Marek MŁYŃCZAK, Tomasz NOWAKOWSKI
Politechnika Wrocławska, Wrocław
David VALIŠ
University of Defence, Brno, Czech Republic

JAK ZARZĄDZAĆ RYZYKIEM? PODEJŚCIE NORMATYWNE

Słowa kluczowe

Zarządzanie ryzykiem, metody analizy ryzyka, normalizacja, programy komputerowe.

Streszczenie

Ryzyko jest miarą zagrożenia, które z natury rzeczy jest zwykle eliminowane lub ograniczane środkami bezpieczeństwa. Potencjalne zdarzenia niepożądane zarówno cywilizacyjne, jak i naturalne, rozwijające się z zagrożeń są zdarzeniami stosunkowo rzadkimi, jednak często o dużym zasięgu i ciężkich skutkach. Rozpoznanie zagrożeń, ich eliminacja lub ograniczanie skutków są działaniami leżącymi w obszarze zarządzania zorientowanego na obniżanie kosztów zewnętrznych i całkowitych kosztów eksploatacji systemów technicznych. Podjęto próbę przedstawienia ugruntowanych i efektywnych metod analitycznych stosowanych w zarządzaniu ryzykiem.

Wprowadzenie

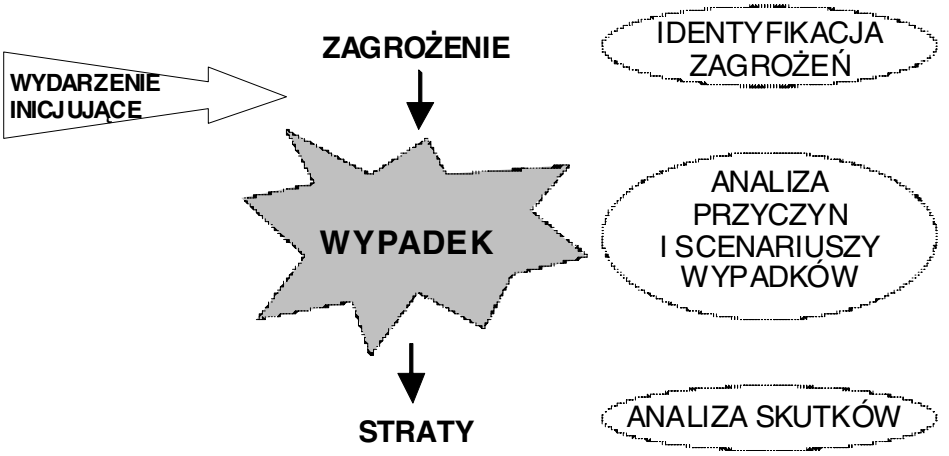
Norma *Risk Management- Risk Assessment Techniques* [4] przywołuje metodykę zarządzania ryzykiem oraz definiuje narzędzia zalecane w procedurze oceny ryzyka. W języku angielskim termin „RISK" ma dwojakie znaczenie, nieco dezorientujące w dyskusji dotyczącej obszaru bezpieczeństwa. Słownik

WNT, (2007) podaje tłumaczenie angielskiego *risk* zarówno jako „ryzyko", jak i „zagrożenie". Podobnie termin „zagrożenie" znajduje jako odpowiedniki angielski termin *hazard* i *risk*. Konieczne jest więc sprecyzowanie i rozdzielenie tych pojęć w odniesieniu do technik zarządzania ryzykiem. Literaturowy przegląd pojęć pokazuje szereg zbieżnych określeń i bliskich rozumieniu normy 60300-3-9 [8]. Bezpieczeństwo jest takim sterowaniem zagrożeniami, aby osiągnąć akceptowalny poziom ryzyka [14]. Bezpieczeństwo jest względnym sposobem oddzielenia od zagrożenia, jest antonimem niebezpieczeństwa [2]. Bezpieczeństwo jest miarą względnej wolności od zagrożeń. Bezpieczeństwo jest stopniem wolności od zagrożeń w każdym środowisku [1]. Bezpieczeństwo jest osądem akceptowalności ryzyka. Rzecz jest bezpieczna, jeżeli ryzyko oceniane jest jako akceptowalne [10].

Norma 60300-3-9 [8] definiuje podstawowe pojęcia używane w nauce o bezpieczeństwie:

- zagrożenie to źródło potencjalnej szkody lub okoliczności potencjalnie szkodliwe,
- ryzyko to kombinacja częstości lub prawdopodobieństwa wystąpienia określonego zdarzenia niebezpiecznego i konsekwencji związanych z tym zdarzeniem.

Powinno się więc łączyć *risk* z pojęciem „ryzyko", a *hazard* z „zagrożeniem". Jest to logicznie powiązane z łańcuchem przyczynowo-skutkowym powstawania wypadków, w którym pierwotnym ogniwem wypadku jest zagrożenie (potencjalne źródło szkody). Wypadek inicjowany jest koincydencją w czasie i miejscu zagrożeń mogących potencjalnie rozwinąć się w wypadek (rys. 1) [12].



Rys. 1. Łańcuch przyczynowo-skutkowy powstawania strat

1. Wielkie katastrofy przemysłowe

W powojennej historii przemysłu odnotowano wiele katastrof o znacznym zasięgu i tragicznych skutkach zarówno dla ludzi, jak i środowiska naturalnego. Wydarzenia te stały się zaczynem nauki o bezpieczeństwie. Spowodowały zainteresowanie tą sferą działania i zaowocowały opracowaniem istotnych regulacji prawnych. W tabeli 1 zestawiono przykłady największych katastrof cywilizacyjnych z krótkim opisem przyczyn i skutków.

Do innych poważnych katastrof cywilizacyjnych należy zaliczyć katastrofy morskie mające znaczące skutki ekologiczne wywołane wyciekiem ropy ze statków: Zatoka Perska (1991), wybrzeże Bretanii (1999), wybrzeże Galicji w Hiszpanii (2002), Zatoka Meksykańska BP (2010).

Katastrofa we Flixborough stała się impulsem do wprowadzenia różnych działań głównie natury prawnej, organizacyjnej i naukowo-technicznej zwracającej uwagę na problem zagrożenia pochodzącego z działalności przemysłowej. Natomiast po katastrofie w Seveso opracowano pierwszą Dyrektywę Unii Europejskiej dotyczącą bezpieczeństwa przemysłowego, zwaną Dyrektywą Seveso (Dyrektywa EWG 82/501/EEC z 24.06.1982 r.). Dyrektywa ta wprowadza ujednolicone działania w krajach Wspólnoty w zakresie zapobiegania poważnym awariom oraz nakłada obowiązek dbałości o bezpieczeństwo na przedsiębiorstwa i administrację publiczną. Zalecono, aby profilaktyka bezpieczeństwa i proaktywana polityka zarządzania bezpieczeństwem stały się częścią spójnego systemu bezpiecznego działania człowieka w otoczeniu technicznym i środowisku naturalnym. Dotyczy to analizy takich aspektów jak: lokalizacja przedsięwzięć przemysłowych, zasięg i wielkość ewentualnych skutków, czas ekspozycji na zagrożenia, wpływ zagrożeń naturalnych na przebieg procesów.

Podstawowymi źródłami informacji o już zaistniałych awariach przemysłowych są bazy danych, np. FACTS – Database for Industrial Safety, MHIDAS – Major Hazard Incident Data Service, The Accident Database.

2. Metodologia zarządzana ryzykiem

Zarządzanie ryzykiem jest kompleksowym działaniem wpisanym obecnie w program zarządzania wielu przedsiębiorstw. Charakterystyka tego procesu jest przedmiotem normy ISO 31000:2009, gdzie określono zależność między: założeniami, strukturą i procesem zarządzania ryzykiem.

Zakłada się, że zarządzanie ryzykiem jest integralną częścią działania przedsięwzięcia włączoną w procesy decyzyjne, prowadzone jest w sposób ciągły i oparty na dostępnej informacji z uwzględnieniem jej niepewności. Zarządzanie dotyczy, oprócz procesów przemysłowych, także człowieka. Jest procesem dynamicznym, transparentnym i w stały sposób usprawniającym zarówno działanie, jak i metodykę zarządzania bezpieczeństwem.

Tabela 1. Wielkie katastrofy przemysłowe

Miejsce	Data	Proces	Przyczyna wypadku	Zdarzenie wypadkowe	Skutki
Flixborough, Wielka Brytania	1.06.1974	reakcja utleniania cykloheksanu	pęknięcie przewodu odciążającego w ciągu reaktorów	wybuch przestrzenny, pożar instalacji	28 ofiar śmiertelnych, 36 rannych, zniszczenie 1821 domów, 167 warsztatów i fabryk (gaszenie pożarów 10 dni)
Seveso, Włochy	9.07.1976	reakcja wytwarzania trójchlorofenylu	utrata szczelności reaktora wskutek przegrzania i wybuchu cieplnego (uwolnienie 2 kg dioksyn)	uwolnienie toksycznego gazu	skażenie toksyczne; 700 rannych, 5000 ewakuowanych, 1500 ha obszaru silnie skażonych, zniszczenia flory i fauny na wielkich obszarach
Bohpal, Indie	2.12.1984	magazynowanie metyloizocyjanianu	niekontrolowana reakcja chemiczna	uwolnienie toksycznych oparów przez zawór bezpieczeństwa	ponad 10 000 ofiar śmiertelnych, 30 000 trwałe kalectwo, 20 000 częściowe kalectwo, 50000 drobne urazy, zniszczenia flory i fauny na wielkich obszarach odszkodowania: 470 mln $ (1987 r.)
Platforma Piper Alpha, Wlka Brytania	6.07.1988	platforma wiertnicza	błąd człowieka, włączenie kompresora spowodowało wybuch gazu	wybuch gazu, pożar	167 ofiar śmiertelnych, zniszczenie platformy, straty 3,7 mld $
Feyzin, Francja	4.01.1966	magazynowanie propanu	wyciek propanu podczas odwadniania zbiornika i pobierania próbek	uwolnienie palnego gazu, powstanie rozlewiska i chmury par, pożar pod zbiornikiem, wybuch BLEVE, efekt domina	18 ofiar śmiertelnych, 81 rannych (w tym 40 ciężko), zniszczenia instalacji, straty ok. 68,8 mln $ (1990 r.)
Mexico City, Meksyk	19.11.1984	magazynowanie paliw LPG	spadek ciśnienia w rurociągu, uszkodzenie rury 200 mm	pożar bazy paliw wybuchy BLEVE	500 ofiar śmiertelnych
Enschede, Holandia	13.05.2000	produkcja materiałów pirotechnicznych	naruszenie przepisów bezpieczeństwa. Składowanie silnie wybuchowych materiałów w zwykłych kontenerach na zewnątrz bunkrów.	wybuch w magazynach materiałów pirotechnicznych	23 ofiary śmiertelne, całkowite zniszczenie 500 budynków, 1000 poważnie uszkodzonych
Rafineria, Czechowice Dziedzice	26.06.1971	rafineria ropy naftowej	uderzenie pioruna, brak zabezpieczeń i systemów p.poż., błędy w akcji gaśniczej	pożar w rafinerii ropy naftowej	37 ofiar śmiertelnych, 105 ciężko poparzonych, zniszczone 22 samochody pożarnicze
Zakłady Chemiczne „ROKITA", Brzeg Dolny	23.12.1976	postój wagonów z materiałem niebezpiecznym	rozszczelnienie cysterny na bocznicy zakładowej	wybuch cysterny z ładunkiem dwóch różnych gazów skroplonych, tworzących w sprzyjającej temperaturze mieszankę wybuchową	zniszczenie budynków i infrastruktury
Czarnobyl, Związek Radziecki	26.04.1986	elektrownia termojądrowa (reaktor bloku IV)	błędy operatora i wyłączenie systemów awaryjnych w trakcie eksperymentu mającego zwiększyć bezpieczeństwo pracy reaktora.	stukrotny wzrost mocy reaktora, wzrost temp. rdzenia do ok. 2000^{o}C, dwa kolejne wybuchy (rozsadzenie układu chłodzenia przez parę wodną i wybuch mieszaniny piorunującej pochodzącej z rozkładu wody na tlen i wodór pod wpływem kontaktu z rozżarzonym grafitem i cyrkonem).	wybuchy rozpoczęły 10-dniowy pożar, w trakcie którego rdzeń reaktora stopił się, a do środowiska przedostała się znacząca ilość substancji promieniotwórczych.

Powyższe założenia wpisują się w cykl zarządzania obejmujący: zaprojektowanie struktury zarządzania ryzykiem, jego implementację w proces działania, przeprowadzanie okresowego lub ciągłego monitorowania i przeglądów oraz ciągłego usprawniania struktury zarządzania. Wnioski z tych przeglądów stają się wytycznymi poprawy zarządzania ryzykiem.

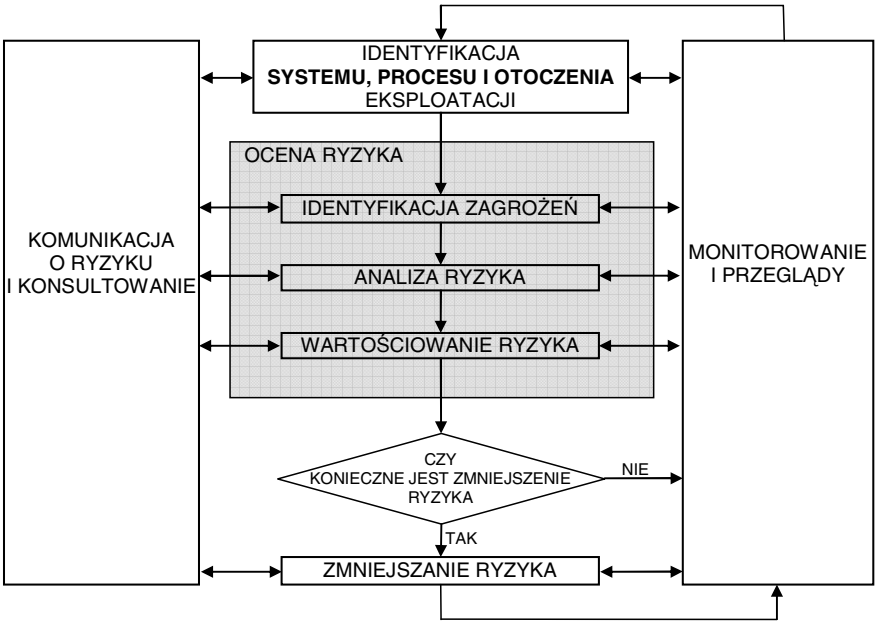
Wykonawczy algorytm procesu zarządzania bezpieczeństwem będący ogniwem powyższego cyklu przedstawiono na rys. 2 [3, 4, 6, 7].

Proces ten obejmuje 4 etapy ujęte w pętlę, która zgodnie z zaleceniami powinna być wykonywana w sposób ciągły. Trzonem procesu jest ocena ryzyka wymagająca wyznaczenia wartości ryzyka i porównania jej z poziomem akceptowalności czy tolerancji.

Analiza i ocena ryzyka wymaga szczegółowych analiz systemu eksploatacji, procesu i otoczenia w celu określenia:

- co może zdarzyć się nieprzewidywalnego, niezgodnego z oczekiwaniami (identyfikacja zagrożeń),
- jaka jest częstość takich zdarzeń,
- jakie potencjalne skutki mogą towarzyszyć takim zdarzeniom (ocena strat dla człowieka, środowiska naturalnego i systemu technicznego).

W algorytmie tym kluczowymi i najtrudniejszymi elementami jest identyfikacja zagrożeń i określenie ich możliwości wystąpienia oraz potencjalnych skutków.



Rys. 2. Algorytm procesu zarządzania ryzykiem

Opr. własne na podst. ISO/IEC 31010:2009 Ed. 1.0: Risk Management- Risk Assessment Techniques.

Analiza i ocena ryzyka opiera się na wiedzy historycznej i obserwacjach podobnych systemów, wiedzy eksperckiej, doświadczeniu analityków oraz dedykowanych metodach opracowanych w toku rozwoju cywilizacji technicznej. Troska o bezpieczeństwo staje się coraz bardziej istotnym elementem działania i zarządzania. W miarę wzrostu świadomości i stawiania wysokich wymagań w odniesieniu do bezpieczeństwa rozwijana jest także wiedza i metodologia działania w tym zakresie. Opracowuje się nowe techniki identyfikacji zagrożeń, stosuje ilościowe podejście do zagrożeń, poprzez kwantyfikację ryzyka oraz poszukiwanie wzorców do akceptacji ryzyka. Wprowadza się do zarządzania techniki stosowane w inżynierii niezawodności oraz niezawodności człowieka, scenariusze i planowanie działań awaryjnych, a także w sytuacjach kryzysowych, badanie przyczyn i skutków wypadków, awarii i katastrof [8, 9].

3. Techniki identyfikacji zagrożeń oraz analizy i oceny ryzyka

W normie *IEC 31010 Ed. 1.0: Risk Management – Risk Assessment Techniques* [4] wspomagającej normę *ISO 31000:2009* [3] zebrano i scharakteryzowano najczęściej stosowane techniki identyfikacji i analizy zagrożeń. W załączniku A zestawiono 31 technik sklasyfikowanych ze względu na ich przydatność w odniesieniu do problemu: identyfikacji zagrożenia, wartościowania częstości i skutków, efektywności wykorzystania jako narzędzia kontrolnego, możliwości wyznaczania ryzyka i jego oceny. Podano również stopień przydatności w każdej z kategorii w skali: mała przydatność, średnia i duża. Załącznik B charakteryzuje każdą z 31 technik podając jej: opis, warunki użycia, wymagania, sposób zastosowania, oczekiwane wyniki oraz wady i zalety.

Techniki można przypisać do różnych zakresów i etapów zarządzania ryzykiem następująco (zgodnie z rys. 2):

- **Identyfikacja zagrożeń:**
  - Check-list,
  - Root cause analysis,
  - Brainstorming,
  - Structured or semi-structured interviews,
  - Delphi,
  - Primary hazard analysis,
  - Hazard and operability studies (HAZOP),
  - Hazard Analysis and Critical Control Points (HACCP),
  - Structure « What if? » (SWIFT),
  - Risk indices,
- **Analiza ryzyka:**
  - Scenario analysis,
  - Failure mode effect analysis,
  - Fault tree analysis,

- Event tree analysis,
- Cause and consequence analysis,
- Cause-and-effect analysis,
- Markov analysis,
- Monte Carlo simulation,
- Human reliability analysis,
- Bayesian statistics and Bayes Nets,
- Sneak circuit analysis,
- Layer protection analysis (LOPA),
- Decision tree,

- **Ocena ryzyka:**
  - Environmental risk assessment,
  - Business impact analysis,
- **Analiza i ocena ryzyka:**
  - Multi-criteria decision analysis (MCDA,
  - Bow tie analysis,
  - FN curves,
  - Consequence/probability matrix,
  - Cost/benefit analysis,
- **Zarządzanie ryzykiem:**
  - Reliability centered maintenance.

4. Komputerowe programy wspomagające analizę i ocenę ryzyka

Oprogramowanie wspomagające analizę i ocenę ryzyka oparte jest najczęściej na przedstawionych powyżej metodach, które w dużej mierze są metodami analitycznymi. Poniżej scharakteryzowano najważniejsze z programów używanych na świecie do zaawansowanych zastosowań w obszarze bezpieczeństwa.

RiskSpectrum® PSA jest pakietem komputerowym wykorzystywanym w większości elektrowni nuklearnych oferującym metodologię opartą na drzewie błędów i wydarzeń. RiskSpectrum PSA komunikuje się z użytkownikiem poprzez intuicyjny interface do modelowania szerokiego zakresu zdarzeń z wykorzystaniem narzędzi od prostych drzew z bramkami AND i OR, aż po zaawansowane drzewa integrujące FTA i ETA i pozwalające modelować rozwój wydarzeń od zdarzeń bazowych po skutki (CCF) z uwzględnieniem wpływu otoczenia. Zintegrowana analiza RiskSpectrum Analysis Tool jest specjalistycznym pakietem dostosowanym do modelowania istotnych zadań z zakresu PSA (Probabilistic Safety Analysis) oferującym narzędzia oparte na: MCS (Minimal Cut Set), BDD (Block Dependability Diagram), Analizie wrażliwości, istotności i zależności czasowej. RiskSpectrum PSA zawiera także edytor MCS i zaawansowane funkcje Post Processing. Najnowsza wersja RiskSpectrum PSA version 1.1.3 została wydana w czerwcu 2010 roku.

RiskSpectrum® RiskWatcher jest programem monitorującym ryzyko w celu właściwego zarządzania nim. Za pomocą tego programu analizuje się poziom ryzyka historycznego, bieżącego i planowanego. Program śledzi i podaje w dowolnej chwili stan systemów, urządzeń i procesów. RiskSpectrum RiskWatcher bazuje i jest zaprojektowany w zgodności z FTA i ETA znanymi jako PRA (Probabilistic Risk Assessment), PSA (Probabilistic Safety Assessment) oraz QRA (Quantitative Risk Assessment). Możliwości oferowane przez RiskSpectrum RiskWatcher to:

- zarządzanie bezpieczeństwem przedsięwzięcia,
- wspieranie zaprogramowanych działań,
- osiąganie większej elastyczności w działaniach operacyjnych,
- uzasadnienia wykonywania obsług podczas pracy,
- dostarczenie informacji o istotności ryzyka dotyczącego elementów będących w obsłudze jak również poza systemem obsługiwania,
- dostarczanie danych do oceny zarówno ilościowej, jak i jakościowej.

Typowymi, oczekiwanymi wynikami dla wspomagania zarządzania ryzykiem są dla elektrowni nuklearnych wykresy: Core Damage Frequency (CDF – częstotliwość stopienia rdzenia) i Large Early Release Frequency (LERF – częstotliwość znacznego wycieku) w funkcji czasu. Ilościowe wyniki wskazują poziom gotowości systemów bezpieczeństwa w kolorach zielonym, żółtym, pomarańczowym i czerwonym. RiskSpectrum RiskWatcher obejmuje zależne od czasu dane o niezawodności umożliwiając badanie wpływu okresów testowania systemów na ryzyko. Zbiory minimalnych przekrojów niezdatności są każdorazowo odnawiane po kolejnych przeliczeniach, w miarę napływu nowych danych. Wydaje się, że jest to najlepszy, dynamiczny sposób zapewnienia poprawności działania i wpływu zmiany stanu systemu na wyniki końcowe i jakość zarządzania ryzykiem. Ostatnia aktualizacja RiskSpectrum RiskWatcher version 1.22 była datowana w grudniu 2008 roku.

ITEM Quantitative Risk Assessment System (iQRAS) wspiera identyfikację zagrożeń, wyszukiwanie głównych sprawców potencjalnych awarii i wspomaga zrozumienie działania systemu. Integracja zdarzeń bazowych z czasem, sekwencje zdarzeń, charakterystyki rozkładu prawdopodobieństwa uszkodzeń, rangowanie zagrożeń oraz analiza wrażliwości zapewnia użytkownikowi, w opinii autorów, efektywne, zintegrowane i wyjątkowe środowisko zarządzania bezpieczeństwem. ***iQRAS*** jest wydajnym i przyjaznym narzędziem w pełni integrującym środowisko opracowywania modeli do analizy ryzyka. Program pozwala na wykonanie PRA (Probabilistic Risk Assessment), opracowanie i ocenę scenariuszy rozwoju wypadków, szacowania numerycznego poziomu ryzyka oraz identyfikowanie głównych czynników zagrażających. Pomimo tego, że ***iQRAS*** został opracowany na potrzeby NACA, obecna wersja pozwala na szeroki zakres zastosowań obejmujących obiekty kosmiczne, wojskowe,

transportowe, jak również medyczne. Program może być pomocny dla inżynierów, analityków, inżynierów bezpieczeństwa poszukujących możliwości poprawy efektów ich pracy. Strona obliczeniowa ***iQRAS*** oferuje algorytmy będące wysoko efektywnymi i w przeciwieństwie do konwencjonalnych metod rozwiązywania nie są narażone na często występujące, istotne błędy przybliżeń. ***iQRAS*** jest nowym pakietem oferowanym przez ITEM dodanym do pakietu narzędzi poświęconych bezpieczeństwu i niezawodności. Ostatnia wersja programu jest finalną wersją przekształcającą oryginalny pakiet utworzony przez University of Maryland i NASA. Nowe środowisko zapewnia zestaw wyjątkowych narzędzi edytowania i raportowania współpracujących z flagowym oprogramowaniem **ITEM ToolKit** w zakresie niezawodności, gotowości, obsługiwalności i analizy ryzyka.

Software-Assistent SISTEMA *(Safety Integrity Software Tool for the Evaluation of Machine Applications)* jest prostą aplikacją opartą na normie EN ISO 13849-1 wspierającą inżynierów rozwoju i bezpieczeństwa w zakresie spełnienia wymagań tej normy. Narzędzie umożliwia modelowanie struktury systemów odpowiedzialnych za bezpieczeństwo i pozwala na wyznaczanie wartości niezawodności dla różnych poziomów szczegółowości systemu i jego obciążenia włącznie z docelowym poziomem wydajności. Najważniejsze parametry wpływające na ryzyko i niezbędne do określenia poziomu wymaganej wydajności są wprowadzane krok po kroku w oknach dialogowych programu. Każda zmiana wartości parametru jest natychmiast wyświetlana w interfejsie użytkownika modyfikując też powiązane parametry systemu. Użytkownik oszczędza czas, ponieważ raporty są tworzone automatycznie przez program. Końcowy wynik pracy może być wydrukowany w postaci zwięzłego raportu. SISTEMA jest oferowany w angielskiej wersji językowej i jest bezpłatnie udostępniany.

Podsumowanie

Metodologia zarządzania ryzykiem jest oparta na prostym cyklu działań: „identyfikuj, zmierz, oceń, podejmij decyzję – popraw lub działaj". W obecnym stanie normalizacji metodologia i działania wykonawcze są dobrze zdefiniowane i opisane. Analiza technik identyfikacji, analizy i oceny zagrożeń pokazuje ich różnorodność i niejednorodność pod względem struktury, szczegółowości analiz, a także występujące podobieństwo procedur dla różnych nazw. Programy komputerowe w znacznym stopniu ułatwiają zarządzanie ryzykiem w szczególności w rozległych systemach technicznych.

Podziękowanie

Przygotowanie niniejszego opracowania było znacząco wsparte finansowo przez projekt nr 1M06047 „The Centre for Production Quality and Dependability" Ministerstwa Edukacji Republiki Czeskiej oraz częściowo wsparte przez

projekt 101/08/P020 „Contribution to Risk Analysis of Technical Sets and Equipment" Czeskiej Fundacji Nauki.

Opracowanie wykonano też w ramach projektu badawczego Ministerstwa Nauki i Szkolnictwa Wyższego nr N509 293735.

Bibliografia

1. Gloss D.S., Wardle M.G.: Introduction to Safety Engineering. John Wiley & Sons, 1984.
2. Hammer W.: *Occupational Safety Management and Engineering*, Prentice-Hall, New York 1989.
3. ISO 31 000:2009 Ed. 1.0: Risk Management- Principles and guidelines on implementation.
4. ISO/IEC 31010:2009 Ed. 1.0: Risk Management- Risk Assessment Techniques.
5. ISO 13824:2009 Ed. 1.0- General principles on risk assessment of systems involving structures.
6. ISO/IEC Guide 73:2002 Ed. 1.0 Risk management – Vocabulary – Guidelines for use in standards.
7. ISO/IEC GUIDE 51:1999 Ed. 1.0 Safety aspects – Guidelines for their inclusion in standards.
8. IEC 60300-3-9 Dependability management - Part 3: Application guide – Section 9: Risk assessment of technological systems.
9. IEC 61508-(1-7)/:2008 Ed. 2.0 Functional Safety of Electrical/ /Electronic/Programmable Electronic Safety-Related Systems.
10. JCSS (Joint Committee on Structural Safety) - Principles, System Representation & Risk Criteria.
11. Lowrance W.W.: Of Acceptable Risk: Science and the Determination of Safety. William Kaufmann, 1976.
12. Młyńczak M.: Podstawy szacowania ryzyka w transporcie. Seria NAVIGAROR. Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław 1997.
13. Valis D., Koucky M.: Selected Overview of Risk Assessment Techniques. Materiały XXXVIII Szkoły Zimowej. Wydawnictwo Naukowe ITeE – PIB. Radom, 2010.
14. U.S. National Safety Council - http://www.nsc.org.

Recenzent:
Lech BUKOWSKI

How to manage risk? the normative approach

Key words
Risk management, risk analysis methods, normalisation, computer programmes.

Summary

Risk is the danger measurement that is usually eliminated or limited with the use of safety measures. Even though potentially undesirable events, both civilisational and natural ones, that are the results of dangers are quite rare, they do have quite a wide range and disastrous effects. The identification of dangers, their elimination or the reduction of their effects are of greatest importance to risk management, whose aim is to reduce the external costs and the total maintenance costs of technical systems. The presentation of tested and effective analytical methods applied in risk management has been attempted in this paper.