prof. dr inż. Tadeusz Missala
Przemysłowy Instytut Automatyki i Pomiarów PIAP, Warszawa

WYKORZYSTANIE METOD BEZPIECZEŃSTWA FUNKCJONALNEGO W OCENIE ZAGROŻEŃ W SIECIACH INFORMATYCZNYCH – PROPOZYCJA

W nawiązaniu do poprzedniej publikacji autora [1] zwrócono uwagę, że na Warsztatach CRITIS'2010 pojawiły się publikacje dotyczące analizy zagrożeń powstających w sieciach informatycznych sterujących infrastrukturą krytyczną i ilościowej oceny odporności na te zagrożenia. Ta tematyka ma wiele aspektów wspólnych z tematyką oceny zagrożeń i ryzyka stosowaną w bezpieczeństwie funkcjonalnym [3]. Zaproponowano zastosowanie tych metod w ocenie zagrożeń w sieciach informatycznych.

PROVIDING OF FUNCTIONAL SAFETY METHODS TO THREATS AND RESILIENCE ANALYSIS IN INFORMATION NETWORKS – PROPOSAL

Referring to the precedent publication of the author [1] the attention is direct to the fact, during Workshop CRITIS'2010 are occurred publications concerning threats analysis in the information networks controlling the critical infrastructure and quantitative assessment of the networks resilience. It is to note the many of aspects of these are common with the methods applied in the functional safety [3]. Use of functional safety methods to threats assessment in information networks is proposed.

1. WPROWADZENIE

Zabezpieczenie (security)[1] jest pewnością dostarczaną przez system, że każde niepoprawne wejście lub każdy nieuprawniony dostęp jest niemożliwy [10e]. Jest składową niezawodności systemu [2] i łącznie z innymi cechami niezawodności wchodzi w skład pojęcia bezpieczeństwa (safety) systemu [10g]. To upoważnia do spojrzenia na zagadnienie analizy i oceny zagrożeń i ryzyka w sieciach informatycznych z punktu widzenia doświadczeń zdobytych przez technikę automatyzacji przy realizacji sterowania i zabezpieczenia infrastruktury krytycznej, to jest przez pryzmat bezpieczeństwa funkcjonalnego.

W dotychczas prezentowanych pracach, m.in. [1, 6, 7, 8], główna uwaga była skierowana na opracowanie systemu zabezpieczającego transmisję danych, w szczególności na zabezpieczenie systemów lokalnych (obiektowych i przedsiębiorstwa) przed zagrożeniami pochodzącymi z sieci rozległych, głównie z Internetu. Dobre inżynierskie metody postępowania w przypadku zagrożeń bezpieczeństwa obiektów przemysłowych, a szczególnie infrastruktury krytycznej, wprowadzone do praktyki międzynarodowej serią norm IEC 61508 [11] (jako normy bezpieczeństwa funkcjonalnego) wskazują, że aby właściwie dobrać zabezpieczenia, należy zacząć od analizy zagrożeń i ryzyka. Takie podejście prezentują także normy międzynarodowe [19, 20, 21].

[1] W nawiasach zamieszczono angielskie nazwy terminów, w celu uzyskania jednoznaczności i uniknięcia pomylenia z terminami stosowanymi w zagadnieniach bezpieczeństwa w automatyzacji. W szczególności należy zaznaczyć, że w automatyce terminem „bezpieczeństwo" tłumaczy się termin „safety", stąd wprowadzenie terminu „zabezpieczenie".

Narzuca się więc zagadnienie doboru metod właściwych do oceny zagrożeń i ryzyka w sieciach komunikacyjnych. Ta tematyka znalazła się w obiektywie Warsztatów CRITIS'10, które odbyły się w Atenach w dniach 23–24 września 2010 r. [4, 5].

Ostatnio wykonany cyberatak na elektrownię atomową w Iranie wskazuje, że zagrożenie systemów infrastruktury krytycznej atakami terrorystycznymi lub wojskowymi jest rzeczą realną. Nakłada to konieczność dbałości o najwyższy poziom zabezpieczenia sieci obsługujących taką infrastrukturę.

2. POJĘCIA PODSTAWOWE

W technice sieci teleinformatycznych do scharakteryzowania właściwości sieci związanych z ich zabezpieczeniem stosuje się następujące terminy [17, 18]:

zagrożenie (threa t) – okoliczność lub zdarzenie, które może wpływać niekorzystnie na działania instalacji (włączając funkcje, wygląd lub opinię), majątek lub jednostki poprzez system informatyczny przez dostęp nieuprawniony, zniszczenie, ujawnienie, modyfikację danych, opóźnienie przesyłek i/lub odmowę usług.

prężność[2] (resilience) – cecha opisująca zdolność systemu do dostosowania się do znaczących zmian w jego środowisku przez wykonanie działań nadzwyczajnych w celu utrzymania akceptowanego działania systemu.

odporność (robustness) – cecha opisująca zdolność systemu do tolerowania znaczących zmian w jego środowisku i utrzymania akceptowalnego działania systemu w sposób niewymagający wykonania działań nadzwyczajnych.

protokół komunikacyjny zabezpieczony (secure communications protocol) – protokół komunikacyjny zapewniający odpowiednie zabezpieczenie poufności, uwierzytelnienia, nienaruszalności zawartości i taktowania przesyłek.

uwierzytelnienie (autentication) – proces ustalający pochodzenie informacji lub określający tożsamość jednostki.

autoryzacja (authorisation) – uprawnienia dostępu przyznane jednostce; przekazanie uprawnienia urzędowego do wykonywania funkcji lub czynności.

poufność (confidentiality) – właściwość, że informacje poufne nie zostaną ujawnione jednostkom nieuprawnionym.

podatność (vulnerability) – cecha opisująca wrażliwość systemu na znaczące zmiany w jego środowisku, prowadząca do utraty jego akceptowanego działania.

metryka (metric, also called „indicator") – wartość obliczona z zaobserwowanych cech miary.

UWAGA 1 – Gdy temperatura jest określona jako 38 °C, to 38 jest metryką, zaś stopnie Celsjusza są miarą.

UWAGA 2 – Dostępność połączenia określona jako 99,99 % (metryka) może być *obliczona* przez sumowanie dostępności indywidualnych (*cech zaobserwowanych)* rutera, linii transmisyjnej dostępu i sieci głównej.

[2] Termin polski – propozycja autora, do dyskusji.

3. METODOLOGIA ANALIZY ZAGROŻEŃ I RYZYKA

Celem analizy zagrożeń i ryzyka jest ocena stanu bezpieczeństwa, porównanie go ze stanem pożądanym i umożliwienie zmniejszenia ryzyka do stanu akceptowanego lub wyeliminowanie obiektów stwarzających takie zagrożenia, lub tak nieodpornych na zagrożenia umyślne, że ich eksploatacja jest bezsensowna.

Przeprowadzenie analizy zagrożeń i ryzyka wymaga wykonania kroków [3, 22]:

- określenie ryzyka akceptowanego,
- określenie granic obiektu (procesu/urządzenia) wraz j jego układem sterowania,
- określenie wszelkich interfejsów zapewniających komunikację z otoczeniem,
- dokładne zdefiniowanie warunków środowiskowych, w tym elektromagnetycznych, w jakich jest gwarantowane poprawne działanie obiektu i jego systemu sterowania,
- dokładne zdefiniowanie warunków środowiskowych, w tym elektromagnetycznych, jakie mogą wystąpić w czasie eksploatacji, a które mogą się nie mieścić w zakresie warunków gwarantowanych,
- zidentyfikowanie słabości (*vulnerabilities*) systemu,
- zidentyfikowanie wszelkich możliwych sytuacji zagrażających, jakie mogą zaistnieć z powodu: niewłaściwego działania obiektu, niewłaściwego działania układu sterowania, w tym ich awarii, zaistnienia nienormalnych warunków środowiskowych, w tym ekstremalnych zaburzeń atmosferycznych, niewłaściwego lub nieuważnego postępowania obsługi (operatorów, serwisantów) i ataków zewnętrznych,
- opracowanie scenariuszy rozwoju zagrożeń przez określenie źródła zagrożenia, dróg jego rozprzestrzeniania się, ujścia zagrożeń (tj. elementów, które będą narażone i mogą zostać uszkodzone lub wytrącone z normalnej pracy),
- oszacowanie konsekwencji, jakie mogą wystąpić,
- oszacowanie prawdopodobieństwa wystąpienia każdej z konsekwencji,
- ocena ryzyka obiektu łącznie z jego układem sterowania i porównanie z ryzykiem akceptowanym,
- określenie wymaganego stopnia zmniejszenia ryzyka, rodzaju środków zabezpieczających i ewentualnie ich nienaruszalności bezpieczeństwa,
- sporządzenie odpowiedniego raportu.

4. METODY ANALIZY ZAGROŻEŃ I RYZYKA PREZENTOWANE W CZASIE WARSZTATÓW CRITIS'2010

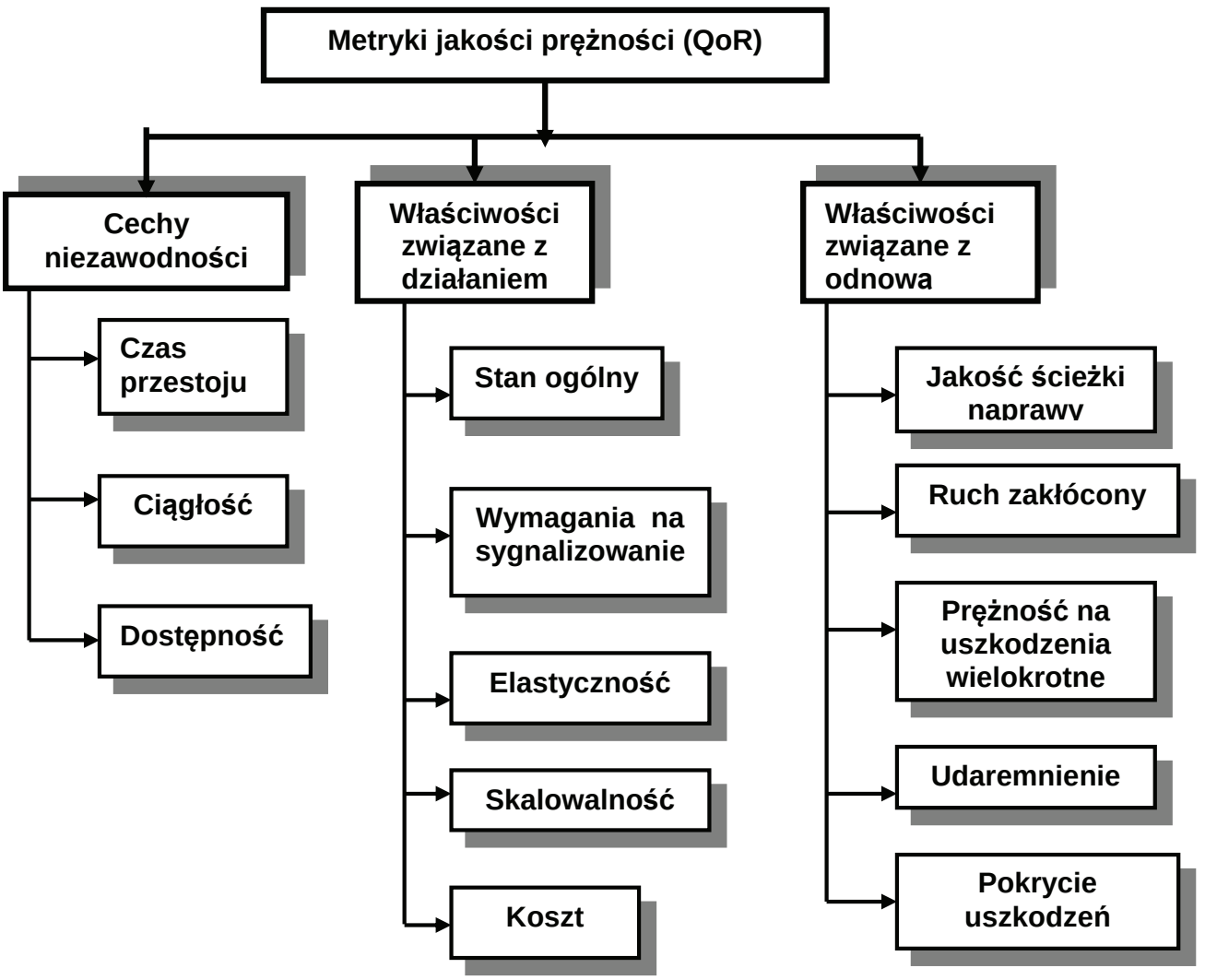
4.1. Propozycja metryk do oceny sieci

Chołda i Jajszczyk w prezentacji [5] przedstawili propozycję metryk do oceny prężności (resiliencse) sieci. Te koncepcję przedstawiono na rysunku 1. Znaczenie niektórych pojęć zaprezentowanych na rysunku Autorzy przybliżają następująco:

- Czas przestoju: średni czas przestoju MTD, średni czas do odnowy MTTR.
- Ciągłość: średni czas zdatności MUT, średni czas do uszkodzenia MTTF, średni czas działania między uszkodzeniami MTBF, intensywność uszkodzeń λ.
- Dostępność: funkcja $A = \dfrac{MUT}{MUT + MTD}$ lub $A = \dfrac{MTTF}{MTTF + MTTR}$

- Jakość ścieżki naprawy zależy od wielu parametrów, np. bitowej stopy błędów, ilorazu sygnału do szumu, utraty pakietu przesyłki, opóźnienia, fluktuacji sygnału, zdolności odbiorczej, zabezpieczenia – powstaje pytanie, jak to mierzyć.
- Ruch zakłócony: bezpośrednio (buforowanie i krótki czas do naprawy czynią go pomijalnym) i pośrednio (nie koniecznie wymagające skierowania ruchu na inną drogę, zależne od stanu sieci, długotrwałe).
- Prężność na uszkodzenia wielokrotne: wymaga większych zasobów, jest natomiast konieczna przy zastosowaniach krytycznych.
- Pokrycie uszkodzeń: naprawianie podsieci łączy/połączeń.

Autorzy wskazali na konieczność uwzględniania krótkoterminowego i długoterminowego zarządzania ryzykiem w relacjach z klientem, jak też wyposażanie go w lepsze środki naprawy uszkodzeń. Zadaniem przyszłościowym jest zwrócenie uwagi na metody określania (metryki) uzyskania stanu ustalonego dostępności. Szczególnie ważnym zadaniem jest wprowadzenie prężności wielopoziomowej. Zaprezentowano także ocenę czułości różnych aplikacji na metryki jakości prężności (QoR); zamieszczono ją w tablicy 1.



Rys.1. Składowe metryki jakości prężności

To podejście jest bardzo zbliżone do prezentowanego w PN-EN 61069 [10].

4.2. Propozycja ilościowej metody analizy ryzyka wynikającego z zagrożeń zamierzonych

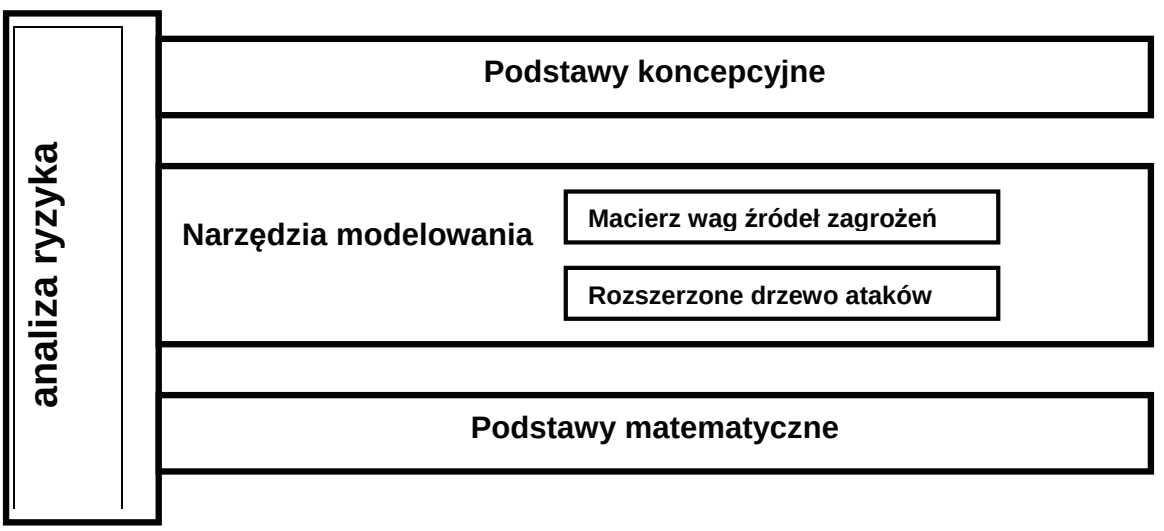
Vavoulas i Xenakis [4] wskazali na stosowane metody jakościowe CORAS, CRAMM, OCTAVE, FRAP. Metody te uznano jako niedostatecznie spełniające obecne wymagania, między innymi ze względu na nie dostarczanie podstaw do analizy kosztów i korzyści. Ponadto zagrożenia zamierzone nie są adekwatnie opisywane metodami jakościowymi, wymagają głębszej analizy, głównie z dwóch powodów:

- możliwości oddziaływania złożonego
- możliwości, jakimi dysponuje atakujący (doświadczenie, zasoby materialne, intelektualne itd.).

Tab. 1. Czułość aplikacji na metryki QoR

	Ciągłość	Dostępność	Czas naprawy	QoR rezerwy	Uszkodzenia wielokrotne
E-mail	Mała	Średnia	Mała	Mała	Mała
FTP	Średnia	Średnia	Duża	Mała	Mała
Głos/video przez IP	Duża	Średnia	Duża	Duża	Średnia
Sterowanie produkcją	Duża	Duża	Duża	Mała	Duża
Współdostęp do pliku	Mała	Średnia	Mała	Mała	Średnia
VoP2P (głos/video)	Mała	Mała	Średnia	Mała	Średnia
Sieć do sieci energetycznej	Duża	Średnia	Średnia	Średnia	Duża

Autorzy zaproponowali własne podejście ilościowe w wersji trzech odrębnych poziomów: podstawy koncepcyjne, narzędzia modelowania, podstawy matematyczne – rys. 2.

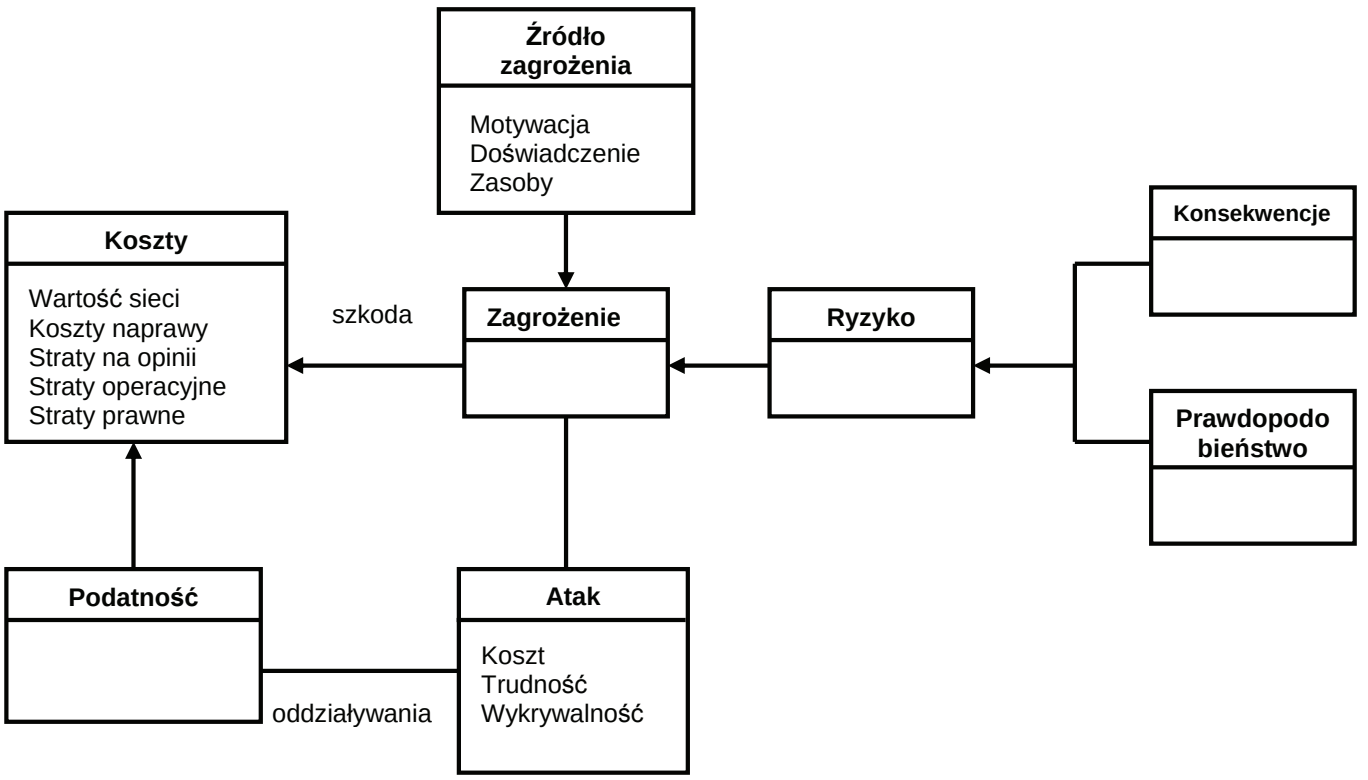


Rys. 2. Koncepcja metody analizy ryzyka

Aczkolwiek wskazano, że źródłami zagrożeń są środowisko, wypadki i ataki, to dalsza analiza koncentruje się na zagrożeniach zamierzonych, których źródłami są ataki. Proponowaną koncepcję metodologii przedstawiono na rysunku 3. Rozpatruje się szkody na majątku, ryzyko powstania szkody, podatność na szkodę, źródła zagrożenia i ataki.

Koncepcję macierzy zagrożenia – koszty przedstawiono w tablicy 2.

Podstawy matematyczne obejmują fundamentalne zależności wynikające z rachunku prawdopodobieństwa; niestety nie przywołano żadnej bazy danych.



Rys. 3. Schemat pojęć i atrybutów analizy ryzyka

Tab. 2. Macierz zagrożenia – koszty

	Źródło zagrożenia A	**Źródło zagrożenia B**	**Źródło zagrożenia C**
Koszt	W_{KA}	W_{KB}	W_{KC}
Trudność	W_{TA}	W_{TB}	W_{TC}
Wykrywalność	W_{WA}	W_{WB}	W_{WC}

4.3. Metoda CORAS [23]

Metoda ta zostanie zaprezentowana w skrócie jako reprezentant metod wymienionych w [4].

Badanie metodą CORAS jest przeprowadzane przez zespół zewnętrzny względem ocenianego obiektu. Do modelowania celów analizy stosuje się język UML (*Unified Modelling Language*), wyniki są prezentowane za pomocą specjalnych wykresów. Badanie jest wykonywane w siedmiu krokach:

- krok 1 – spotkanie wprowadzające: wskazanie przez przedstawicieli klienta całkowitych celów analizy, obiektów do przeanalizowania oraz przekazanie informacji o przedmiocie analizy;
- krok 2 – spotkania oddzielne z poszczególnymi grupami przedstawicieli klienta, przedstawienie przez analistów rozumienia sprawy i bardzo zgrubnych, ogólnych wyników analizy, a ponadto pierwsze zidentyfikowanie zagrożeń, słabości, scenariuszy rozwoju zagrożeń i zdarzeń niepożądanych;
- krok 3 – dokładniejsze opisanie obiektów do przeanalizowania oraz założeń i wniosków wstępnych; zakończenie kroku następuje po zaakceptowaniu dotychczasowych wyników przez klienta;
- krok 4 – ten krok jest organizowany jako warsztaty projektowane przez osoby zorientowane w obiekcie analizy, celem jest zidentyfikowanie jak największej liczby potencjalnych zdarzeń niepożądanych, a także zagrożeń, słabości i scenariuszy rozwoju zagrożeń;
- krok 5 – ten krok też jest organizowany jako warsztaty, których celem jest estymacja konsekwencji i prawdopodobieństwa wystąpienia wcześniej zidentyfikowanych zdarzeń niepożądanych;
- krok 6 – w tym kroku zostaje przedstawiony klientowi pierwszy obraz ryzyka całkowitego, który z reguły wymaga jeszcze poprawek i doprecyzowania;
- krok 7 – jest przeznaczony na identyfikację zabezpieczenia oraz wskazanie kosztów względem korzyści z nich; wskazane jest też zorganizowanie go jako warsztatów.

5. PRZ EGLĄD PROPONOWANYCH METOD Z TECHNIKI BEZPI ECZEŃSTWA FUNKCJONALNEGO

5.1. Ustalenie ryzyka akceptowanego

Podstawową wadą przedstawionych powyżej propozycji jest niewyeksponowanie etapu ustalenia ryzyka akceptowanego. Bez tego nie można określić dostateczności zabezpieczeń istniejących i dalszych, potrzebnych.

Vavoulas i Xenakis [4] wymieniają grupy kosztów, jakie może ponieść korporacja w wyniku awarii sieci informatycznej (patrz rys. 3) . Do tych grup należy dodać: wypadki przy pracy i w wyniku awarii sieci (urazy, inwalidztwa, zgony) oraz straty w środowisku, gdy awaria infrastruktury informatycznej spowoduje awarię w przedsiębiorstwie stwarzającym zagrożenie dla środowiska lub w sieci energetycznej.

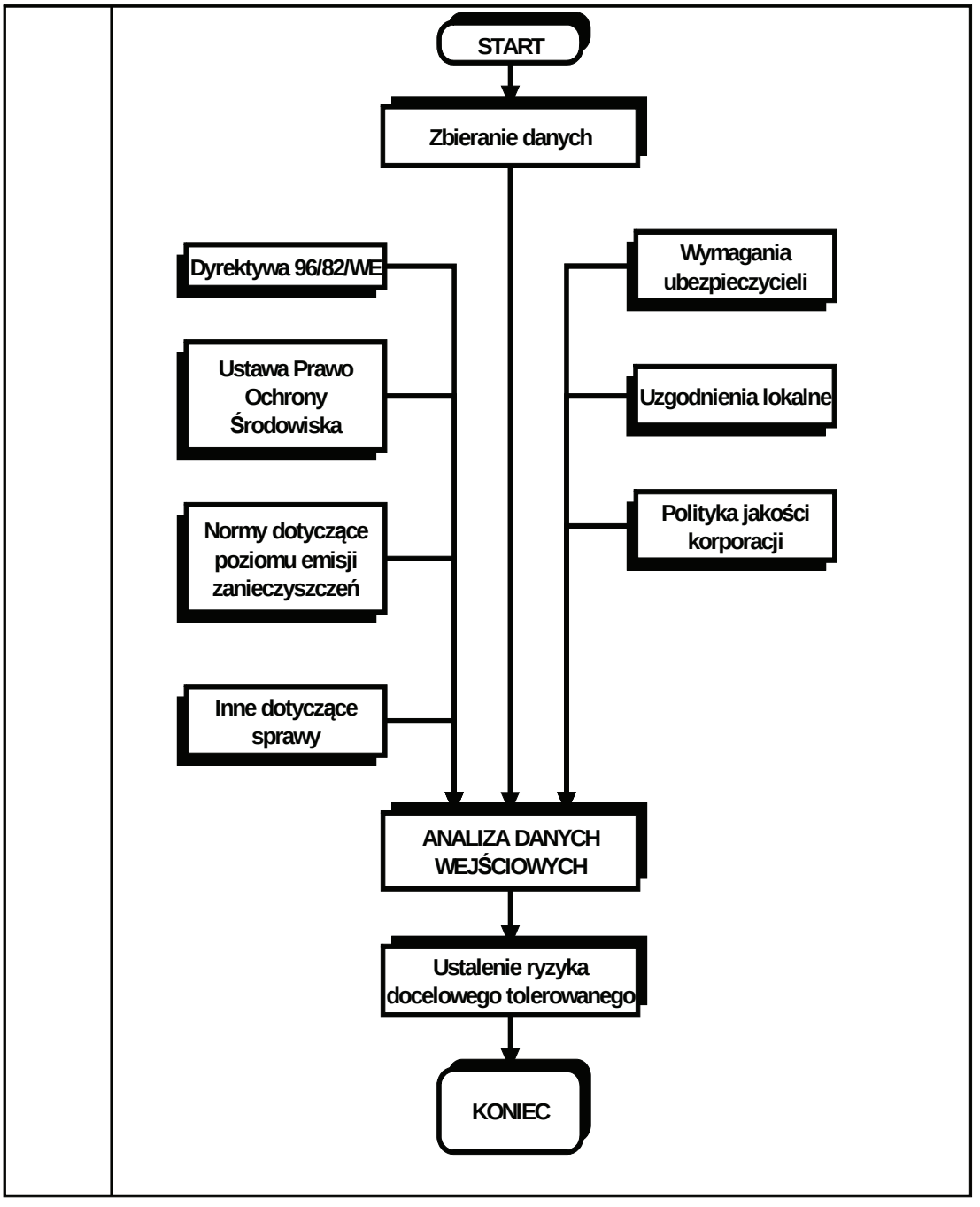
Ryzyko akceptowane to jest ten poziom ryzyka, który może przyjąć korporacja lub kraj w przypadku, np. sieci energetycznej elektrycznej, gazociągów, zaopatrzenia w wodę.

Poziom ten ustala się między innymi na podstawie [3, 11e, 12c]:

- wytycznych odpowiedniej jednostki określającej przepisy bezpieczeństwa,
- dyskusji i uzgodnień z różnymi stronami zaangażowanymi w konkretne zastosowanie,
- norm i przewodników przemysłowych, telekomunikacyjnych i innych odpowiednich,
- międzynarodowych dyskusji i uzgodnień; w tym rozmaitych wytycznych i rekomendacji wydawanych przez organizacje międzynarodowe i krajowe,
- wyników prac badawczych prowadzonych ostatnio w wielu konsorcjach międzynarodowych i w ramach programów rządowych ,
- norm krajowych i międzynarodowych, dyrektyw UE,

- najlepszych niezależnych porad przemysłowych, eksperckich i naukowych ze strony instytucji doradczych,
- wymagań prawnych, tak ogólnych jak i dotyczących bezpośrednio konkretnego zastosowania.

Przykładowy diagram ustalania ryzyka tolerowanego przedstawiono na rys. 4 [25].



Rys. 4. Ustalenie ryzyka tolerowanego – przykład

5.2. Ogólna zasada zmniejszania ryzyka [3, 11a, 12a]

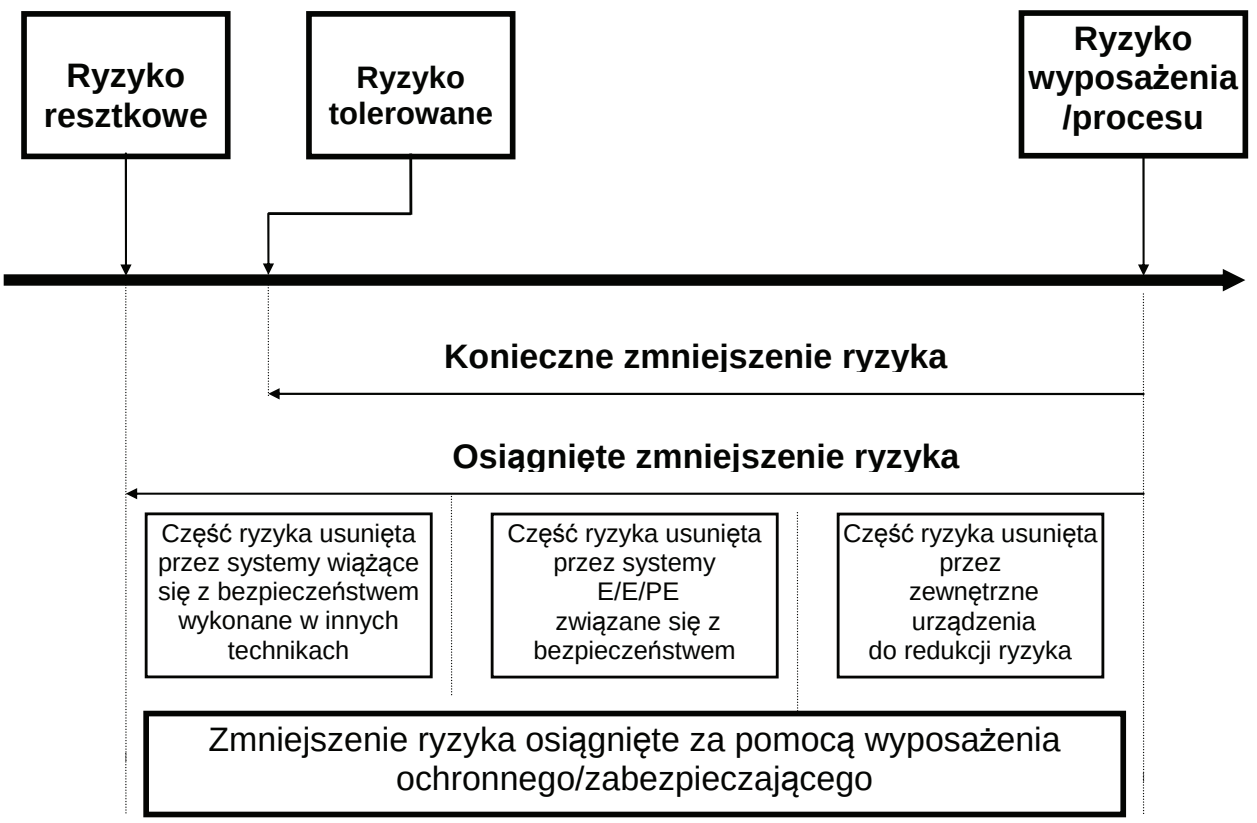
Na rys. 5 przedstawiono ogólny schemat zmniejszania ryzyka, który zakłada, że:

- występuje urządzenie sterowane i jego system sterowania;
- są wprowadzone powiązane czynniki ludzkie;
- na urządzenia ochronne/zabezpieczające składają się:
  - ⇒ zewnętrzne urządzenia do zmniejszania ryzyka;
  - ⇒ elektryczne i/lub elektroniczne i/lub elektroniczne programowalne systemy związane z bezpieczeństwem (E/E/PE), w tym przyrządowe systemy bezpieczeństwa (SIS);
  - ⇒ urządzenia związane z bezpieczeństwem wykonane w innych technikach.

Schemat przedstawiony na rys. 5 powinien być modyfikowany w konkretnych przypadkach tak, aby odzwierciedlał rzeczywistą sytuację. Odpowiednia modyfikacja umożliwi dostosowanie go do zagadnień bezpieczeństwa i zabezpieczenia sieci informatycznych.

Różne rodzaje ryzyka wskazane na schemacie mają następujące znaczenie:

- *ryzyko urządzenia/procesu* – ryzyko, w odniesieniu do określonego zdarzenia zagrażającego, istniejące w urządzeniu/procesie, systemie sterowania urządzeniem/procesem i powiązanymi z nim czynnikami ludzkimi, przy czym nie jest brane pod uwagę żadne wyposażenie ochronne/zabezpieczające
- *ryzyko tolerowane* – ryzyko, które jest akceptowane w określonym kontekście na bazie bieżących wskaźników przyjętych w społeczeństwie
- *ryzyko szczątkowe* – w rozumieniu IEC 61508-5 [11e] jest to ryzyko, w odniesieniu do określonego zdarzenia zagrażającego, pozostające w wyposażeniu/procesie, systemie sterowania urządzeniem/procesem i powiązanymi z nim czynnikami ludzkimi, lecz po wprowadzeniu kompletnego wyposażenia ochronnego/zabezpieczającego.



Rys. 5. Zasada zmniejszania ryzyka [3]

Wskazane wyżej *ryzyko urządzenia/procesu*, w przypadku sieci informatycznej będzie odpowiadało ryzyku uszkodzenia sieci niezabezpieczonej ani sprzętowo, ani programowo przed uszkodzeniami własnymi i działaniem intruzów.

5.3. Identyfikacja potencjalnych zagrożeń

Do identyfikacji potencjalnych zagrożeń wynikających z działania czynników zewnętrznych jak też z niedoskonałości działania systemu w technice bezpieczeństwa funkcjonalnego stosuje się studium HAZOP (Badanie zagrożeń i zdolności do działania) [3, 13]. Jest ono zbliżone do metody CORAS [23] oraz do metod ontologicznych [8], jednak ma pewne ważne zalety.

Istotnymi cechami tego studium HAZOP jest praca zespołowa wykonywana przez zespół interdyscyplinarny złożony w zasadzie z pracowników korporacji. Zasady HAZOP są następujące:

- Badanie prowadzi się przez systematyczne stosowanie ciągu słów wiodących w celu identyfikowania potencjalnych odchyleń od zamierzenia projektowego i używania tych odchyleń do stymulowania członków zespołu do rozpatrzenia, jak takie odchylenie mogłoby powstać i jakie mogłoby wywołać konsekwencje.
- Badanie jest prowadzone pod kierunkiem wyszkolonego i doświadczonego lidera, który musi zapewnić wyczerpującą analizę badanego systemu, stosując rozumowanie logiczne i analityczne. Z badania powstają zapisy o zidentyfikowanych zagrożeniach i/lub zaburzenia działania w celu dalszego badania i rozwiązania problemu.
- Badanie jest wykonywane przez specjalistów z różnych dziedzin mających odpowiednie wyszkolenie i doświadczenie, dysponującymi intuicją i dobrym sądem.
- Badanie przeprowadza się w atmosferze myślenia pozytywnego i otwartej dyskusji – rozpatrzenie zidentyfikowanych problemów odkłada się na później; problem, który został zidentyfikowany, zostaje zapisany i następnie problemy są kolejno oceniane i rozwiązywane.
- Zalecenia do rozwiązania zidentyfikowanych problemów nie są pierwszoplanowym celem badania HAZOP, lecz mogą zostać zapisane do rozważenia przez osoby odpowiedzialne za projekt.

Badanie HAZOP składa się z czterech kolejnych kroków, jak to pokazano na rys. 6.

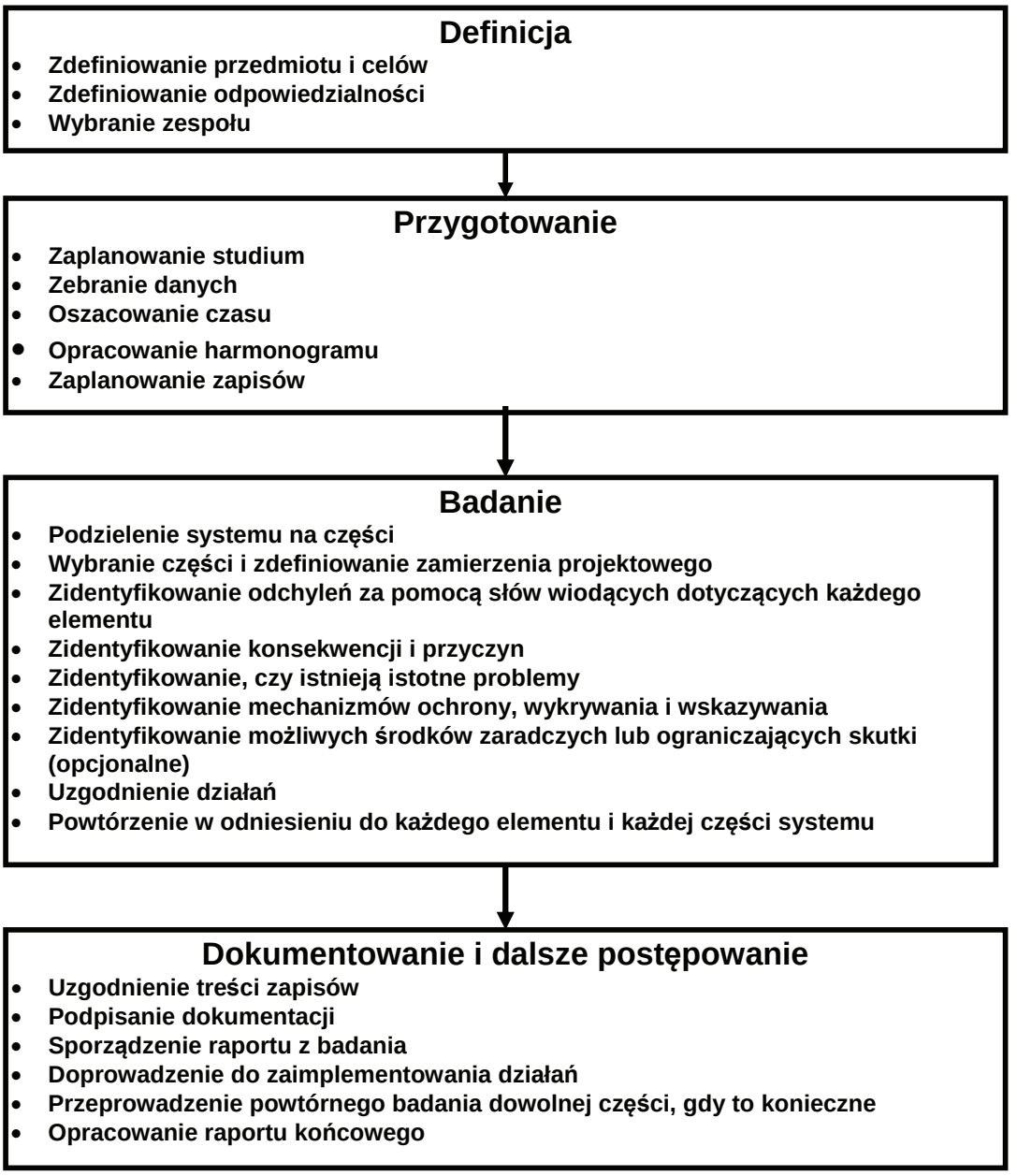
Podstawą HAZOP jest „badanie według słów wiodących”, które jest przemyślanym poszukiwaniem odchyleń od zamierzenia projektowego. W celu ułatwienia badania system dzieli się na części w taki sposób, aby zamierzenie projektowe dotyczące każdej z nich mogło być odpowiednio zdefiniowane. Rozmiar wybranych części zaleca się dobierać zależnie od złożoności systemu i ostrości zagrożeń. W przypadku systemów złożonych lub powodujących wysokie zagrożenie, części powinny być małe. W przypadku systemów prostych, o niskich zagrożeniach, przyjęcie dużych części usprawni badanie. Zamierzenie projektowe dotyczące określonej części systemu wyraża się przez elementy, które dają pojęcie o jej istotnych właściwościach i przedstawiają jej naturalny podział. Wybór elementów do zbadania jest do pewnego stopnia decyzją subiektywną, która może mieć kilka kombinacji prowadzących do uzyskania wymaganego zamierzenia i wybór może także zależeć od konkretnego zastosowania. Elementami mogą być;

- dyskretne kroki lub etapy w procedurze,
- pojedyncze sygnały lub urządzenia w systemie sterowania,
- wyposażenie lub komponenty procesu lub systemu elektronicznego,

- materiały wejściowe otrzymywane ze źródła,
- czynności wykonywane na materiałach,
- produkt przekazywany do ujścia.

Często może być użytecznym dalsze zdefiniowanie elementów przez ich charakterystyki ilościowe lub jakościowe.

.



Rys. 6. Schemat realizacji HAZOP [13]

Zespół HAZOP bada każdy element (i parametry, gdy są istotne) z punktu widzenia odchyleń od zamierzenia projektowego, które mogą prowadzić do niepożądanych konsekwencji. Identyfikację odchyleń od zamierzenia projektowego osiąga się przez „przepytywanie" systemu za pomocą przygotowanych „słów wiodących". Zadaniem słów wiodących jest stymulowanie myślenia obrazowego, w celu zogniskowania studium i wydobycia idei i spowodowania dyskusji, a tym samym doprowadzenia do maksimum szans na kompletność studium.

5.4. Scenariusze rozwoju zagrożeń

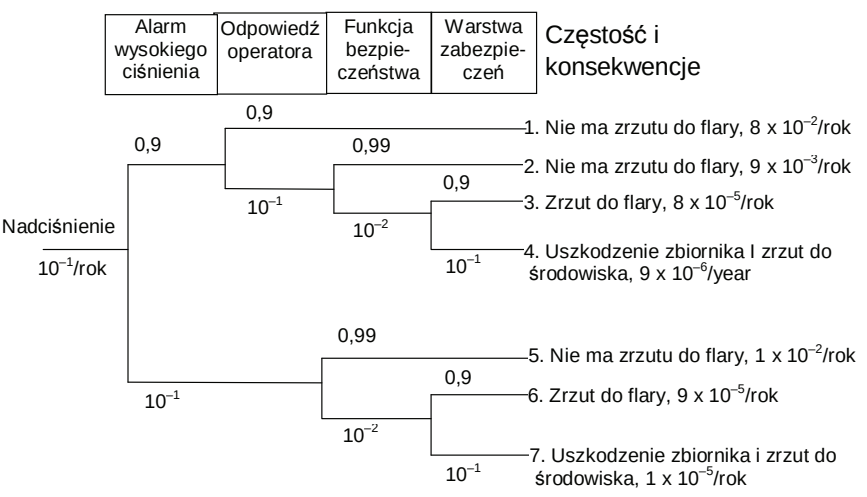
Metoda półilościowa analizy ryzyka [3, 12c] wykorzystuje scenariusze rozwoju zagrożeń. Przykład przedstawiono na rys. 7.

Rys. 7. Przykładowy scenariusz rozwoju zagrożeń

W tym konkretnym przypadku nie zostały spełnione wymagania dotyczące ryzyka tolerowalnego (10^{-4}), wobec czego wprowadzono nowe zabezpieczenie i otrzymano kolejny scenariusz – patrz rys. 8.

W tym przypadku wymagania dotyczące ryzyka tolerowanego zostały spełnione.

Przedstawione przykłady wskazują na możliwość opracowania analogicznych scenariuszy dostosowanych do specyfiki sieci informatycznych.



Rys. 8. Przykładowy scenariusz rozwoju zagrożeń

5.5. Zasada Tak Niskie Jak Rozsądnie Uzasadnione (ALARP) [3, 12c]

W sytuacji rzeczywistej instalacji (np. procesowej lub sieci informatycznej) mogą wystąpić trzy sytuacje wykrywane przy analizie zagrożeń i ryzyka:

a. ryzyko jest tak duże, że w ogóle odrzuca się możliwość eksploatowania obiektu,

b. ryzyko jest lub może być tak małe, że można je uważać za bez znaczenia,

c. ryzyko mieści się między stanami a i b, i może zostać zmniejszone do najniższego praktycznie uzasadnionego poziomu, mając na względzie korzyści wynikające z jego zaakceptowania i biorąc pod uwagę koszty dalszej redukcji.

W odniesieniu do przypadku c zasada ALARP zaleca, aby dowolne ryzyko zostało zredukowane do poziomu tak niskiego, jak to jest rozsądnie wykonalne. Jeśli ryzyko mieści się między wymienionymi wyżej dwiema skrajnościami i zastosowano zasadę ALARP, to ryzyko wynikowe jest ryzykiem dopuszczalnym w danej konkretnej sytuacji.

Ryzyko powyżej pewnego poziomu uznaje się za niedopuszczalne i nie może być ono usprawiedliwione żadnymi zwykłymi okolicznościami.

Poniżej tego poziomu jest obszar tolerowania, w którym jest dopuszczalna działalność w założeniu, że związane z nią ryzyko zostało zmniejszone tak, jak to jest rozsądnie wykonalne. Tolerowane oznacza co innego niż dopuszczalne (akceptowalne) – wskazuje na chęć życia z ryzykiem, tak by chronić pewne korzyści, jednocześnie spodziewając się, że będzie ono analizowane i redukowane jak tylko będzie to możliwe do wykonania. W tej sytuacji zaleca się stosowanie rachunku ekonomicznego, albo bezpośrednie, albo pośrednie, w celu wyważenia kosztów i uzyskiwanych korzyści uzasadniających wprowadzenie dodatkowych środków zabezpieczających/ochronnych lub zaniechanie tego działania.

Poniżej zakresu tolerancji, poziom ryzyka jest uważany za na tyle nieznaczący, że organ wydający przepisy nie potrzebuje żądać dalszych ulepszeń. Jest to powszechnie akceptowalny obszar, w którym ryzyko jest małe w porównaniu do codziennego ryzyka, które wszyscy ponosimy. Aczkolwiek w tym powszechnie akceptowalnym obszarze nie ma potrzeby szczegółowego działania w celu wykazania spełnienia zasady ALARP, to jednakże jest konieczne stałe czuwanie, aby ryzyko pozostawało w tym obszarze.

Koncepcja ALARP może być stosowana gdy przyjęto tak jakościowe jak i ilościowe cele przy określeniu ryzyka. Szersze informacje są zawarte w normie [12.c]. Przykładem stosowania zasady ALARP z podaniem kategoryzacji ryzyka jest norma kolejowa [9]. Zdefiniowano w niej 24 klasy ryzyka przypisując do nich wymagane poziomy nienaruszalności bezpieczeństwa wyposażenia związanego z bezpieczeństwem [11a], co zestawiono w tablicy 3.

Tablica 3 – Kategoryzacja klas ryzyka wg PN-EN 50128 [9]

Wskaźniki zdarzeń zagrażających – Poziomy nienaruszalności bezpieczeństwa						
	POZIOMY CZĘSTOŚCI ZDARZEŃ					
Poziom ostrości zdarzenia	**Częsty**	**Prawdo-podobny**	**Okazjonalny**	**Przypad-kowy**	**Niepraw-dopodobny**	**Niewiary-godny**
Katastrofi-czny	1 – SIL4	2 – SIL4	3 – SIL3	4 – SIL3	5 – SIL3	6 – SIL2
Krytyczny	7 – SIL4	8 – SIL3	9 – SIL3	10 – SIL3	11 – SIL2	12 – SIL2
Marginalny	13 – SIL3	14 – SIL3	15 – SIL3	16 – SIL2	17 – SIL2	18 – SIL1
Nieznaczący	19 – SIL3	20 – SIL3	21 – SIL2	22 – SIL2	23 – SIL1	24 – SIL1

Poziomy 1, 2, 7 są uznane za nietolerowane (ryzyko bardzo wysokie), poziomy 3, 4, 5, 8, 9, 10, 13, 14, 14, 19 i 20 uznano za niepożądane (ryzyko wysokie), poziomy 6, 11, 12, 16, 17, 21, 22 – za tolerowane (ryzyko średnie) zaś poziomy 18, 23 i 24 za pomijalne (ryzyko niskie).

Tego rodzaju kategoryzacja może być wykorzystana w metodach proponowanych przez Vavoulasa i Xenakisa [4] oraz Chołdę i Jajszczyka [5].

5.6. Analiza warstw zabezpieczeń

Sieć informatyczna jest zabezpieczana na wiele sposobów, tak sprzętowo, jak i programowo. Stosowane zabezpieczenia tworzą „warstwy zabezpieczeń". Do analizy skuteczności i dostateczności wprowadzonych i/lub przewidzianych zabezpieczeń może posłużyć metoda LOPA (*Layer of Protection Analysis*) [3, 12c]. Danymi wejściowymi metody są dane uzyskane w Badaniu HAZOP [13]; następnie uwzględnia się każde zidentyfikowane zagrożenie, przez udokumentowanie, przyczyny inicjującej i warstw zabezpieczenia zapobiegających lub ograniczających zagrożenie. Tym samym może zostać określony całkowity istniejący zakres redukcji ryzyka i przeanalizowana potrzeba jego dalszego zmniejszenia. LOPA jest metodą realizowaną przez zespół multidyscyplinarny do określenia dostateczności zabezpieczeń. W przypadku analizy sieci informatycznej zespół powinien składać się z:

- operatora doświadczonego w prowadzeniu rozpatrywanego rodzaju sieci,
- inżyniera z doświadczeniem w rozpatrywanym rodzaju sieci,
- menedżera sieci,
- inżyniera automatyka procesu sterowanego rozpatrywaną siecią,
- osoby serwisu przyrządów/elektrycznego z doświadczeniem w zakresie rozważanego rodzaju sieci i procesu sterowanego,
- specjalisty ds. analizy ryzyka.

Jeden z członków zespołu powinien być przeszkolony w metodologii LOPA.

Informacje wymagane przez LOPA są zawarte w danych zgromadzonych i opracowanych w HAZOP. W tablicy 4 przedstawiono zależność między danymi wymaganymi przez LOPA i danymi opracowanymi w czasie HAZOP. Na rys. 9 przedstawiono typowy arkusz kalkulacyjny, który może być zastosowany do LOPA. Wartości liczbowe zamieszczone w tym arkuszu są przykładowe.

Tablica 4 – Dane do LOPA opracowane w HAZOP

Informacje wymagane przez LOPA	Informacje opracowane w HAZOP
Zdarzenie oddziałujące	Konsekwencja
Poziom ostrości	Ostrość konsekwencji
Przyczyna inicjująca	Przyczyna
Prawdopodobieństwo zainicjowania	Częstość zaistnienia przyczyny
Warstwy zabezpieczeń	Zabezpieczenia istniejące
Wymagane ograniczenie dodatkowe	Zalecane nowe zabezpieczenia

#	1	2	3	4		5		6	7	8	9	10	11
					WARSTWY ZABEZPIECZEŃ								
	Opis zdarzenia oddziałującego F.3 F.14.1	Poziom ostrości F.4 F.14.1	Przyczyna inicjująca F.5 F.14.2	Prawdopodobieństwo zainicjowania F.6 F.14.3	Ogólny projekt procesu F.14.4	BPCS F.14.5	*Alarmy itp.* F.14.6	Ograniczenie dodatkowe, dostęp ograniczony, F.8 F.14.7	IPL Dodatkowe tamy ogranicz., dekompresja F.9 F.14.8	Prawdopodobieństwo średnie zdarzenia F.10 F.14.9	Poziom nienaruszalności SIF F.11 F.14.10	Prawdopodobieństwo zdarzenia ograniczającego F.12 F.14.10	Uwagi
1	Ogień z pęknięcia kolumny destylacyjnej	S	Brak dopływu wody chłodzącej	0,1	0,1	0,1	0,1	0,1	PRV 01	10^{-7}	10^{-2}	10^{-9}	Wysokie ciśnienie powoduje pęknięcie kolumny
2	Ogień z pęknięcia kolumny destylacyjnej	S	Uszkodzenie pętli regulacji pary	0,1	0,1		0,1	01	PRV 01	10^{-6}	10^{-2}	10^{-8}	To samo co wyżej
N													

IEC 3025/02

UWAGA Poziom ostrości: E = Rozległy; S = Poważny; M = Niewielki

Wartości prawdopodobieństwa są liczbami zdarzeń na rok, inne wartości liczbowe są średnimi prawdopodobieństwami uszkodzenia przy przywołaniu

Rys. 9. Raport Analizy Warstw Zabezpieczeń (LOPA)

6. PODSUMOWANIE

Wykazano zbieżność metod stosowanych w technice bezpieczeństwa funkcjonalnego do analizy ryzyka i oceny dostateczności zabezpieczeń z potrzebami, jakie się ujawniły w związku z podobnymi ocenami sieci informatycznych. Zaproponowano zastosowanie niektórych metod. Przedstawione tu propozycje będą rozwijane.

Opracowanie zostało sfinansowane w ramach zadania 4.R.08 „Modele i procedury oceny zgodności bezpieczeństwa funkcjonalnego systemów zabezpieczeniowych sektorze przemysłu procesowego" Programu Wieloletniego „Poprawa bezpieczeństwa i warunków pracy" koordynowanego przez CIOP-PIB.

BIBLIOGRAFIA

1. Missala T.: *Zabezpieczenie sieci przemysłowych przed intruzami – temat dnia.* Pomiary, Automatyka, Robotyka nr 2/2010, s. 180–189.
2. Missala T.: *Walidacja złożonych systemów automatyki i robotyki.* Pomiary, Automatyka, Robotyka nr 2/2009, s. 201–213.
3. Missala T.: *Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa.* Monografia. Przemysłowy Instytut Automatyki i Pomiarów. Warszawa, 2009 r.

4. Vavoulas N., Xenakis Ch.: *A Quantitative Risk Analysis Approach for deliberate Threats.* Conference Pre-Proceedings, 5th International Workshop on Critical Information Infrastructures Security, CRITIS'10, Athens, 2010 r., s. 13–26.
5. Chołda P., Jajszczyk A.: *Resilience metrics*. Presentation on the special session of 4th International Workshop on Critical Information Infrastructures Security, CRITIS'09, Athens, 2010 r.
6. Duessel P. et all.: *Cyber-Critical Infrastructure Protection Using Real-time Payoload-Based anomaly Detection.*, 4th International Workshop on Critical Information Infrastructures Security, CRITIS'09, Bonn, 2009 r., Springer, Conference Revised Papers, s. 85–97.
7. Batista Jr. A.B. et all.: *Application Filters for TCP/IP Industrial Automation Protocols.* 4th International Workshop on Critical Information Infrastructures Security, CRITIS'09, Bonn, 2009 r.,Springer,Conference Revised Papers, s. 111–123.
8. Choraś M. et all.: *Ontology-Based Reasoning Combined with Inference Engine for SCADA-ITC Independencies, Vulnerabilities and Treats Analysis.* 4th International Workshop on Critical Information Infrastructures Security, CRITIS'09, Bonn, 2009 r., Springer, Conference Revised Papers, s. 98–110.
9. PN-EN 50128:2002, Zastosowania kolejowe – Łączność, sygnalizacja i systemy sterowania – Programy dla kolejowych systemów sterowania i zabezpieczenia (*oryg.*).
10. PN-EN 61069, Pomiary i sterowanie procesami przemysłowymi – Określenie właściwości systemu w celu jego oceny.
    a. PN-EN 61069-1:2002, Część 1: Postanowienia ogolne i metodologia.
    b. PN-EN 61069-2:2002, Część 2: Metodologia oceny.
    c. PN-EN 61069-3:2002, Część 3: Ocena funkcjonalnosci systemu.
    d. PN-EN 61069-4:2002, Część 4: Ocena parametrów systemu.
    e. PN-EN 61069-5:2004, Część 5: Ocena niezawodności systemu.
    f. PN-EN 61069-6:2004, Część 6: Ocena współdziałania systemu z operatorem.
    g. PN-EN 61069-7:2004, Część 7: Ocena bezpieczeństwa systemu.
    h. PN-EN 61069-8:1004, Część 8: Ocena niewiążących się z zadaniem właściwości systemu.
11. PN-EN 61508 (IEC 61508): Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem:
    a PN-EN 61508-1:2010 Część 1:Wymagania ogólne *(oryg.).*
    b PN-EN 61508-2:2010 Część 2: Wymagania dotyczące elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem *(oryg.).*
    c PN-EN 61508-3:2010 Część 3: Wymagania dotyczące oprogramowania *(oryg.).*
    d PN-EN 61508-4:2010 Część 4: Definicje i skrótowce *(oryg.).*
    e PN-EN 61508-5:2010 Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa *(oryg.).*

f PN-EN 61508-6:2010 Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3 *(oryg.)*.

g PN-EN 61508-7:2010 Część 7: Przegląd technik i miar *(oryg.)*.

12. PN-EN 61511 (IEC 61511): Bezpieczeństwo funkcjonalne – Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego:
    a. PN-EN 61511-1:2005 Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania.
    b. PN-EN 61511-2:2008 Część 2 : Wytyczne do stosowania IEC 61511-1.
    c. PN-EN 61511-3:2009 Część 3: Wytyczne do określania poziomów nienaruszalności bezpieczeństwa .
13. PN-EN 61882:2005, Badanie zagrożeń i zdolności do działania (badania HAZOP) – Przewodnik zastosowań.
14. PN-EN ISO 9000:2006, Systemy zarządzania jakością – Podstawy i terminologia.
15. PN-ISO/IEC 27001:2007, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem – Wymagania.
16. PN –ISO/IEC 13332-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management.
17. ITU-T E800, Telecommunication Standardization Sector of ITU, (09/2008) – Series E: Overall network operation, Telephone service, service operation and human factors – Quality of telecommunication services: concepts, models, objectives and dependability planning – Terms and definitions related to the quality of telecommunication services – Definitions of terms related to quality of service. Recommendation ITU.
18. ISA-100.11a-2009, An ISA Standard – Wireless systems for industrial automation: Process control and related application.
19. IEC 62443-1-1: 2009: Industrial communication networks – network and system security – Part 1-1: Terminology, concepts and models.
20. IEC 62443-2-1(65/438/CDV: Industrial communication networks – network and system security – Part 2-1: Establishing an industrial automation and control system security program.
21. IEC/TR 662443-3-1:2009: Industrial communication networks – network and system security – Part 5: Security technologies for industrial automation and control systems.
22. NIST National Institute of Standard and Technology; USA – SP 800-30: Risk Management Guide for Information Technology Systems – Recommendations, July 2002.
23. The CORAS Method [http://coras.souceforge.net/].
24. Facilitated Risk Analysis Process (FRAP) [www.wikipedia.org/Risk_analysis_(buissnes)].
25. Model krok po kroku [www.piap.pl/certyfikacja].