THE CONCEPT OF IDENTIFICATION OF LAYERS OF SAFETY SYSTEM MODELS THROUGH CLASSIFICATION OF RISK REDUCTION MEASURES

Adrian Gill, Adam Kadziński

Poznan University of Technology
Faculty of Machines and Transport
Piotrowo 3, 60-965 Poznan, Poland
tel.:+48 61 6652017, +48 61 6652267, fax: +48 61 6652204
e-mail: adrian.gill@put.poznan.pl, adam.kadzinski@put.poznan.pl

Abstract

The article is an introduction to the analysis of the functioning of the safety systems with the use of layered models. The idea behind these models is the classification of elements of safety systems into independent groups referred to as the layers of protection. It seems that the functioning of the safety systems is usually based on the concept of multi-layer securities. Modern technological installations of high-risk industrial facilities are fitted with multi layer security systems. The definition of the safety systems and a review of the definitions of hazard risk reduction measures as part of those systems are presented. A layer of the model of a safety system comprises the measure of risk reduction in terms of the stage of classification. It has been assumed that the safety system model will depend on the adopted classification of these measures. The classification of risk reduction measures used in safety systems of technical objects depending on the form of these measures is presented. Assuming that the form of the safety system model depends on the adopted classification of the risk reduction measures we can perform an identification of the layers of this model. The concept of identification of protection layers in multi-layers safety systems based on classifications is developed. The notation used in the classification of types of risk reduction measures is also presented. Schematic of safety system identification of transport systems objects according to the adopted classification of types of risk reduction measures is developed. According to these schematics, we can describe the safety system models of object other than those related to transport. An example of such an adaptation has been developed for a multi-layer safety system model of objects in the processing industry.

Keywords*: risk, risk reduction measures, safety systems, models of safety systems, layers of protection*

1. Introduction

Eliminating sources of risks or limiting of the levels of exposure to these sources is realized through appropriate elements of the safety systems (ESS). These are systems defined by three components [23]: objective of the systems, elements of the system (man, tangible elements, intangible elements) and structure of the system. The elements of the safety systems (ESS) that eliminate the sources of risks or limit the exposure that comes from these sources can be referred to as the *risk reduction measures*. Pursuant to the EEC ruling regarding the adoption of a common method of safety assessment within risk valuation and assessment [16] (the authors construe this process as analysis and valuation of risk) these measures are also considered as *safety measures*. They, according to the said ruling, denote a set of actions reducing the frequency of risk (according to the authors of this paper – possibility of risk activation) or mitigating its consequences, which aims at reaching or maintaining of an admissible (tolerable) level of risk. In machine safety standards [1, 2], the measures of risk reduction are referred to as the measures *of protection*. This is understood as measures taken for the reduction of risk. The measures of risk reduction are also simply referred to as the *securities*. The number of risk reduction measures, their types and level of reliability decide about the efficiency of the risk reduction by the safety system.

For the analysis of the functioning of the safety systems, many authors i.a. [5, 8, 11-14, 21] propose using multi-layer models of these systems. The idea behind these models is the classification of ESS into independent groups referred to as the layers of protection. Drawing on the definition of the layers of protection as given by K.T. Kosmowski [9] we further understand the applied ESS that reduce risk through prevention of risk source formation, localization of the risk sources and reduction of the consequences of unwanted events. The adoption of a layer model of safety systems allows systemization of formation of these models and significantly facilitates risk assessment– particularly making scenarios of the development of the unwanted initiating events. The analysis of functioning of so modelled safety systems is usually carried out through LOPA (*Layer of Protection Analysis*). A more detailed description of LOPA can be found in works [19].

It seems that the functioning of the safety systems is usually based on the concept of multi-layer securities. Modern technological installations of high-risk industrial facilities are fitted with multi layer security systems [9]. This is the case particularly for processing installations (chemical). The examples of solutions are described by i.e. A.S. Markowski in works [12-14]. The elements of a safety system are layers reducing the risks related to the facility.

The safety systems of technological objects can be built according to its layer model. In such a case each of the layers would have its own physical (tangible or intangible) equivalent in the safety system i.e. appropriate element of this system. These elements, similarly to the system layers, should be independent. In practice it is difficult to build such a safety system partly because the layers defined in the model are usually a combination of measures of risk reduction. A unique case of a safety system is the one in the model of which a single layer constituted a single measure of risk reduction.

A layer of the model of a safety system comprises the measure of risk reduction in terms of the stage of classification. It has been assumed that the safety system model will depend on the adopted classification of these measures.

The aim of this paper is to present a concept of identification of model layers of the safety systems with the use of a classification of the risk reduction measures.

2. Classification of risk reduction measures in safety systems in transport

It has been assumed that there are at least two kinds of classification of risk reduction measures. The first type is the classification developed in terms the security functions realized by the risk reduction measures. In the simplest form these classifications are relatively non-complex (2 or 3 stages of classification) as they are formed from a general division of the functions of the safety systems. The authors of [7] give one of such divisions of safety functions. Safety systems are built so that their elements can be divided into 3 groups i.e. elements realizing the tasks in the area of safety: active, passive, post-accident (in the aspect of realization of the given functions, from the safety point of view [7]). An example of the classification of risk reduction measures depending on the safety functions realized by these measures have been shown in Fig. 1.

Another type is the classifications in terms of the form of the risk reduction measures. In the further part of the paper a part of that classification has been presented. The division of classification has been presented into: two three and multi stage ones.

The proposal of one out of the two stage classifications of risk reduction measures results from the definition of the safety systems and a division of the element of this systems. The risk reduction measures– equivalent to the elements of the safety system– can be divided into: tangible and intangible. Tangible risk reduction measures are proposed to be construed as those of technical nature, also known as *technical protection measures* according to PN-EN ISO 12100-1:2005 [1]. The indicated standard defines the technical protection measures (tangible risk

reduction measures) as screens/shields or other protective tools where a shield denotes (according to that standard) a physical barrier designed as a part of the machine, whose function is to protect against injury. An example of tangible risk reduction measures are: alarm systems, shields and screens, security systems etc.

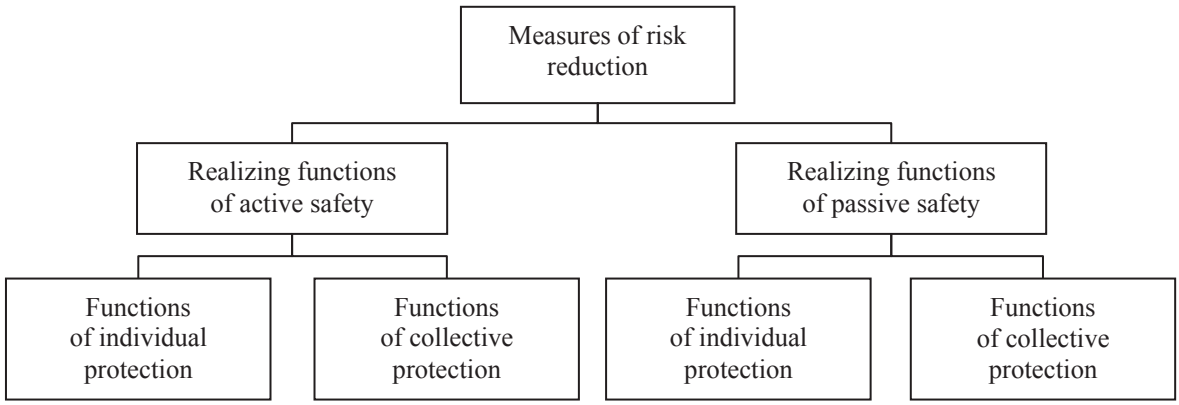

Fig. 1. Schematics of general classification of risk reduction measures depending on the safety function realized by these measures in safety systems of objects in transport

Intangible measures of risk reduction can be those of an organizational nature. This could for example be a group of people operating according to preset procedures. In this type of measures we can include the measures referred to by R. Studenski (work [18]) *safety standards.* These are standards formulated in regulations, norms and procedures. For their formation knowledge is used that was previously acquired while identifying risks and during risk assessment [18]. The said author says that 'behavioural standards' are of particular importance, among which we can distinguish patterns of realization and patterns of conduct. According to R. Studenski [18] the safety standards can be divided into formal and informal ones. Formal are all those patterns and criteria that comply with the existing regulations and safety standards. Informal standards are both those more stringent standards superimposed by the superiors or the participants of the task groups (more stringent than it results from the applicable norms and regulations) and those less stringent standards superimposed by the superiors or the participants of the task groups [18].

The standards related to the safety of technical objects (e.g. [1, 2]) provide the following classification of risk reduction measures (in these standards referred to as protection measures) [1]: designer (design solutions safe in themselves, shields and other protection devices as well as supplementary protection measures, user information), user (routines of safe operation, supervision, systems of permits for initiation of work, application and use of additional technical protection measures, use of individual protection measures, training).

The authors of work [15] state that the constructor of an object, in order to ensure an acceptable level of risk related to that object can take advantage of a three stage method that consists in using of object operation safety techniques. These are: direct, indirect and warning.

A three-stage classification of risk reduction measures can also be built based on the risk analysis conducted by A.S. Markowski in work [13] for warehousing installations of liquefied gases. The author distinguishes three layers of the safety system:

- preventive layer that prevents occurrence of conditions for releasing of a hazardous substance from the processing apparatus,
- protection layer that protects the processing object and the employees against the consequences of the hazardous substance release,
- counteracting layer that minimizes the consequences of the hazardous substance release.

J. Wicher [22] states that it has been assumed to distinguish two basic vehicle types of safety:

active and passive. However, he indicates another criterion of the division of safety of means of transport and distinguishes its following types [22]: active, passive, post accidental, ecological, constructional. Additionally, he divides the passive safety into internal and external.

The classifications of elements of safety systems are also given by the authors of [7]. According to these authors, we can distinguish the following elements of the safety systems [7]: autonomous/non-autonomous, internal/external, assigned/non-assigned, automated/non-automated.

The classification of the risk reduction measures can also be built in relation to the principle of *deep defence* and *line of prevention* in accident prevention, both resulting from this principle. A. Szymanek states (work [20]) that according to G.L.M. van Wijk in accident prevention there are 5 *lines of prevention*:

1. Safe conduct and anticipation of hazard.
2. Prevention of accidents through protection of an object.
3. Limiting of losses after an accident (loss limitation); examples: evacuation plans, emergency telephones (Fire Department, Police etc).
4. Rapid restoration of system efficiency in order to reduce the losses.
5. Restoration of full system efficiency (revalidation).

In the second line of prevention– prevention of accidents through protection of an object– we can distinguish the following measure of risk reduction [20]:

a. Personal protection measures,
b. General and collective protection measures (fencing, barriers),
c. Improvisation behaviours,
d. Product safety,
e. Product protection e.g. protection against external damage/destruction.

The classification of safety barriers has also been presented by S. Sklet in [17]. The schematics of this classification have been presented in Fig. 2.

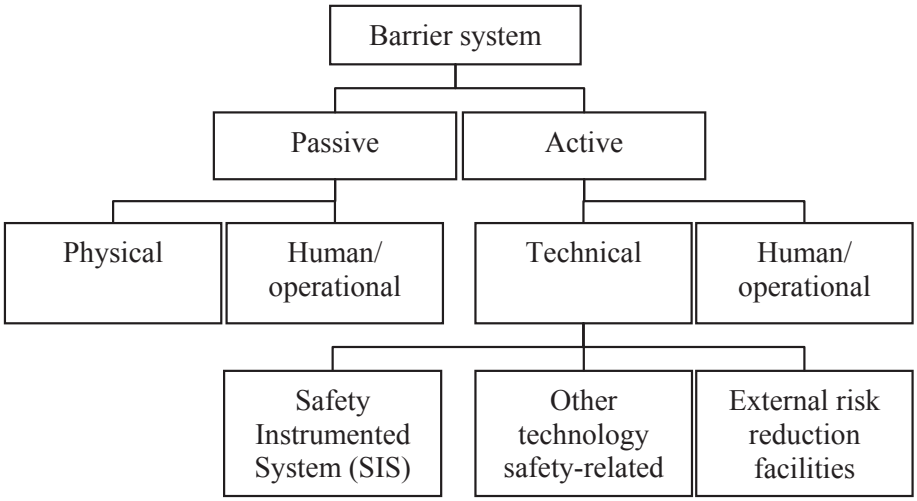

Fig. 2. Schematics of classification of safety barriers [17]

Using the here presented classifications (Fig. 3) schematics of risk reduction measures have been presented in safety systems of technical objects.

3. The concept of identification of safety system model layers

3.1. Preliminary remarks

Assuming that the form of the safety system model depends on the adopted classification of the risk reduction measures we can perform an identification of the layers of this model. The identification consists in determining (naming and marking) of the layers of the model according

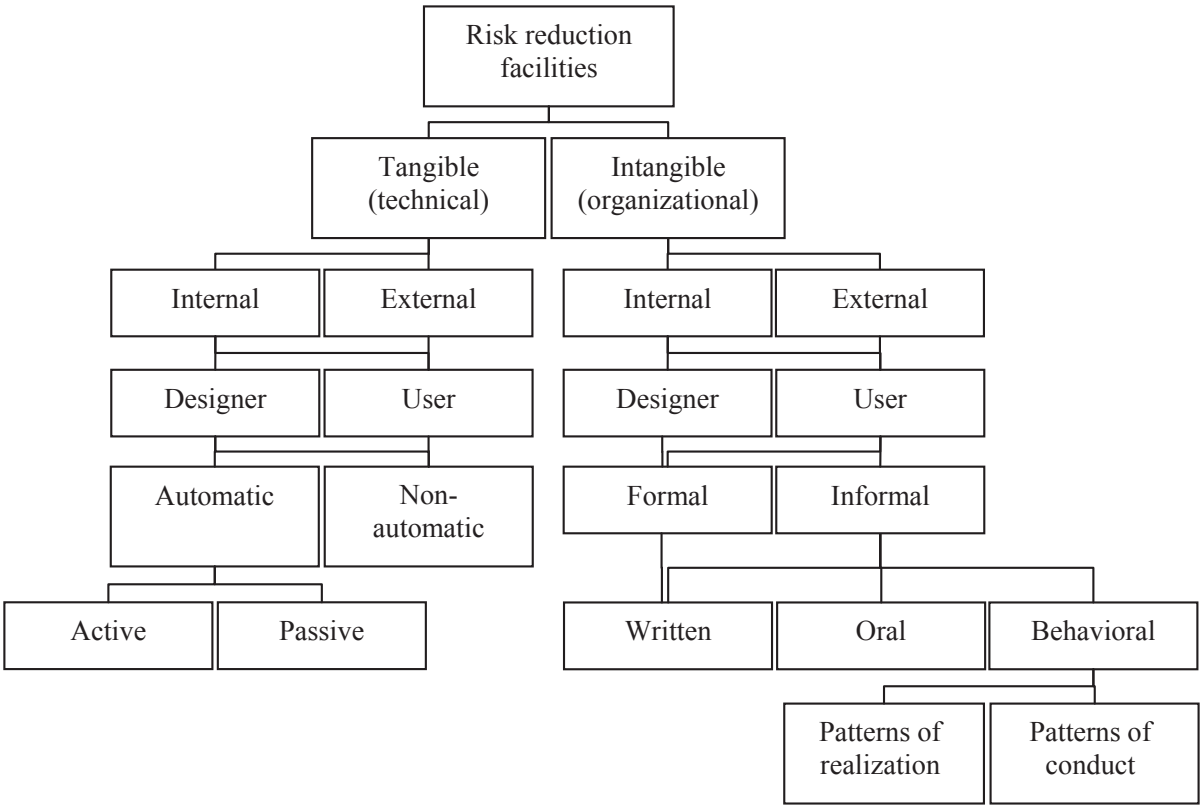

Fig. 3. The schematics of the classification of risk reduction measures used in safety systems of technical objects depending on the form of these measures. Own design based on [1, 2, 7, 13, 15]

to the adopted classification and assigning the risk reduction measures used in the safety system to the appropriate layers of this model. The here presented concept of identification of the object safety system model layers assumes three consequent ways of the realization of the identification process (schematically presented in Fig. 4):

1. Determining (naming and marking) of the safety system model layers based on the existing safety system.
2. Adopting of a layer model of the safety system according to the classification of the risk reduction measures.
3. Identification of the safety system model layers based on the known multi layer safety systems.

The schematic of one of the stages of the identification that includes the adopted classification of the risk reduction measures has been shown in Fig. 5. On the stage of assigning of the risk reduction measures to appropriate layers of the model of the safety system it is helpful to use full descriptive layers of this model. Such names are obtained based on the marks formulated according to the schematics shown in Fig. 5 and the notations as described in chapter 3.2.

A small number of the layers of the safety system model results in difficulties determining the level of risk reduction. It is the case in complex models of safety systems where to one layer several risk reduction measures of different form and purpose can be assigned. At the preliminary stage of the analyses it is proposed to adopt the most complex form of the safety system model (as shown in Fig. 1) and then carry out simplifications of this model through 'switching off' of individual layers.

3.2. The notation used in the classification of types of risk reduction measures

In the adopted notation a layer in the safety system is described with an appropriate number of symbols divided by a slash. Each of the symbols denotes an individual feature of the safety system

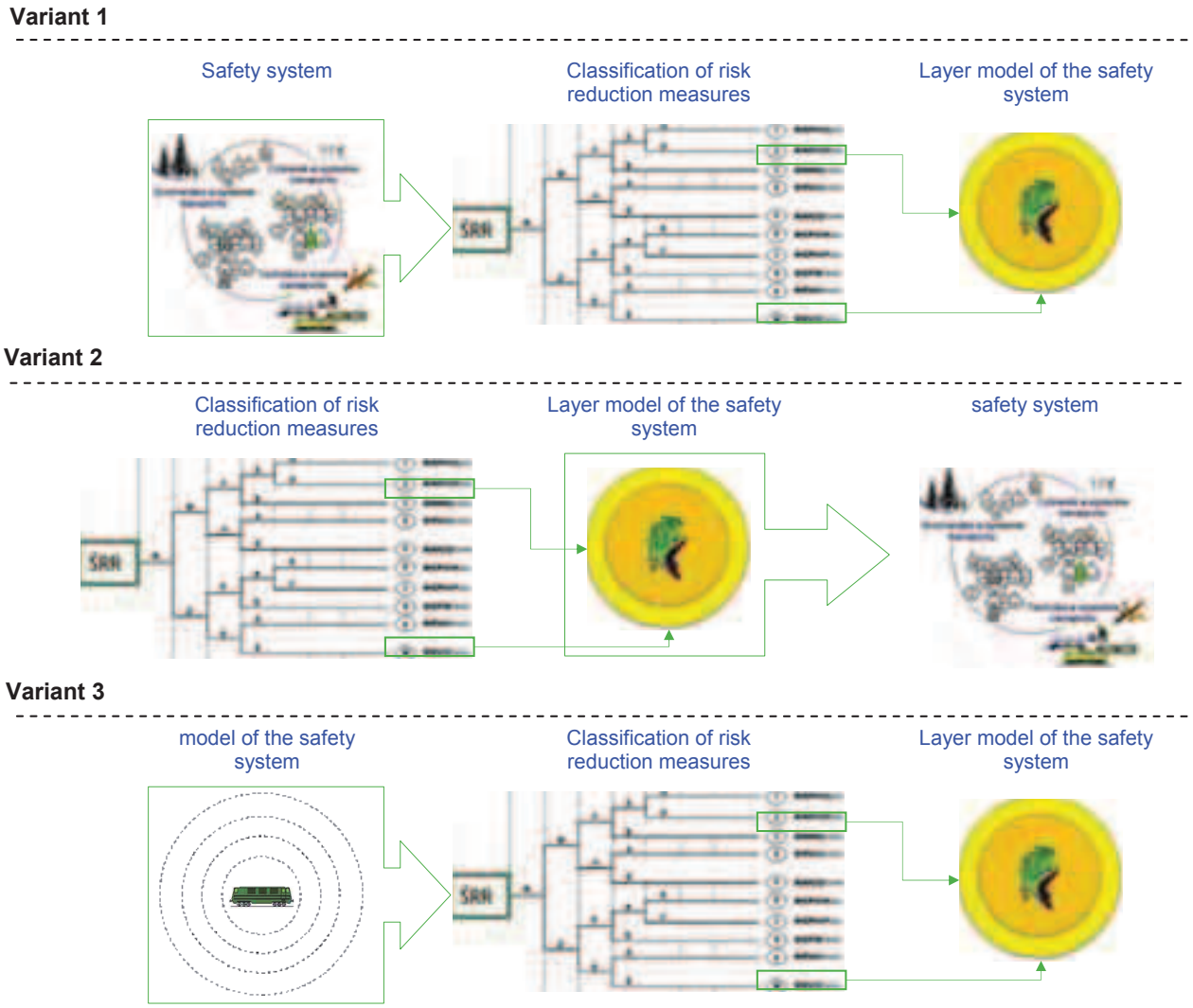

Fig. 4. The concepts of use of the classification of risk reduction measures in identification of the safety system model layers

layer resulting from the adopted classification of the risk reduction measures. In the case of the proposed seven-stage classification we can distinguish fifteen symbols:

M – T*angible risk reduction measures*. These are measures of technical nature, whose task is to eliminate sources of hazard or reduce the exposure to these sources through blocking a flow or stream of energy, materials or information.

N – *intangible risk reduction measures*. These are measures of organizational nature whose task is to eliminate sources of risk or reduce the exposure that comes from these sources as well as reducing the consequences of unwanted events through appropriately established procedures.

W – *internal risk reduction measures*. These are tangible measures inside a technical object (usually integrated with the object) or intangible measures that refer exclusively to the object under analysis.

Z – ex*ternal risk reduction measures*. These are tangible measures located outside a technical object or intangible measures designed for a wider variety group of objects not under analysis here.

P – *risk reduction measures introduced by the designer*. These are tangible measures located inside a technical object (usually integrated with the object) or procedures (manuals) designed and introduced by the designer of the object.

U – *risk reduction measures introduced by the user*. These are tangible measures located inside a technical object (usually integrated with the object), measures applied by the user (individual protection measures).
A – *automatic risk reduction measures*. These are tangible measures located inside or outside a technical object that actuate automatically. For their proper functioning interaction with man is not necessary.
E – *non-automatic risk reduction measures*. These are tangible measures located inside or outside a technical object that do not actuate automatically.
A – *active risk reduction measures*. These are tangible measures whose existence in the system and proper functioning is necessary for the realization of given tasks by the system (basic elements).
P – *passive risk reduction measures*. These are tangible measures (elements of an object) capable of taking over functions of another element of an object (backup elements).
F – *formal risk reduction measures*. Organizational measures (patterns and criteria, actions of operators) compliant with applicable regulations and safety standards.
N – *informal risk reduction measures*. Organizational measures such as own requirements– imposed by the management or the participants of the task forces, more stringent requirements than it would results from the regulations and standards as well as less stringent requirements than it would results from the regulations and standards.
P – *written communications*. Formal or informal communications in a written form initiated by the management or the participants of task forces.
U – *oral communications*. Formal or informal communications in an oral form initiated by the management or the participants of task forces.
B – *behavioural risk reduction measures*. Organizational measures determining the detailed methods of operation (patterns of performance) and determining the behaviour not directly related with the performed tasks (patterns of behaviours).

3.3. Identification of the safety system model layers based on the multi layer safety system models

One of the examples of a layer model of a safety system of objects in transport systems is the safety system model of rail vehicles presented by the authors here (in [3, 4]). In this model a general, two stage classification of the model layers: *preventive layer* whose task is to prevent object damage and *counteracting layer* whose task is to secure a system against serious consequences of damage.

According to the presented schematics of formation of a layer safety system model we can describe the safety system models of object other than those related to transport. An example of such an adaptation (Tab. 1) has been developed for a multi-layer safety system model of objects in the processing industry provided herein [5].

Tab. 1. An example of the adaptation of the idea of identification of safety system model layers of objects on transport to a multi-layer safety system model of objects on the processing industry

Number of layer	Names of the safety system model layers of objects in the processing industry [1]	Identification of the safety system model layer[2]
1	Process automatics	M/W/P/A/A/--/--
2	Alarms + operator	M/W/P/E/--/--/--
3	Failsafe systems	M/Z/P/A/P/--/--
4	Failsafe devices	M/Z/U/A/--/--/--
5	Physical shields	M/W/P/A/P/--/--
6	In-company operational/rescue plans	N/W/U/--/--/F/--
7	External operational/rescue plans	N/Z/U/--/--/F/--

[1] – names of safety system model layers presented in [5]
[2] – identification compliant with the classification of risk reduction measures adopted in this paper (Fig. 5)

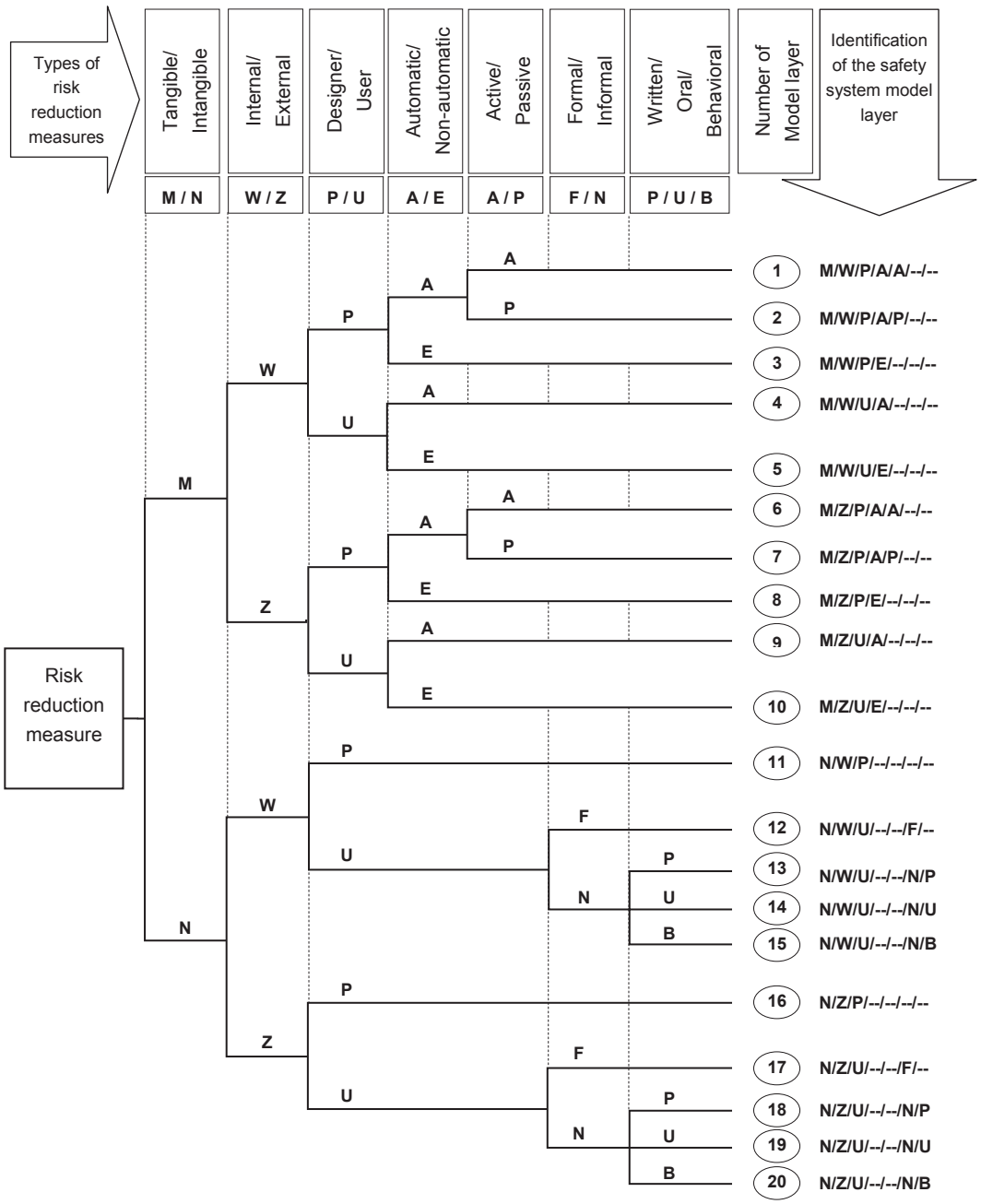

Fig. 5. Schematics of safety system identification of transport systems objects according to the adopted classification of types of risk reduction measures

The model of object safety systems in transport can be presented in the form of *links of the chain of securities* (name used by A. Szymanek, works [19, 20]) designed to the principle (or philosophy) of deep defence. This principle demands formation of chains of physical, technical, procedural and organizational securities that - designed for the MTE system - are to improve the safety level. The subsequent layers of the safety system model adapted analogically to the links of the chain of securities and according to the principle of deep defence would have the following form [20]:

1. 'Process equipment', safe technologies and safe procedures– their role is conducting the process under normal conditions,
2. Safety systems– their role is the realization of protective actions in case of process disturbance,
3. Safety barriers– their role is suppressing (retarding) the development of the sequences (scenarios) of the accident,
4. Safety zones– their role is to limit the spread of the accident results.

Based on so defined links of the chain of securities the layers of the safety system model of objects in transport have been identified and the result have been shown in Tab. 2.

Tab. 2. Example of identification of safety system model layers based on the links of the chain of securities (philosophy of deep defence)

Description of the layer of the model of the object safety system [1]	Number of layer acc. to Fig. 2	Identification of the safety system layer[2]
Process equipment'	1 2	M/W/P/A/A/--/-- M/W/P/A/P/--/--
Safety systems	6	M/Z/P/A/A/--/--
Safety barriers	7	M/Z/P/A/P/--/--
Safety zones	7	M/Z/P/A/P/--/--

[1] – names of safety system model layers presented in works [19, 20]

E. Hollnagel presented (work [6]) types of *safety barriers*. These barriers can be treated as further layers of the model of safety systems. For the sake of identification of the layers of the object safety system model the authors used both the names of the types of barriers and determinations of the safety roles that these barriers play. The results of the identification have been shown in Tab. 3.

Tab. 3. Example of identification of safety system model layers based on the classification of the safety barriers and their safety functions

Description of the layer of the object safety system model		Number of layer acc. to Fig. 2	Identification of the safety system layer[2]
Type of barrier[1]	Functions of the barrier[1]		
Tangible, physical	Retarding	7	M/Z/P/A/P/--/--
	Limiting	7 2	M/Z/P/A/P/--/-- M/W/P/A/P/--/--
	Maintaining, merging	1	M/W/P/A/A/--/--
	Separating, blocking	2	M/W/P/A/P/--/--
Functional	Preventing motion or mechanical operation	3	M/W/P/E/--/--/--
	Preventing flow of information or logical action	11	N/W/P/--/--/--/--
	Obstructing action	2	M/W/P/A/P/--/--
	Water sprinkling, soothing	1	M/W/P/A/A/--/--
	Dispersing, absorbing	2	M/W/P/A/P/--/--
Symbolic	Counteracting	5	M/W/U/E/--/--/--
	Regulative	11	N/W/P/--/--/--/--
	Influencing	2	M/W/P/A/P/--/--
	Permitting	12	N/W/U/--/--/F/--
	Communicating	13 14	N/W/U/--/--/N/P N/W/U/--/--/N/U
Intangible	Monitoring	6	M/Z/P/A/A/--/--
	Recommending	16	N/Z/U/--/--/F/--

[1] – names of the safety barriers and their functions are based on [6]

5. Final remarks

The authors of the paper presented a concept of identification of protection layers in multi-layers safety systems. The realization of the identification process can be – as per the presented idea – conducted in three ways. The authors presented a way consisting in determining of the safety system model layer based on the known multi-layer models of these systems. It has been observed that in the known (existing) model of safety systems the protection layers are usually defined in a general way and it is difficult to indicate the exact criteria of classification of these layers. Besides, the names used in the models, are not unified even in the case of similar safety systems. This became a basis for the development of the here presented concept of identification of protection layers in multi-layer models of safety systems. The basis of the identification process is the developed classification of the risk reduction measures and the schematically presented procedure of determining (naming and marking) of the model layers and assigning the risk reduction measures to their appropriate layers. This aims at systemizing the procedures of analysis of the functioning of the safety system particularly at the stage of creation of the models of these systems and at the stage of evaluation of efficiency of the protection layers. An important element of the procedures, particularly in the aspect of creation of their computer algorithms, is the here presented notation of the protection layers.

References

[1] *Bezpieczeństwo maszyn. Pojęcia podstawowe, ogólne zasady projektowania*. Część 1: Podstawowa terminologia, metodyka. PN-EN ISO 12100-1:2005.

[2] *Bezpieczeństwo maszyn. Pojęcia podstawowe, ogólne zasady projektowania.* Część 2: Zasady techniczne. PN-EN ISO 12100-2:2005.

[3] Gill, A., Kadziński, A., *System obsługiwania pojazdów szynowych jako element w warstwowym modelu ich systemów bezpieczeństwa*, Pojazdy Szynowe, Nr 4, pp. 31-38, 2006.

[4] Gill, A., *Procedury decyzyjne w obsługiwaniu obiektów systemów technicznych uwzględniające analizę ryzyka*, rozprawa doktorska, Politechnika Poznańska, Wydział Maszyn Roboczych i Transportu, Poznań 2007.

[5] Głodek, W., *Automatyka zabezpieczeniowa w przemyśle procesowym – przegląd unormowań*. Warsztaty SIPI61508, http://www.sipi61508.com/ciks/pl.glodekw.pdf, Gdynia 2003.

[6] Hollnagel, E., *Risk+barriers=safety?* Safety Science 46, pp. 221–229, wersja elektroniczna: zasoby Science Direct, Wyd. Elsevier Journals, 2008.

[7] Jaźwiński, J., Ważyńska-Fiok, K., *Bezpieczeństwo systemów*, Wyd. PWN, Warszawa 1993.

[8] Kosmowski, K. T., *Aktualne problemy analizy ryzyka i zarządzania bezpieczeństwem w systemach technicznych*, w mat. konferencji Analiza ryzyka i zarządzanie bezpieczeństwem w systemach technicznych, pp. 33-52, Gdańsk–Gdynia 2001.

[9] Kosmowski, K. T., *Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych*, monografia, Wyd. Politechniki Gdańskiej, Gdańsk 2003.

[10] Kosmowski, K. T., *Rozwój techniki i problemy zarządzania bezpieczeństwem*, w mat. konferencji naukowo-technicznej z sesjami warsztatowymi Zarządzanie bezpieczeństwem funkcjonalnym, pp. 21-46, Jurata 2004.

[11] Kosmowski, K. T., *An integrated analysis of protection layers in hazardous systems*, w mat. The 4th International Conference on Safety and Reliability, Journal of KONBiN, Wyd. Instytutu Technicznego Wojsk Lotniczych, Nr 1, pp. 305-313, Warszawa 2006.

[12] Markowski, A. S., *Zapobieganie stratom w przemyśle*, cz. 3, Zarządzanie bezpieczeństwem i higieną pracy, Wyd. Politechniki Łódzkiej, Łódź 2000.

[13] Markowski, A. S., *Ilościowa analiza ryzyka dla instalacji magazynowych gazów skroplonych*, w mat. Konferencji Analiza ryzyka i zarządzanie bezpieczeństwem w systemach technicznych, pp. 121-137, Gdańsk–Gdynia 2001.

[14] Markowski, A. S., Borysiewicz, M., *Zastosowanie analizy warstwy zabezpieczeń do oceny ryzyka dla rurociągów*, w mat. z warsztatów nt. Modele i narzędzia dla oszacowania ryzyka związanego z transportowaniem niebezpiecznych substancji rurociągami, MANHAZ, Instytut Energii Atomowej, Otwock-Swierk.
[15] Pahl, G., Beitz, W., *Nauka konstruowania*, Wydawnictwa Naukowo-Techniczne, WNT, Warszawa 1984.
[16] Rozporządzenie Komisji (WE) Nr 352/2009 z dnia 24 kwietnia 2009 r w sprawie przyjęcia wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka, o której mowa w art. 6 ust. 3 lit. a) dyrektywy 2004/49/WE Parlamentu Europejskiego i Rady. Dziennik Urzędowy Unii Europejskiej.
[17] Sklet, S., *Safety barriers: Definition, classification, and performance*. Journal of Loss Prevention in the Process Industries 19, pp. 494–506, Wyd. Elsevier Journals, 2006.
[18] Studenski, R., *Organizacja bezpiecznej pracy w przedsiębiorstwie*, Wydawnictwo Politechniki Śląskiej, Gliwice 1996.
[19] Szymanek, A., *Bezpieczeństwo i ryzyko w technice*, Wydawnictwo Politechniki Radomskiej, Radom 2006.
[20] Szymanek, A., *Zasada głębokiej obrony a zarządzanie bezpieczeństwem transportu*, VII Konferencja Naukowo-Techniczna LOGITRANS nt. Logistyka, Systemy Transportowe, Bezpieczeństwo w Transporcie, Szczyrk 2010.
[21] Valis, D., Koucky, M., *Selected overview of risk assessment techniques*, Problemy Eksploatacji, Wyd. Instytutu Technologii Eksploatacji – PIB, Z. 4, (75), pp. 19-32, Radom 2009.
[22] Wicher, J., *Bezpieczeństwo samochodów i ruchu drogowego*, WKŁ, Warszawa 2002.
[23] Krystek, R., (red.), *Zintegrowany System Bezpieczeństwem Transportu*, *Uwarunkowania rozwoju integracji systemów bezpieczeństwa transportu*, Politechnika Gdańska, T. 2, R. 7.3.2, Kadziński A., Gill A., Integracja pojęć, WKŁ, pp. 285-288, Warszawa 2009.