziński A., Gill A., Pruciak K., *Rozpoznawanie źródeł zagrożeń jako ważny element metod zarządzania ryzykiem w komunikacji tramwajowej*. Czasopismo Techniczne – Mechanika, Wydawnictwo Politechniki Krakowskiej, Kraków 2011, journal 2-M, pp. 57-66.

[11] Kosmowski K. T., *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*, Monografia, Wydawnictwo Politechniki Gdańskiej, Gdańsk 2003.

[12] Layer of Protection Analysis – Simplified Process Risk Assessment. Center for Chemical Process Safety / American Institute of Chemical Engineers, New York 2001, e-version: http://www.knovel.com/

[13] Markowski A.S., Borysiewicz M., *Zastosowanie analizy warstwy zabezpieczeń do oceny ryzyka dla rurociągów*. Mat. z warsztatów nt. Metody i modele oceny ryzyka związanego z transportowaniem niebezpiecznych substancji rurociągami, Management Of Health And Environmental Hazards (MANHAZ), Instytut Energii Atomowej, Otwock-Swierk, 2003, e-version: http://manhaz.cyf.gov.pl/manhaz

[14] Summers A.E., Introduction to layers of protection analysis, Journal of Hazardous Materials 104, 2003, pp. 163÷168, e-version.

[15] Szymanek A., *Bezpieczeństwo i ryzyko w technice*, Wyd. Politechniki Radomskiej, 2006.

[16] Szymanek A., *Zasada „głębokiej obrony" a zarządzanie bezpieczeństwem transportu*,

[17] Wei C., Rogers W.J., Mannan M.S., *Layer of protection analysis for reactive chemical risk assessment*, Journal of Hazardous Materials 159 (2008) 19÷24. E-version: www.elsevier.com/locate/jhazmat.

[18] *Zintegrowany System Bezpieczeństwem Transportu. Tom* 2. *Uwarunkowania rozwoju integracji systemów bezpieczeństwa transportu.* Redaktor pracy zbiorowej Krystek R., Politechnika Gdańska, Gdańsk 2009, WKŁ, Warszawa, 2009.

Adrian Gill
Poznan University of Technology, Poland
adrian.gill@put.poznan.pl