Journal of KONBiN 3(6)2008
ISSN 1895-8281

DOI 10.2478/v10040-008-0060-4

METHODOLOGICAL ISSUES OF SECURITY VULNERABILITY ANALYSIS AND RISK ASSESSMENT

METODYCZNE PROBLEMY ANALIZY PODATNOŚCI NA UTRATĘ INTEGRALNOŚCI I OCENY RYZYKA

Aleksandra Bobcow[1], Kazimierz T. Kosmowski[2]

Gdansk University of Technology, Faculty of Electrical and Control Engineering
Politechnika Gdańska, Wydział Elektrotechniki i Automatyki
G.Narutowicza 11/12, 80-952 Gdansk

(1) a.bobcow@ely.pg.gda.pl, (2) k.kosmowski@ely.pg.gda.pl

Abstract: This article addresses methodological issues associated with the safety and security management of hazardous plants. It is emphasized that there are important installations and systems for the safety and security that require a special attention. A knowledge-based methodology for integrated LOPA (layer of protection analysis) & ROPA (rings of protection analysis) is proposed for further research to develop relevant methods and tools for supporting integrated safety and security management based on assessments of relevant risks.

Keywords: safety of hazardous plants, security vulnerability analysis

Streszczenie: Niniejszy artykuł przedstawia problemy metodyczne związane z zarządzaniem bezpieczeństwem i ochroną instalacji podwyższonego ryzyka. Podkreślono, że występują ważne dla bezpieczeństwa i ochrony instalacje, które wymagają specjalnej uwagi. Zaproponowano do dalszych badań metodykę opartą na wiedzy do zintegrowanej analizy LOPA (warstw zabezpieczeń) i ROPA (pierścieni zabezpieczeń) w celu opracowania metod i narzędzi do wspomagania zintegrowanego zarządzania bezpieczeństwem i ochroną w oparciu o oceny odpowiednich ryzyk.

Słowa kluczowe: bezpieczeństwo instalacji podwyższonego ryzyka, analiza podatności na utratę integralności

METHODOLOGICAL ISSUES OF SECURITY VULNERABILITY ANALYSIS AND RISK ASSESSMENT

1. Introduction

The safety management of hazardous plants and critical infrastructures is currently in the face of a need to assess whether the security measures address sufficiently current and emerging threats [4, 6, 7]. The problem is to recognize the situation at given site and make rational enhancements to provide balanced safety and security measures to protect effectively the workers, public and the environment [5, 8, 9].

Security of technical systems should be balanced with some objectives, and has to be commensurate with the potential consequences of critical scenarios and their likelihood. In some industrial plants, like refineries and chemical plants, the range of hazards is relatively high. In such plants managing the security vulnerabilities is a key issue [8]. Thus, the safety and security oriented risk assessment should be performed in an integrated way in life cycle of the plant. The problem is quite complex and requires a new approach. An example of the problem could be how to design and operate the access control system within security system of a hazardous industrial plant [2].

This article is devoted to some methodological aspects of security vulnerability analysis and risk assessment in the process of integrated safety and security management of hazardous plants. It is emphasized that there are hazardous installations and systems requiring a special concern and protection, especially the information and communication technologies (ICT) systems, distributed control and protection systems supervised from the control room and other communication facilities, e.g. from the level of BMS (*ang. building management system*). These issues are related to implementing in practice the series of international standards ISO/IEC 27000 (Information Safety Management System). Challenges concerning the security vulnerabilities managing in potential situations of malicious acts are also discussed.

A widely accepted in USA methodology for dealing with security aspects in hazardous industrial plants is the security vulnerability analysis (SVA) methodology [12]. It allows companies to evaluate the vulnerability of their hazardous plants to terrorist attack or other malicious acts and, based upon

the risk assessment, to plan enhanced security measures where appropriate [8]. Prior to September 11th, 2001 threats from terrorist attack on hazardous installation were considered to be unlikely, so that they were not included in security plans or in the safety and security analyses, except in special circumstances. The relatively high consequence events that are possible from malicious acts at chemical sites should now be considered in the design and operation of these plants and critical infrastructures in general [3, 4, 6, 7, 11]. The research works in the security area have been also undertaken in Europe [10, 11, 15, 16].
In this article some issues associated with integrated safety and security management of hazardous plants are also discussed.

2. Safety and security vulnerability analysis of hazardous plants

2.1. Layers of protection of industrial hazardous plant

Hazardous industrial plants are nowadays designed according to a concept of defense in depths with distinguishing several protection layers. Designing these layers and safety-related systems is based on the risk analysis and assessment. The safety integrity of these systems is verified using methods of probabilistic modeling. Figure 1 shows typical layers of protection of a hazardous industrial plant. An interesting methodology for preliminary risk analysis and safety-related decision making is the layer of protection analysis (LOPA) methodology [14].

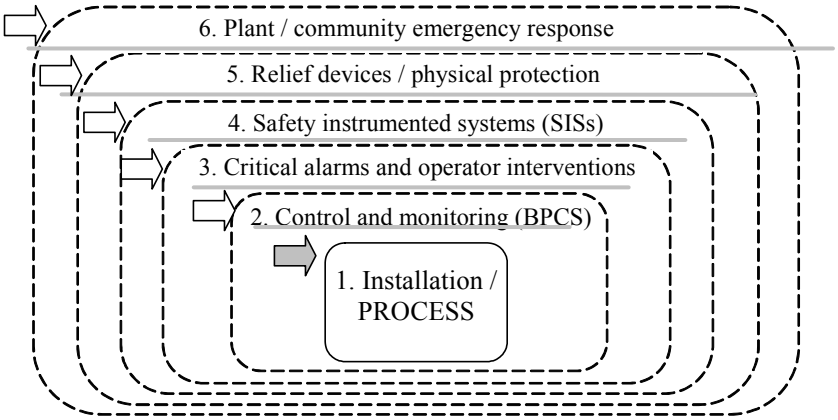


Figure 1. Typical protection layers in hazardous installation

2.2. Security vulnerability analysis and management

The security vulnerability analysis (SVA) is a process of determining the likelihood of an adversary successfully exploiting this vulnerability leading to a degree of impact or damage on assets. The SVAs are qualitative analyses based on the best judgment of the security and safety experts [12]. The determination of risks is of interest to provide the basis for ranking the security-related risks to establish priorities for the application of safeguards and countermeasures. Assets may be categorized as people, chemicals (used or produced), information, environment, equipment, facilities, activities and operations, etc.

Threat (T) is any indication, circumstance, or event with the potential to cause the loss of, or damage to, an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets [12]. Adversaries may be categorized as: insiders, outsiders, and insiders acting in collusion with outsiders.

The vulnerability (V) is the characteristic of an element of the critical infrastructure, assessed in design or operation, which renders it susceptible to destruction or incapacitation by a threat. Vulnerabilities include any weakness that can be exploited by an adversary to gain access to an asset. Vulnerabilities can include, but are not limited to: building characteristics, equipment properties, personnel behavior, locations of people, equipment and buildings, or operational practices and personnel customs, etc.

The risk expresses the potential for damage to or loss of an asset. It is an expression of the likelihood (L) that a specific vulnerability (V) of a particular attractive target (AT) will be exploited by a defined threat (T) to cause a given consequence (C) on an asset with evaluated severity (S) [12]. A risk assessment provides the basis for ranking risks and thus establishing priorities for the application of countermeasures.

The risk management is a deliberate process of understanding risk and deciding upon, to implement actions aimed at reducing risk to a defined level to an acceptable level of risk and at rational cost. This approach is characterized by identifying, evaluating and controlling risks to a level commensurate with an assigned level. It includes the process of selecting and implementing security countermeasures to achieve an acceptable level of risk at an acceptable cost.

2.3. Rings of protection analysis including physical and cyber security

The fundamental concept of rings of protection is that, if possible, the most important or most vulnerable assets should be placed in the center of concentric levels of increasingly more stringent security measures [12]. For example, where feasible, the control room in hazardous plant should not be placed right next to the building's reception area but rather it should be located deeper within the building. So that, to reach the control room, an intruder would have to penetrate numerous rings of protection, such as a fence at the property line, a locked exterior door, an alert receptionist, an elevator with key-controlled floor buttons, and a locked door to the control room.

Technical security is implemented using the electronic systems for increased protection or security purposes including the access control systems, card readers, keypads, electric locks, remote control openers, alarm systems, intrusion detection equipment, annunciating and reporting systems, central stations monitoring, video surveillance equipment, voice communications systems, listening devices, and computer security, encryption, data auditing, scanners, etc. [12].

Examples of protection rings and their component countermeasures are graphically depicted in Figure 2. The security oriented risk analysis will be called the rings of protection analysis (ROPA). Two kinds of solutions are distinguished: physical security and cyber security.

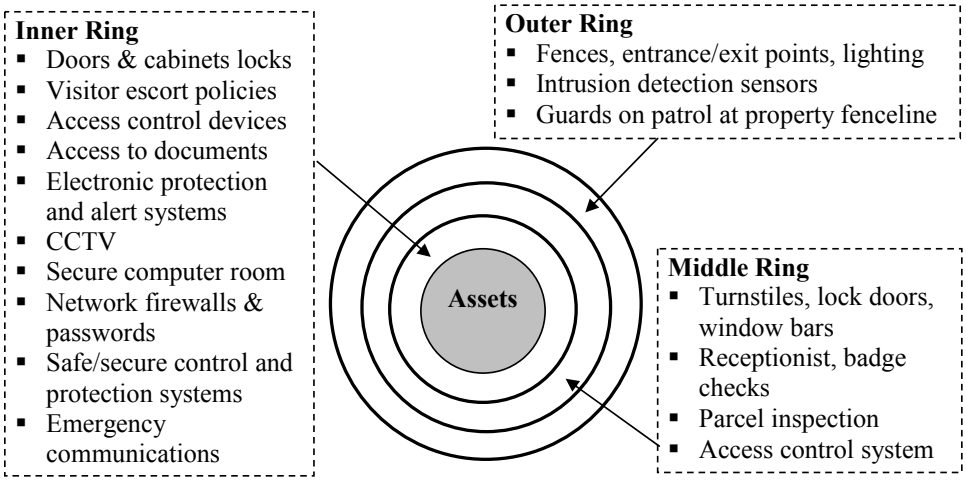


Figure 2. Rings of protection (adaptation of [12])

The objective of physical security (PSec) is primarily to deter or to detect and delay a malicious act by systems and architectural features to improve protection. Examples include fencing, doors, gates, walls, turnstiles, locks, vehicle barriers, and hardened glass, etc.
The objective of cyber security (CSec) is to protect the vital information systems that include hardware, software, infrastructure as well as the information loss due to corruption, theft, or damage.
In a hazardous chemical facility, protecting the information and computer networks means more than safeguarding company's proprietary information and keeping the business running. It also means protecting chemical processes from hazardous disruptions and preventing unwanted chemical releases. An adversary network access can provide the power to harm the company, its employees, and the community at large [2, 8, 9, 12]. It is also related to using safe programmable electronic systems operating in networks: local area network (LAN) and wide area network (WAN).
The objective is to establish physical security and procedural control measures in the control room and safety-related systems to provide their integrity. It concerns also distributed control systems (DCS) including programmable basic process control system (BPCS) and programmable logic controllers (PLC) as elements of the safety instrumented systems (SISs) [4, 14].

3. Security-related risk assessment and management

The qualitative determination of risk, which is one of the desired outcomes of the SVA [12], provides the basis for establishing priorities to apply countermeasures. It is similar to the qualitative risk analysis process that is routinely applied is assessing accidental risk [14] at the same facilities. Countermeasures are actions taken to reduce or eliminate one or more vulnerabilities. The countermeasure may also affect the threat(s) as well as properties an asset or set of assets. The cost of a countermeasure may be monetary, but may also be non-monetary costs such as reduced operational effectiveness, adverse publicity, unfavorable working conditions, and political consequences.

During the SVA process (see Figure 3) the assessments are made of the effectiveness and reliability of the countermeasures against the threats and vulnerabilities of the assets. If deemed necessary due to a high level of risk, enhanced countermeasures may be considered to improve the existing security systems. Examples of the countermeasures' types are as follows: physical security, access control, loss prevention, material control and

inventory management, control room security, crisis management and emergency response as well as policies and procedures, and information/cyber security. Security-related intelligence and inherent safety of the installation can be also considered as countermeasures [12].
The inherent safety is a characteristic of hazardous plant with relatively low probability and limited consequences of abnormal states and accidents in situations of external disturbances, failures and human errors. Also in cases of malicious acts the resulting consequences are usually relatively low than in hazardous plants not having such properties of inherent safety.

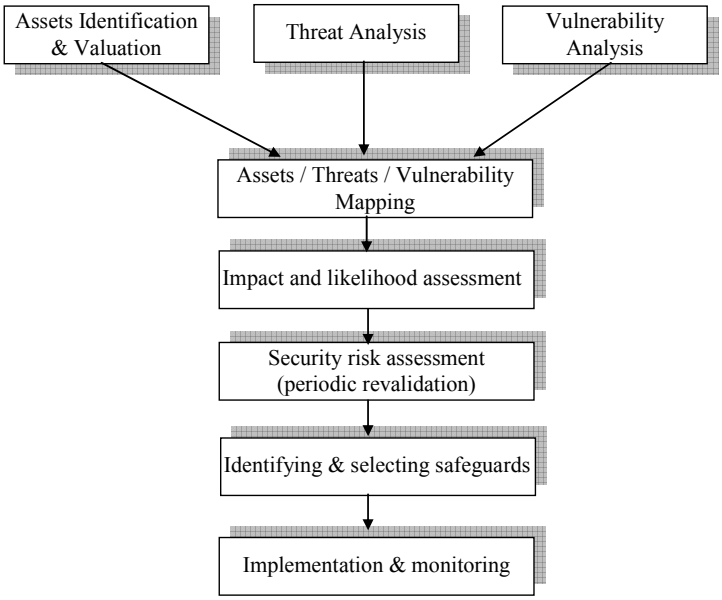


Figure 3. Security-related risk assessment and identifying safeguards

An example of the risk ranking matrix as the result of SVA analysis is shown in Figure 4. Each category of severity is to be defined as it is justified in given case. For instance, the severity S_5 can be defined in qualitative or semi-quantitative way as follows [12]:

A. Many offsite fatalities from large-scale toxic or flammable release possible;
B. Major environmental, food chain, or product impact with possible widespread major health impact on the population (e.g., large-scale toxic contamination of drinking water);
C. More than $ 100 millions of property damage.

S→ L↑	S_1	S_2	S_3	S_4	S_5
L_5	R_3	R_3	R_4	R_5	R_5
L_4	R_2	R_3	R_3	R_4	R_5
L_3	R_2	R_2	R_3	R_3	R_4
L_2	R_1	R_2	R_2	R_3	R_3
L_1	R_1	R_1	R_2	R_2	R_3

Figure 4. An example of the risk ranking matrix for five levels of severity (S), likelihood (L) and risk (R)

Examples of qualitative description of security–related categories of likelihood and severity of potential undesired events in a hazardous industrial plant are presented in Table 1.

Table 1. Qualitative description of security–related categories of likelihood and severity of potential undesired events in hazardous plants

Likelihood categories	L_1 *Very low*	L_2 *Low*	L_3 *Medium*	L_4 *Probable*	L_5 *Frequent*
Description	*Malicious act unlikely*	*Malicious act no likely*	*Malicious act rather likely*	*Malicious act likely*	*Malicious act very likely*
Severity categories	S_1 *Negligible*	S_2 *Marginal*	S_3 *Large*	S_4 *Critical*	S_5 *Catastrophic*
Description of severity: Health Environment	*Negligible health effects* *Negligible environmental impact*	*Injuries or illness* *Impact to immediate site only*	*Widespread health effects* *Major environmental impact*	*Few offsite fatalities* *Local food chain or product impact*	*Many offsite fatalities* *Widespread food chain impact*

The qualitative risk ranking scheme, similar to the preliminary hazard analysis (PHA), method can be used, e.g. according to MILSTD- 882B [12]. The risk levels to be assessed may be classified as follows: R_1 – acceptable, R_2 – acceptable conditionally, only if costs of the risk reduction is very high

(unacceptable), R_3 – the risk must be reduced in given time horizon, R_4 – the risk must be reduced in a relatively short time horizon agreed upon, R_5 – the plant must be shut-down immediately, start up is possible after proving that the security risk was reduced at least to the level R_2.
How risk should be reduced is supported by the analysis of countermeasures to identify where a shortfall between the existing security and the desirable security is, or when additional formal requirements are introduced to reduce risks. Each potential target is protected against the highest-level threat associated with that specific target. Safeguards are selected from source guide with suggested list of countermeasures [12].
The SVA team should make some determination using expert judgement, that if the selected measures were implemented, what level of risk reduction will be achieved. There are two approaches for identifying protections:

- The asset-based approach applies a predetermined security performance standard to increase protection for given target.
- The scenario-based approach may yield more cost effective solutions, as the solutions are tailored to each of the scenarios developed.

Depending on the scenario, the policy or procedural changes, physical security upgrades, barriers, software upgrades, the addition guard, etc. are considered. For instance, the access control system classification considers the security level based on two basic items: identification class and access classification. For each access control point 5 classes of identification and verification were distinguished [1].
There is a substantial problem to protect the computer resources, which should be supported by *Information Security System Management* (ISSM), designed e.g. according to the ISO/IEC 27001:2005. ISSM must be carefully designed to enable protecting the information resources and infrastructures with regard to results of the risk assessment. ISSM should support also the security management of programmable control and protection systems of technological processes and computerized information systems in relevant networks [2, 8].

4. Conclusion

The industry is currently in the face of a need to assess whether current security measures effectively address new threats and make enhancements to provide effective safety and security measures to protect adequately the workers, public and the environment. Security of industrial hazardous plants has to be balanced with other objectives to be commensurate with the threat and likelihood of critical scenarios. In some industrial plants, like refineries

and chemical plants, the range of hazards is relatively high. In such plants managing the security vulnerabilities is a key issue.
The risk assessment methods used for the safety management are not fully applicable for the security assessment. The system security analysis and risk assessment for the security management are based intensively on expert opinions and qualitative information. Due to importance of the problem for industrial practice and critical infrastructures, further research should be undertaken to develop integrated methodology and criteria for the safety and security assessments. A knowledge-based methodology integrating the LOPA (layer of protection analysis) & ROPA (rings of protection analysis) is currently in development together with relevant methods and tools for supporting integrated safety and security management, based on assessments of relevant risks.

References

1. Bobcow A., Kosmowski K.: *Managing the Security Vulnerabilities of Critical Systems and Hazardous Plants*. Chapter 16 in: Functional Safety Management in Critical Systems. Gdansk University of Technology. Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk, 2007.
2. Byres E., Lowe J.: *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*. British Columbia Institute of Technology, Burnaby. Canada & PA Consulting Group, London, 2004.
3. Gheorghe V., Mili L. (Editorial): *In risk management, integrating the social, economic and technical aspects of cascading failures across interdependent critical infrastructures*. International Journal of Critical Infrastructures 1, 2004 (1-7).
4. Kosmowski K.T.: *Challenges in security and safety management of critical systems and infrastructures*. Proceedings of the International Conference on Technologies for Homeland Security and Safety (eds. A. Stepnowski, A. Ruciński, K. Kosmowski). Gdansk University of Technology, Gdańsk, 2005 (511-520).
5. Landoll D.J.: *The Security Risk Assessment Handbook*. Auerbach Publications, Taylor & Francis Group. New York, 2006.
6. Masse T., O'Neil S., Rollins J.: *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*. Prepared for Members and Committees of Congress, Congressional Research Service, 2007.

7. Moteff J., Copeland C., Fischer J.: *Critical Infrastructures: What Makes an Infrastructure Critical?* Congressional Research Service, The Library of Congress; Resources, Science, and Industry Division; August 30, 2002.
8. Sticles R.P., Ozog H.: *Facility Major Risk Survey*. ioMosaic Corporation. Salem, 2002.
9. Sticles R.P., Ozog H., Mohindra S.: *Security Vulnerability Assessment (SVA) Revealed*. ioMosaic Corporation. Salem, 2003.
10. Commission Decision of 4th February 2005: *Concerning the adoption of the Programme of Work 2005 for the Preparatory Action in the field of Security Research*. C(2005) 259. Brussels, 18.01.2005.
11. *Critical Infrastructure Protection in the fight against terrorism*. Communication from the Commission to the Council and the European Parliament. COM(2004) 702 final. Brussels, 20.10.2004.
12. *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*. Center for the Chemical Process Safety of the American Institute of Chemical Engineers. New York, 2003.
13. *General Security Risk Assessment Guideline*. ASIS International. Alexandria 2003.
14. *Layer of Protection Analysis, Simplified Process Risk Assessment.* Center for Chemical Process Safety, American Institute of Chemical Engineers. New York, 2001,
15. *On the implementation of the Preparatory Action on the enhancement of the European industrial potential in the field of Security Research*, Towards a programme to advance European security through Research and Technology. COM (2004) 72 final. Brussels, 3.02.2004.
16. *Research for a Secure Europe*. Report of the Group of Personalities in the field of Security Research. Luxembourg, Office for Official Publications of the European Communities, 2004.

METODYCZNE PROBLEMY ANALIZY PODATNOŚCI NA UTRATĘ INTEGRALNOŚCI I OCENY RYZYKA

1. Wstęp

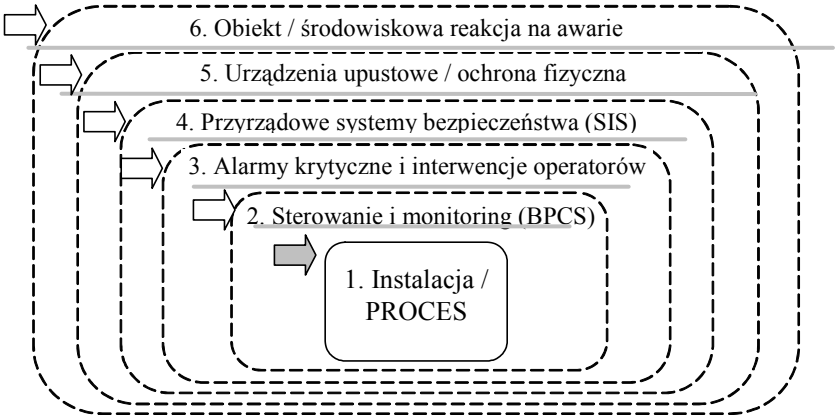
Zarządzanie bezpieczeństwem w obiektach podwyższonego ryzyka i infrastruktur krytycznych staje obecnie w obliczu potrzeby oceny, czy stosowane środki bezpieczeństwa i ochrony są efektywne w odniesieniu do istniejących i wyłaniających się zagrożeń [4, 6, 7]. Problemem polega na rozpoznaniu sytuacji w danym miejscu i racjonalnemu jej ulepszeniu w celu zapewnienia równowagi pomiędzy przedsięwziętymi środkami zaradczymi ochrony i bezpieczeństwa tak, aby ochronić efektywnie pracowników, społeczeństwo i środowisko [5, 8, 9].
Zabezpieczenie systemów technicznych powinno być zrównoważone w odniesieniu do określonych zadań i proporcjonalne do potencjalnych konsekwencji scenariuszy krytycznych i ich prawdopodobieństwa. W niektórych obiektach przemysłowych, jak na przykład rafinerie czy instalacje chemiczne, skala niebezpieczeństwa jest relatywnie duża. W takich obiektach zarządzanie podatnością na utratę integralności jest zadaniem kluczowym [8]. Zatem oceny ryzyka zorientowane na bezpieczeństwo i ochronę powinny być wykonywane w sposób zintegrowany w całym cyklu życia obiektu. Problem jest całkiem złożony i wymaga nowego podejścia. Przykładem może być problem zaprojektowania i użytkowania systemu kontroli dostępu w ramach systemu ochrony obiektu przemysłowego podwyższonego ryzyka [2].
Niniejszy artykuł jest poświęcony aspektom metodycznym analizy podatności na utratę integralności (ang. *security vulnerability analysis*) i oceny ryzyka w procesie zintegrowanego zarządzania bezpieczeństwem i ochroną obiektów podwyższonego ryzyka. Podkreśla się, że występują instalacje i systemy podwyższonego ryzyka wymagające specjalnej troski i ochrony, szczególnie systemy informatyczne i telekomunikacyjne ICT (*ang. information and communication technologies*), rozproszone systemy sterowania i zabezpieczeń nadzorowane ze sterowni i inne urządzenia do komunikowania się, na przykład z poziomu BMS (*ang. building management system*). Zagadnienia te są związane z implementacją w praktyce serii norm międzynarodowych ISO/IEC 27000 (*Information*

Safety Management System). Omówione są ponadto wyzwania dotyczące zarządzania podatnością na utratę integralności w potencjalnych sytuacjach działań nieprzyjaznych.
Szerzej akceptowaną metodyką w USA do zajmowania się aspektami ochrony przemysłowych obiektów podwyższonego ryzyka jest metodyka analizy podatności na utratę integralności (SVA) [12]. Pozwala ona przedsiębiorstwom ocenić podatność ich instalacji podwyższonego ryzyka na ataki terrorystyczne i inne nieprzyjazne działania, a także, bazując na ocenie ryzyka, zaplanować udoskonalone środki ochrony, jeśli to uzasadnione [8]. Przed 11 września 2001 roku uważano zagrożenia związane z atakiem terrorystycznym na instalacje podwyższonego ryzyka za nieprawdopodobne, tak, że nie były one uwzględniane w planach bezpieczeństwa i ochrony, za wyjątkiem szczególnych okoliczności. Stosunkowo wysokie konsekwencje zdarzeń wynikających z potencjalnych działań nieprzyjaznych powinny być rozpatrywane w fazie projektowania, a następnie użytkowania tych instalacji oraz systemów infrastruktury krytycznej [3, 4, 6, 7, 11]. Prace badawcze w zakresie zabezpieczeń (ochrony) są podejmowane również w Europie [10, 11, 15, 16].
W niniejszym artykule przedstawia się również niektóre problemy związane z zintegrowanym zarządzaniem bezpieczeństwem i ochroną obiektów podwyższonego ryzyka.

2. Analiza podatności na utratę integralności obiektów podwyższonego ryzyka

2.1. Warstwy zabezpieczeń w przemysłowym obiekcie podwyższonego ryzyka

Obiekty przemysłowe podwyższonego ryzyka są obecnie projektowane zgodnie z zasadą obrony w głąb z wyróżnieniem kilku warstw zabezpieczeniowo-ochronnych. Projektowanie tych warstw i systemów związanych z bezpieczeństwem (ang. *safety-related systems*) bazuje na analizie i ocenie ryzyka. Integralność systemów w rozumieniu bezpieczeństwa (ang. *safety*) jest weryfikowana stosując metody modelowania probabilistycznego. Rys. 1 pokazuje typowe warstwy zabezpieczeniowo-ochronne obiektu przemysłowego podwyższonego ryzyka. Ciekawą metodyką służącą do wstępnej analizy ryzyka oraz podejmowania decyzji związanych z bezpieczeństwem jest metodyka analizy warstw zabezpieczeniowo-ochronnych LOPA (*ang. layer of protection analysis*) [14].



Rys. 1. Typowe warstwy zabezpieczeniowo-ochronne w instalacjach podwyższonego ryzyka

2.2. Analiza i zarządzanie podatnością na utratę integralności

Analiza podatności na utratę integralności SVA (*ang. security vulnerability analysis*) oznacza proces określania prawdopodobieństwa skutecznego wykorzystania tej podatności prowadzący do wpływu w pewnym stopniu na lub zniszczenia aktywów (ang. *assets*). SVA jest analizą jakościową, bazującą na najlepszej ocenie ekspertów w dziedzinie bezpieczeństwa i ochrony [12]. Wyznaczenie określonych ryzyk stanowi podstawę do szeregowania ryzyk związanych z ochroną w celu ustalenia priorytetów zastosowania środków zaradczych i przeciwdziałania. Aktywa mogą klasyfikowane jako: ludzie, chemikalia (używane lub produkowane), informacje, środowisko, wyposażenie, urządzenia, działania i operacje, itp.
Zagrożenie T (ang. *threat*) jest dowolnym znakiem, okolicznością lub zdarzeniem mogącym mieć wpływ na utratę lub zniszczenie aktywów. Zagrożenie może być również zdefiniowane jako zamiar i możliwość przeciwnika podejmującego przedsięwzięcia szkodliwe wobec aktywów krytycznych [12]. Przeciwnicy mogą być klasyfikowani jako: osoby z zewnątrz, personel, oraz personel będący w zmowie z osobami z zewnątrz.
Podatność V (ang. *vulnerability*) jest charakterystyką elementu systemu krytycznego, ocenianą w trakcie projektowania lub użytkowania, który w wyniku zagrożenia staje się podatny na destrukcję lub ubezwłasnowolnienie. Te podatności obejmują wszelkie osłabienia, które

mogą być wykorzystane przez przeciwnika w dostępie do aktywów. Podatności mogą zawierać, ale nie ogranicza się ich do: charakterystyk budowli, właściwości sprzętu, zachowania personelu, rozmieszczenia osób, wyposażenia i budynków lub praktyki operacyjnej i zwyczajów personelu, itp.

Ryzyko wyraża potencjał zniszczenia lub utraty aktywów. Jest ono wyrażane przez prawdopodobieństwo L (ang. *likelihood*), że dana podatność V (ang. *vulnerability*) określonego atrakcyjnego celu AT (ang. *attractive target*) będzie wykorzystana poprzez rozważane zagrożenie T (ang. *threat*) powodujące potencjalnie skutek C (ang. *consequence*) na aktywach z określoną krytycznością S (ang. *severity*) [12]. Ocena ryzyka stanowi podstawę do szeregowania ryzyk i ustalenia w ten sposób priorytetów zastosowania środków zaradczych.

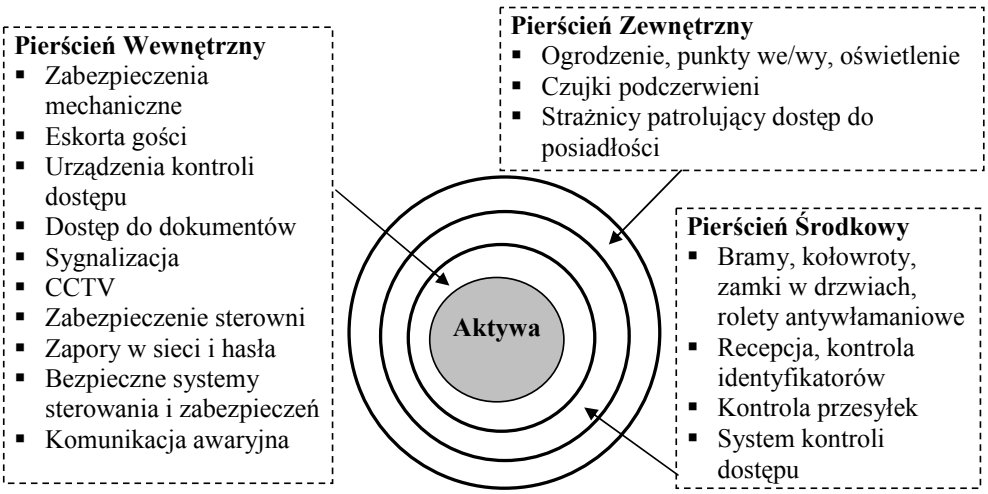
Zarządzanie ryzykiem jest przemyślanym procesem zrozumienia ryzyka oraz podejmowania decyzji, w celu zaimplementowania odpowiednich działań mających na celu zredukowanie ryzyka do akceptowalnego poziomu przy racjonalizowaniu kosztów. Podejście to charakteryzuje się identyfikacją, wyznaczeniem i sterowaniem ryzykiem na określonym poziomie. Łączy się to z wyborem oraz implementacją odpowiednich środków zaradczych, mających na celu uzyskanie akceptowanego poziomu ryzyka przy akceptowalnych kosztach.

2.3. Analiza pierścieni zabezpieczeń fizycznych i cybernetycznych

Podstawą koncepcją pierścieni zabezpieczeń jest, aby, jeśli to możliwe, usytuować najważniejsze lub najbardziej podatne aktywa w centrum koncentrycznych poziomów, coraz bardziej wymagających środków ochrony [12]. Przykładowo, jeżeli to możliwe, sterownia obiektu podwyższonego ryzyka nie powinna znajdować się w pobliżu miejsca recepcji, lecz powinna być usytuowana możliwie jak najgłębiej wewnątrz budynku. Tak, aby intruz przed dostępem do sterowni musiał pokonać jak najwięcej warstw ochronnych, takich jak: ogrodzenie, zamknięte drzwi zewnętrzne, recepcjonistę (strażnika), windę z kontrolą dostępu do poszczególnych poziomów, czy zamykane drzwi do sterowni.

Zabezpieczenia techniczne są wdrażane za pomocą elektronicznych systemów podnoszących poziom bezpieczeństwa lub w celach ochronnych, włączając w to systemy kontroli dostępu, czytniki kart, klawiatury, zamki elektroniczne, zdalne systemy otwierania, systemy alarmowe i raportowania, system monitoringu, podgląd video, systemy komunikacji głosowej oraz powiadamiania o intruzach, oraz zabezpieczenie komputera,

kodowanie danych, uwierzytelnianie dostępu do zasobów komputera, skanowanie, itp. [12].
Przykłady pierścieni ochronnych wraz ze związanymi z nimi środkami zaradczymi zostały zobrazowane na rys. 2. Analizy ryzyka zorientowane na ochronę zostały nazwane analizami pierścieni zabezpieczeń ROPA (ang. *rings of protection analysis*). Wyróżnia się dwa rodzaje zabezpieczeń: zabezpieczenia fizyczne oraz zabezpieczenia cybernetyczne.



Rys. 2. Pierścienie ochrony (adaptacja [12])

Zadaniem zabezpieczeń fizycznych PSec (ang. *physical security*) jest głównie odstraszenie lub wykrycie i zatrzymanie nieprzyjaznych działań przez systemy i rozwiązania architektoniczne w celu poprawy ochrony. Przykładami są ogrodzenia, drzwi, bramy, ściany, kołowroty, zamki, szlabany oraz okna antywłamaniowe, itd.

Zadaniem zabezpieczeń cybernetycznych CSec (ang. *cyber security*) jest ochrona istotnych systemów informacyjnych, które obejmują sprzęt, oprogramowanie, infrastrukturę informacyjną, jak również zagadnienia utraty informacji z powodu korupcji, kradzieży, czy zniszczenia.

W przemysłowych obiektach podwyższonego ryzyka bezpieczeństwo informacji i sieci komputerowej znaczy więcej niż ochrona informacji handlowej. Oznacza to również zabezpieczenie procesu chemicznego przed zaburzeniem i zapobieganie uwolnieniom awaryjnym. Niepowołany dostęp

do zasobów sieciowych może doprowadzić do zaszkodzenia firmie i jej pracownikom oraz stratom społecznym w ogóle [2, 8, 9, 12]. Jest to również związane z zastosowaniem bezpiecznych programowalnych systemów pracujących w sieciach: lokalnej LAN (ang. *local area network*) i rozległej WAN (ang. *wide area network*).

Celem jest wprowadzenie zabezpieczeń fizycznych i proceduralnych środków zaradczych w sterowni i systemach związanych z bezpieczeństwem w celu zapewnienia ich integralności. Dotyczy to również rozproszonych systemów DCS (ang. *distributed control systems*) z włączeniem podstawowego systemu sterowania procesem BPCS (ang. *basic process control system*) oraz programowalnych sterowników PLC (ang. *programmable logic controllers*) jako elementów przyrządowych systemów bezpieczeństwa SIS (ang. *safety instrumented systems*) [4, 14].

3. Ocena i zarządzanie ryzykiem

Jakościowe wyznaczenie ryzyka, które jest jednym z głównych wyników analizy podatności SVA [12], jest podstawą ustalenia priorytetów do wyboru środków zaradczych. Jest to podobne do procesu jakościowej analizy ryzyka, przeprowadzanego rutynowo w ocenie ryzyka awarii [14] w tym samym obiekcie. Środkami zaradczymi są rozwiązania i działania podjęte w celu redukcji lub wyeliminowania podatności na utratę integralności. Środki zaradcze może również wpływać na zagrożenie lub zagrożenia, jak również na właściwości pojedynczego lub zbioru aktywów. Koszty przedsięwzięcia środków zaradczych mogą być wyrażone w jednostkach monetarnych lub w inny sposób, jak na przykład: redukcja efektywności produkcji, negatywny rozgłos, mniej korzystne warunki pracy, a także konsekwencje o charakterze politycznym.

Podczas analizy podatności SVA (zob. rys. 3), są podejmowane oceny efektywności i niezawodności środków zaradczych do stosowania w sytuacji zagrożeń i możliwości utraty aktywów. Jeżeli istnieje taka potrzeba, z uwagi na wysoki poziom ryzyka, mogą zostać rozważone, w celu ulepszenia istniejącego systemu ochrony i zabezpieczeń, szczególne środki zaradcze. Przykładami rodzajów środków zaradczych są: zabezpieczenia mechaniczne, zabezpieczenia fizyczne, kontrola dostępu, zapobieganie stratom, kontrola materiałowa i zarządzanie zapasami, zabezpieczenie i ochrona sterowni, zarządzanie kryzysowe i działania awaryjne, jak również prowadzona polityka i procedury oraz

bezpieczeństwo informacji (cybernetyczne). Zbieranie informacji (ang. *intelligence*) dotyczącej bezpieczeństwa oraz stosowanie rozwiązań inheretnego bezpieczeństwa obiektów mogą być również rozważane jako potencjalne środki zaradcze [12].

Bezpieczeństwo inherentne jest własnością obiektu podwyższonego ryzyka, polegającą na stosunkowo małym prawdopodobieństwie zdarzeń awaryjnych i ograniczonych ich skutkach w sytuacji zewnętrznych zakłóceń, uszkodzeń i błędów ludzkich. Również w przypadkach nieprzyjaznych działań powstające skutki w takich obiektach są zwykle stosunkowo małe w porównaniu z obiektami podwyższonego ryzyka, które nie mają właściwości inherentnego bezpieczeństwa.

Rys. 3. Ocena ryzyka podatności na utratę integralności i identyfikacja środków zaradczych

Przykładową matrycę do klasyfikacji ryzyka na podstawie analizy podatności SVA przedstawiono na rys. 4. Każda kategoria szkodliwości jest definiowana zgodnie z daną sytuacją. Przykładowo, szkodliwość S_5 może być opisana w sposób jakościowy lub półilościowy w następujący sposób [12]:

A. Potencjalnie wielu poszkodowanych w otoczeniu zakładu z uwagi na możliwość wycieku na dużą skalę substancji toksycznych lub palnych;

B. Możliwy poważny skutek środowiskowy lub w łańcuchu żywnościowym powodujący poważne skutki zdrowotne w populacji (na przykład skażenie na dużą skale wody pitnej);

C. Zniszczone mienie na ponad 100 milionów $.

S→ L↑	S_1	S_2	S_3	S_4	S_5
L_5	R_3	R_3	R_4	R_5	R_5
L_4	R_2	R_3	R_3	R_4	R_5
L_3	R_2	R_2	R_3	R_3	R_4
L_2	R_1	R_2	R_2	R_3	R_3
L_1	R_1	R_1	R_2	R_2	R_3

Rys 4. Przykładowa macierz do szeregowania ryzyka dla pięciu stopni szkodliwości S (ang. *severity*), prawdopodobieństwa L (ang. *likelihood*) i ryzyka R (ang. *risk*)

Przykładowe jakościowe definiowanie kategorii prawdopodobieństwa i szkodliwości związanych z utratą integralności (ang. *security*) w obiektach przemysłowych podwyższonego ryzyka zostało przedstawione w tablicy 1.

Tablica 1. Jakościowy opis kategorii prawdopodobieństwa i szkodliwości potencjalnych zdarzeń utraty integralności w obiektach podwyższonego ryzyka

Kategorie prawdopodobieństwa	L_1 *Bardzo małe*	L_2 *Małe*	L_3 *Średnie*	L_4 *Prawdopodobne*	L_5 *Częste*
Opis	*Szkodliwe zdarzenie nieprawdopodobne*	*Szkodliwe zdarzenie mało Prawdopodobne*	*Szkodliwe zdarzenie raczej Prawdowodobne*	*Szkodliwe zdarzenie Prawdowodobne*	*Szkodliwe zdarzenie bardzo Prawdowodobne*
Kategorie szkodliwości	S_1 *Nieistotna*	S_2 *Marginalna*	S_3 *Duża*	S_4 *Krytyczna*	S_5 *Katastroficzna*
Opis szkodliwości: zdrowotnej i środowiskowej	*Nieistotny wpływ na zdrowie* *Nieistotny wpływ na środowisko*	*Zranienia lub zachorowania* *Wpływ tylko na bliskie otoczenie*	*Szeroki zakres skutków zdrowotnych* *Poważny wpływ na środowisko*	*Kilka ofiar śmiertelnych* *Wpływ na łańcuch żywnościowy lub produkty*	*Wiele ofiar śmiertelnych* *Rozległy wpływ na łańcuch żywnościowy*

Schemat szeregowania ryzyka ocenionego jakościowo, podobny do wstępnej analizy ryzyka (PHA – *ang. preliminary hazard analysis*), może być stosowany na przykład zgodnie z MILSTD- 882B [12]. Stopnie ocenianego ryzyka mogą być klasyfikowane następująco: R_1 – dopuszczalne, R_2 – dopuszczalne warunkowo, tylko, jeżeli koszty redukcji ryzyka są bardzo wysokie (nie do zaakceptowania), R_3 – ryzyko musi być zredukowane w danym horyzoncie czasu, R_4 – ryzyko musi zostać zredukowane w możliwie krótkim uzgodnionym czasie, R_5 – obiekt musi być natychmiast odstawiony, a rozpoczęcie produkcji może nastąpić dopiero po udowodnieniu, że ryzyko zostało zminimalizowane przynajmniej do stopnia R_2.

W jaki sposób ryzyko powinno być redukowane zależy od analizy dostępnych środków zaradczych oraz identyfikacji niedostatku pomiędzy istniejącymi a pożądanymi zabezpieczeniami, lub ewentualnie od wprowadzonych dodatkowych formalnych wymagań związanych z redukcją ryzyka. Każdy potencjalny cel jest chroniony przed zagrożeniem najwyższego stopnia związanym z tym szczególnym celem. Środki zaradcze są dobierane zgodnie z istniejącym przewodnikiem źródłowym, zawierającym sugerowaną listę środków zaradczych [12].

Zespół SVA powinien sprawdzać w oparciu o wiedzę ekspertów, jaki poziom redukcji ryzyka zostanie uzyskany w następstwie podjęcia środków zaradczych. Występują dwa podejścia do identyfikacji uzasadnionych zabezpieczeń:

- Podejście bazujące na aktywach, które wymaga zastosowania ustalonych z góry standardów bezpieczeństwa w celu zwiększenia stopnia zabezpieczenia danego celu.
- Podejście bazujące na scenariuszu, które może dawać rozwiązania bardziej efektywne pod względem kosztownym, ponieważ są one dostosowane do konkretnego opracowanego scenariusza.

W zależności od scenariusza, rozważa się zmiany polityki lub proceduralne, rozbudowę ochrony fizycznej i barier, uaktualnianie oprogramowania, dodatkowe zabezpieczenia lub zasady dostępu, itp. Przykładowo, system klasyfikacji kontroli dostępu uwzględnia stopień zabezpieczenia w oparciu o dwa podstawowe elementy: klasę identyfikacji oraz klasyfikację dostępu. Dla każdego punktu kontrolnego dostępu wyróżniono 5 klas identyfikacji i weryfikacji [1].

Istotnym problemem jest ochrona zasobów komputera, która powinna być wspierana przez system zarządzania bezpieczeństwem informacji ISSM (ang. *Information Security System Management*) zaprojektowany, na przykład zgodnie z normą ISO/IEC 27001:2005. ISSM powinien być starannie zaprojektowany, aby zabezpieczać zasoby informacji i infrastruktury w nawiązaniu do wyników oceny ryzyka. ISSM powinien wspierać również zarządzanie integralnością programowalnych systemów sterowania i zabezpieczeń procesów technologicznych oraz systemów informatycznych w odpowiednich sieciach [2, 8].

4. Podsumowanie

Przemysł staje przed potrzebą oceny czy aktualne środki zaradcze uwzględniają w sposób efektywny nowe zagrożenia i zapewniają adekwatną ochronę pracowników, społeczeństwa i środowiska. Podatność na utratę integralności (ang. *security*) obiektów przemysłowych podwyższonego ryzyka musi być współmierna do zagrożenia i prawdopodobieństwa scenariuszy krytycznych. W niektórych obiektach przemysłowych, jak rafinerie czy obiekty chemiczne, skala zagrożeń jest relatywnie wysoka. W takich obiektach zarządzanie podatnością na utratę integralności jest zagadnieniem kluczowym.

Metody oceny ryzyka stosowane w zarządzaniu bezpieczeństwem nie dają się w pełni zastosować do celów oceny podatności na utratę integralności (ang. *security*). Systemy analizy podatności na utratę integralności i oceny ryzyka wykorzystywane w zarządzaniu bezpieczeństwem oparte są głównie na opiniach ekspertów i informacji jakościowej. Z uwagi na znaczenie zagadnienia w praktyce przemysłowej i infrastrukturach krytycznych, powinny być podjęte dalsze badania, które umożliwią opracowanie zintegrowanej metodyki i kryteriów oceny bezpieczeństwa i ochrony. Metodyka oparta na wiedzy integrująca analizy LOPA (*ang. layer of protection analysis*) i ROPA (*ang. rings of protection analysis*) jest obecnie opracowywana wraz z odpowiednimi metodami i narzędziami przeznaczonymi do wspomagania zintegrowanego zarządzania ochroną i bezpieczeństwem, bazując na ocenach odpowiednich ryzyk.

Mgr inż. **Aleksandra Bobcow**, absolwentka Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej ze specjalnością Automatyka (2006). Słuchaczka Studium Doktoranckiego na tym wydziale od 2006 roku.
Specjalizacja: zintegrowane systemy bezpieczeństwa, kontrola dostępu (biometryki), systemy alarmowe, CCTV.

Prof. **Kazimierz Kosmowski,** tytuł doktora uzyskał w 1981, zaś habilitację w 2003 roku w Politechnice Gdańskiej. Od 2006 kierownik Katedry Automatyki na Wydziale Elektrotechniki i Automatyki. Od 2007 wiceprzewodniczący Polskiego Towarzystwa Bezpieczeństwa i Niezawodności (PTBN).
Specjalizacja: niezawodność i bezpieczeństwo systemów technicznych, niezawodność człowieka, bezpieczeństwo funkcjonalne systemów sterowania.