Współczesna Gospodarka

Contemporary Economy
Electronic Scientific Journal
www.wspolczesnagospodarka.pl

Vol. 7 Issue 2 (2016) 53-69
ISSN 2082-677X

UWARUNKOWANIA ANALIZY RYZYKA W INFRASTRUKTURZE KRYTYCZNEJ SEKTORA ENERGII

Przemysław Borkowski

Streszczenie

Artykuł podejmuje problem oceny ryzyka w infrastrukturze krytycznej. W szczególności koncentruje się na uwarunkowaniach modelu identyfikacji i ewaluacji ryzyka wynikających ze specyfiki infrastruktury krytycznej sektora energii. Przedstawiono ograniczenia, jakim podlegał będzie taki model, zaproponowano koncepcję klasyfikacji ryzyka możliwą do zastosowania w odniesieniu do infrastruktury krytycznej oraz wskazano na różnice w stosunku do klasycznych procedur modelowania ryzyka.

Słowa kluczowe: ryzyko w infrastrukturze krytycznej, analiza ryzyka w infrastrukturze, zarządzanie ryzykiem infrastrukturalnym

Wstęp

Sprawne funkcjonowanie gospodarki jest w dużym stopniu uzależnione od efektywnego działania infrastruktury. Infrastruktura warunkuje współdziałanie różnych gałęzi gospodarki, umożliwia wymianę i produkcję. Wybrane elementy infrastruktury mogą mieć tak duże znaczenie, że przyjęło się nazywać je „infrastruktura krytyczną". Pojęcie infrastruktury krytycznej zdefiniowane zostało na gruncie europejskim w „Europejskim programie ochrony infrastruktury krytycznej" (The European Programme for Critical Infrastructure Protection) oraz dyrektywie Komisji Europejskiej[1] jako: składnik, system lub część infrastruktury zlokalizowanej na terytorium państw członkowskich, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu

[1] Dyrektywa Rady UE z 8 grudnia 2008 roku w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz potrzeb w zakresie poprawy jej ochrony, Dziennik Urzędowy Unii Europejskiej L 345 z 23.12.2008.

materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo członkowskie w wyniku utracenia tych funkcji. W myśl ustawodawstwa polskiego są to: systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[2].

Do infrastruktury kluczowych sektorów w których występują obiekty infrastruktury krytycznej w Polsce (funkcjonującej w obiegu cywilnym) zaliczyć można infrastrukturę związaną z transportem, infrastrukturę energetyczną (zarówno produkcyjną jak i przesyłową) infrastrukturę sektora paliwowego (wytwarzania i przerobu paliw oraz przesyłową). W szerokiej interpretacji do infrastruktury krytycznej zaliczyć można także systemy łączności, finansowe, zaopatrzenia w żywność, ochronę zdrowia, ratownicze i zapewniające ciągłość funkcjonowania administracji publicznej.

Zgodnie z tym zbiorem definicji niemal każdy rodzaj infrastruktury w istocie ma charakter krytyczny. Wynika to z rosnącej specjalizacji produkcji i konieczności angażowania coraz bardziej różnorodnych zasobów na każdym etapie procesu gospodarowania. Niewątpliwie typem infrastruktury, której istnienie jest warunkiem koniecznym dla funkcjonowania wszystkich innych sektorów jest infrastruktura sektora produkcji i dystrybucji energii.

1. Infrastruktura krytyczna sektora energii w Polsce

Zgodnie z wytycznymi Komisji Europejskiej to na władzach krajowych ciąży obowiązek przedstawienia listy obiektów wchodzących w skład infrastruktury krytycznej. W Polsce za jej tworzenie odpowiedzialne jest Rządowe Centrum Bezpieczeństwa. W odniesieniu do sektora energii zakres infrastruktury krytycznej determinuje dodatkowy akt prawny[3] wprowadzający listę instalacji specjalnego znaczenia (np. gazociągów, linii elektroenergetycznych, magazynów ropy, terminali LNG itp.) nazywanych „infrastrukturą krytyczną". Na ostateczny przyszły kształt krajowej infrastruktury krytycznej składają się istniejące i realizowane obiekty. W zakresie sektora energii za mające wpływ na kształtowanie inwestycji w infrastrukturę krytyczną sektora uznać należy dokumenty:

- Strategia Europa 2020,
- Strategia Energia 2020,
- Krajowy Program Reform Europa 2020,
- Polityka energetyczna Polski do 2030 roku.

W dokumentach tych wskazuje się na konieczność rozwoju poprzez inwestycje oparte na wiedzy i innowacjach, na zrównoważony wzrost dążący do tworzenia gospodarki niskoemisyjnej i rozwój zapewniający spójność terytorialną i społeczną.

Z punktu widzenia rozbudowy infrastruktury krytycznej sektora energii znaczenie ma przede wszystkim drugi z wymienionych priorytetów, wpływa bowiem na możliwe zastosowane technologie, a także limituje sam zakres możliwych nowych inwestycji i wymusza inwestycje modernizacyjne Wynika to wprost z celu graniczenie emisji gazów cieplarnianych o co najmniej 20% w porównaniu z poziomem z 1990 r. oraz zwiększenia udziału odnawialnych źródeł energii w UE do 20%.

Cele krajowe przyjęte przez Polskę to m.in. ograniczenie wykorzystania energii pierwotnej do poziomu ok. 96 Mtoe; wzrost wykorzystania OZE do poziomu 15,5 % w 2020 r. i redukcja emisji CO2 o 20% wobec roku bazowego (1990). To zaś oznacza z jednej strony, że istniejąca

[2] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, art. 3 pkt. 2, Dz.U. 2007 nr 89 poz. 590.

[3] Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego dla spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, Dz.U. 2010 nr 65 poz. 404.

infrastruktura krytyczna jest niewystarczająca, z drugiej, że jej struktura jest przestarzała. W konsekwencji wymuszać to będzie realizację dwutorowej strategii rozwoju infrastruktury krytycznej – wzrostu ilościowego i zmiany jakościowej. Wpisując się w nową europejską strategię zdefiniowaną przez programy „Energia 2020" i „Europa 2020", które mają zapewnić UE zrównoważone dostawy energii i wspierać wzrost gospodarczy, polityka energetyczna Polski do 2030 zmierza do redukcji energochłonności gospodarki. Działania takie możliwe jest jedynie poprzez nowe inwestycje w zakresie infrastruktury energetycznej.

Listę nowych obiektów infrastruktury krytycznej zawiera dokument: „Lista Projektów Strategicznych dla infrastruktury energetycznej w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020"[4]. W zakresie infrastruktury przesyłu energii elektrycznej mowa jest o 24 projektach inwestycyjnych i 188 projektach rozbudowy sieci dystrybucyjnej energii. W zakresie infrastruktury przesyłu gazu są to 23 projekty, a w zakresie jego magazynowania - 6 projektów. W ramach rozbudowy sieci dystrybucji gazu przewidziano do realizacji 45 projektów infrastrukturalnych. Oddzielnym zadaniem inwestycyjnym jest rozbudowa terminalu LNG w Świnoujściu. Zestawienie wielkości planowanych inwestycji w infrastrukturze krytycznej przedstawiono w tablicy 1.

Tablica 1. Planowane inwestycje w infrastrukturę krytyczną sektora energii w Polsce w latach 2014-2020

L.P.	Typ infrastruktury	Wielkość inwestycji
1.	Budowa i modernizacja gazociągów przesyłowych lub dystrybucyjnych 2 300	591 km
2.	Budowa i modernizacja elektroenergetycznych sieci przesyłowych i dystrybucyjnych	717 km
3.	Zwiększenie zdolności przeładunkowych terminala LNG do odbioru gazu dostarczanego droga morską	2400 mln m^3
4.	Rozbudowa magazynów podziemnych gazu w celu zaspokojenia szczytowego dobowego zapotrzebowania	13 mln m^3
5.	Zwiększenie pojemności czynnej wspartych podziemnych magazynów gazu ziemnego	1000 mln m^3

Źródło: opracowanie własne na podstawie: *Lista Projektów Strategicznych dla infrastruktury energetycznej w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020*, Ministerstwo Gospodarki, Warszawa 2015.

Alternatywą dla ekstensywnej rozbudowy infrastruktury sektora energii jest poprawa efektywności energetycznej jaka może nastąpić przede wszystkim poprzez zwiększenie bezpieczeństwa dostaw paliw i energii, dywersyfikację ich źródeł, a także dywersyfikację samej struktury wytwarzania energii. Warunkiem realizacji zarówno strategii ilościowej jak i jakościowej jest zachowanie utrzymanie zdolności operacyjnej i cech funkcjonalnych istniejących i nowych obiektów wchodzących w skład infrastruktury krytycznej – a więc działania pozwalające na wyeliminowanie ryzyka dla infrastruktury krytycznej w sektorze energii.

[4] *Lista Projektów Strategicznych dla infrastruktury energetycznej w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020*, Ministerstwo Gospodarki, Warszawa 2015.

3. Ryzyko infrastruktury krytycznej w sektorze energii

Ryzyko w sektorze energii dotyczy zarówno producentów i dystrybutorów jak i nabywców energii. Z punktu widzenia ryzyka dotyczącego kluczowej infrastruktury energetycznej jest to jednak ryzyko leżące niemal wyłącznie (wyjątkiem będą awarie dotykające podmioty zewnętrzne) po stronie podażowej. Spośród podstawowych rodzajów ryzyka rozpoznawanych w sektorze energii wymienić należy[5]:

- ryzyko polityczne w tym:
  - ryzyko wojny,
  - ryzyko rewolucji,
  - ryzyko zamieszek i niepokojów społecznych,
  - ryzyko terroryzmu,
  - ryzyko nacjonalizacji,
  - ryzyko regulacyjne i prawne,
- ryzyko środowiskowe,
- ryzyko siły wyższej i zdarzeń losowych,
- ryzyko ekonomiczne, w tym:
  - ryzyko popytu,
  - ryzyko finansowe (w szczególności kredytowe i stóp procentowych),
  - ryzyko konkurencji,
  - ryzyko rynkowe (w szczególności cenowe w zakresie surowców i nośników energii),
  - ryzyko projektu (kosztowe),
- ryzyko technologiczne.

Z punktu widzenia funkcjonowania infrastruktury krytycznej tego sektora kluczowe będą niektóre elementy ryzyka politycznego. Skrajnie niekorzystny wpływ na funkcjonowanie infrastruktury sektora będzie miało ryzyko wojny. W warunkach pokoju natomiast za istotne z punktu widzenia bezpieczeństwa infrastruktury krytycznej uznać trzeba ryzyko terroryzmu, ryzyko siły wyższej i zdarzeń losowych, których konsekwencją jest ryzyko awarii. Pośrednio generować mogą one ryzyko środowiskowe i ryzyko bezpieczeństwa dla stron trzecich, np. dla ludności zamieszkującej obszary na których infrastruktura krytyczna jest zlokalizowana. W stosunkowo małym stopniu na ryzyko dla infrastruktury krytycznej wpływać będzie w krajach o systemie demokratycznym ryzyko zamieszek i wojny domowej. Te ostatnie jest znikome z uwagi na bardzo niskie prawdopodobieństwo wystąpienia w krajach demokratycznych. Natomiast ryzyko niepokojów społecznych zależne jest od stabilności systemu politycznego. Kraje o ugruntowanej demokracji charakteryzują się dużą odpornością na tego typu zjawiska i nawet gdy one wystąpią, przyjmują formę protestów ulicznych, strajków i demonstracji, a więc zdarzeń nie zagrażających bezpośrednio funkcjonowaniu infrastruktury krytycznej.

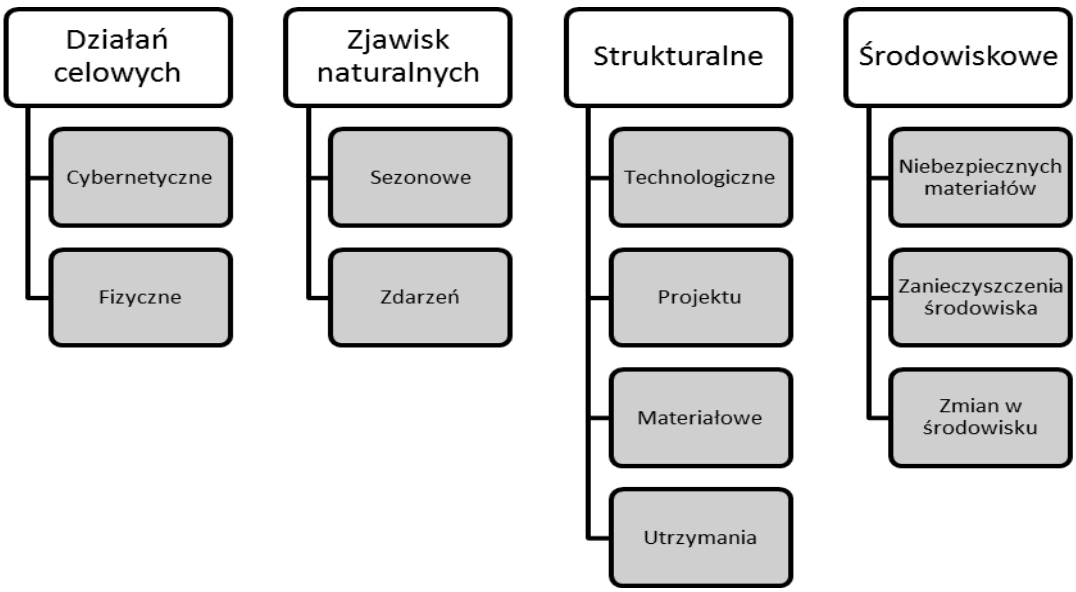
Najpoważniejszy wymiar dla bezpieczeństwa infrastruktury krytycznej ma ryzyko terroryzmu. W odniesieniu do sektora energii dotyczyć ono będzie zarówno instalacji wydobycia jak i przesyłu surowców energetycznych i energii. Na akty terroru narażone są zarówno instalacje morskie jak i lądowe, w szczególności – z uwagi na rozmiary – infrastruktura przesyłowa. Teoretycznie najpoważniejsze konsekwencje w sektorze energetycznym może przynieść atak terrorystyczny skierowany przeciwko elektrowni atomowej. Ryzyko to jest jednak ograniczane bardzo rozbudowanymi systemami zabezpieczeń i szacowane jako bardzo mało prawdopodobne. W energetyce atomowej standardem jest

[5] P. Borkowski, *Kluczowe czynniki ryzyka w sektorze energetycznym*, (w:) *Zarządzanie ryzykiem w działalności gospodarczej*, red. J. Winiarski, D. Wach, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2015, s. 41.

posługiwanie się miarami prawdopodobieństwa realizacji ryzyka określającymi jego częstość jako mniejszą niż raz na 10000 lat (stosuje się wówczas pojęcie "*black swan event*")[6].

Natomiast ryzyko ekonomiczne w sektorze energii ma niewielki bezpośredni wpływ na ryzyko dla infrastruktury krytycznej. Objawia się ono zmniejszeniem zapotrzebowania na wykorzystanie infrastruktury i może prowadzić do okresowego wyłączania jej obiektów lub w przypadku, gdy zjawisko ma charakter trwały – do jej likwidacji. Wówczas jednak z definicji infrastruktura ta przestaje mieć „:krytyczne" znaczenie dla gospodarki kraju. Pośrednią ale istotną konsekwencją ryzyka ekonomicznego może być spadek wydatków na zapewnienie bezpiecznego funkcjonowania infrastruktury krytycznej i w konsekwencji zwiększona jej awaryjność. Bardzo poważne konsekwencje może mieć ryzyko siły wyższej i zdarzeń losowych. Ekstremalne zjawiska naturalne mogą powodować uszkodzenia obiektów infrastrukturalnych. W szczególności na ryzyko to narażone są w sposób powtarzalny elementy infrastruktury liniowej (infrastruktura przesyłowa). W fazie inwestycyjnej za ważne uznać należy ryzyko kosztowe, które prowadzić może do zawieszenia realizacji projektu infrastrukturalnego. Z punktu widzenia zarządzania ryzykiem infrastruktury krytycznej pod uwagę bierze się jednak przede wszystkim ryzyko występujące w fazie eksploatacyjnej, wówczas, gdy infrastruktura ta funkcjonuje.

Ten ogólny przegląd ryzyka sektora uprawnia do sformułowania wniosku, że podczas analizowania ryzyka w infrastrukturze krytycznej charakterystycznym jest większe skupianie się na konsekwencjach ryzyka niż na prawdopodobieństwie i źródłach jego pochodzenia. Z tego powodu wiele rodzajów ryzyka ważnych w klasycznej analizie ryzyka sektora energetycznego nie ma znaczenia w odniesieniu do problematyki ryzyka zawężonej do kwestii funkcjonowania samej infrastruktury sektora. W odniesieniu do problemu identyfikacji ryzyka dotyczącego tylko i wyłącznie infrastruktury krytycznej wydaje się więc być celowym zawężenie powyższej ogólnej typologii ryzyka sektora, tak aby wyłączyć te rodzaje ryzyka, które nie są bezpośrednio związane z infrastrukturą. Zaproponować można zmodyfikowana typologię ryzyka stanowiącą instrument bardziej adekwatny dla potrzeb analizy kluczowych przejawów ryzyka w odniesieniu do problematyki funkcjonowania infrastruktury sektora energii (zob. rysunek 1).



Rysunek 1. Typologia ryzyka w infrastrukturze krytycznej sektora energii

Źródło: opracowanie własne.

[6] W. Wade, *Scenario planning. A field guide to the future*, Wiley, Hoboken 2012, s. 150.

Przede wszystkim taka dopasowana do potrzeb aplikacji do infrastruktury krytycznej typologia ryzyka powinna wskazywać na te jego rodzaje, które mają krytyczne znaczenie – a więc mogą doprowadzić do zaburzenia ciągłości funkcji infrastruktury lub jej wyeliminowania. Dlatego wskazać trzeba przede wszystkim na ryzyko: działań celowych, wynikające z przyczyn naturalnych, strukturalne będące rezultatem sposobu budowy obiektów infrastruktury i ryzyko środowiskowe. W tym ostatnim przypadku istotne znaczenie ma istniejące sprzężenie zwrotne między infrastrukturą a otoczeniem. Choć ryzyko środowiskowe generowane jest przez infrastrukturę krytyczną i oddziałuje na otoczenie, to jego realizacja uniemożliwia także funkcjonowanie tejże infrastruktury. Przykładowo wyciek substancji radioaktywnych do środowiska z elektrowni atomowej uniemożliwia także dalsze jej funkcjonowanie (przykład japońskiej Fukushimy) lub przynajmniej bardzo ogranicza możliwości tego funkcjonowania (np. elektrownia w Czarnobylu).

Ryzyko działań celowych (ang. *willfull actions risk*) przejawia się przede wszystkim w postaci możliwości ataku cybernetycznego na systemy informatyczne obsługujące dany obiekt infrastruktury (ang. cyber attack risk) lub na ataku fizycznym (ang. physical attack risk). W pierwszym przypadku w zależności od rodzaju ataku mówić można o ataku zmierzającym do uszkodzenia oprogramowania, zablokowania jego działania lub o ataku zmierzającym do przejęcia części informacji z systemu informatycznego, czy też o ataku zmierzającym do przejęcia kontroli nad systemem informatycznym umożliwiającej fizyczną manipulację infrastrukturą. W drugim przypadku infrastruktura może ulec zniszczeniu na skutek wandalizmu lub ataku terrorystycznego.

Ryzyko zjawisk naturalnych (ang. *natural hazards risk*) odzwierciedla procesy i zdarzenia opisywane w klasycznych metodologiach ryzyka, jako siła wyższa lub ryzyko losowe. W odniesieniu do infrastruktury krytycznej ważniejsze jest spoglądanie na skutki niż przyczyny ryzyka. Z tego wynika też proponowana zmiana podejścia do klasyfikacji ryzyka. O ile klasyczne klasyfikacje ryzyka wskazują głównie na źródła ryzyka, w odniesieniu do infrastruktury krytycznej ważniejsze są jego skutki. Dlatego celowe jest m.in. rozróżnienie między ryzykiem o charakterze sezonowym i cyklicznym (ang. *seasonal risk*) a ryzykiem o charakterze jednorazowym (ang. *event risk*). W obrębie tej pierwszej grupy mowa o ryzyku wynikającym z warunków pogodowych uzależnionych od klimatu w jakim dana infrastruktura się znajduje. Np. opady śniegu mogą powodować dodatkowe obciążenie i załamanie konstrukcji niektórych obiektów– ale są one do przewidzenia, mają bowiem związek z cyklicznymi zmianami pogody. Zdarzeniem jednorazowym byłyby te same, ale niespotykanie obfite opady śniegu. Zatem obie kategorie składowe ryzyka naturalnego dotyczą w istocie tych samych zjawisk, różna jest jednak ich częstotliwość i nasilenie. Do zagrożeń pierwszego typu operator infrastruktury krytycznej powinien być przygotowany rutynowo, to druga grupa może być powodem niekontrolowanego wzrostu poziomu ryzyka.

Ryzyko strukturalne (ang. *structural risk*) dotyczy możliwych awarii wynikających z problemów, które wystąpiły (ale nie zostały ujawnione) na etapie budowy infrastruktury. Ryzyko technologiczne (ang. *technology risk*) dotyczyć tu będzie zastosowania przestarzałej i awaryjnej technologii, lub technologii nieodpowiedniej do realizacji określonych zadań. Np. rurociąg może charakteryzować się określonymi parametrami wytrzymałościowymi, a w praktyce pracować pod obciążeniami je przekraczającymi. Ryzyko projektu (ang. *design risk*) odzwierciedla błędy techniczne popełnione na etapie projektowania infrastruktury. Ryzyko materiałów (ang. *material risk*) dotyczy zwiększonej podatności na uszkodzenia lub szybszego niż zakładane zużywanie się elementów technicznych na skutek zastosowania nieodpowiednich materiałów budowlanych w konstrukcji obiektów. Ryzyko utrzymania (ang. *maintenance risk*) odzwierciedla brak lub ograniczenia prac przeglądowych i konserwatorskich skutkujące zwiększonym prawdopodobieństwem awarii.

Ryzyko środowiskowe obejmuje zarówno oddziaływanie infrastruktury na środowisko poprzez emisje do powietrza, zanieczyszczenie wód i gleby (ang. *pollution risk*) jak i zwiększone oddziaływanie szkodliwych biologicznie substancji, środków chemicznych czy izotopów radioaktywnych (ang. *hazardous materials risk*). W grę wchodzić mogą efekty wtórne generowane np. na skutek wcześniejszego fizycznego uszkodzenia obiektów na skutek zaistnienia jednego z wcześniej wymienianych typów ryzyka. Ponadto inwestycje w obiekty infrastruktury krytycznej często wymagają rozbudowanych prac ziemnych, w istotny sposób ingerujących w walory krajobrazowe danego obszaru (ang. *environment alteration risk*). Przykładowo rozbudowa kopalni odkrywkowych surowców energetycznych prowadzić może do masowych dewastacji krajobrazu, ale także - przy niewłaściwym prowadzeniu prac wydobywczych - uniemożliwiać funkcjonowanie samej kopalni.

3. Uwarunkowania tworzenia procedur identyfikacji i oceny ryzyka w zakresie infrastruktury krytycznej sektora energii

Procedury ryzyka dotyczącego infrastruktury krytycznej wywodzą się z teorii systemów. Natomiast praktyczne narzędzia redukcji ryzyka powstały w wyniku ulepszania procedur kontroli wywodzących się z przemysłu i sfery zarządzania bezpieczeństwem.

Ryzyko, w tym przypadku, definiowane będzie zatem przede wszystkim poprzez analizę negatywnych konsekwencji jego realizacji. W sferze działalności przemysłowej znajduje to odzwierciedlenie w rozdzielaniu ryzyka dopuszczalnego i niedopuszczalnego. Zwraca uwagę, iż jest to już podejście zarządcze – proces identyfikacji ryzyka prowadzi wprost do zadysponowania mechanizmów jego redukcji. Skoro ryzyko jest dopuszczalne, to mechanizm taki jest zbędny, jeśli jest niedopuszczalne – implikuje konieczność niezwłocznego podjęcia działań zaradczych. W pierwszym przypadku oceniający akceptuje poziom ryzyka, w drugim dąży do jego ograniczenia. Wartościowanie ryzyka odbywa się głównie w oparciu o parametr siły oddziaływania, któremu przypisywana jest większa waga niż parametrowi prawdopodobieństwa. W tradycyjnym ujęciu ekonomicznym oba te parametry uznawane są za jednakowo istotne, a samo ryzyko opisywane jako ich iloczyn.

Oceniając ryzyko systemu infrastruktury krytycznej wyjściową będzie funkcja zależności ryzyka od prawdopodobieństwa (mniej istotny parametr) oraz konsekwencji ryzyka (bardziej istotny parametr). Z punktu widzenia funkcjonowania danego systemu infrastruktury krytycznej niewiadome sprowadzają się do pytania o to co może się stać, jakie jest prawdopodobieństwo, że to się stanie i - jeśli się stanie - jakie będą konsekwencje?[7] Na podstawie odpowiedzi na te pytania możliwym jest oszacowanie wielkości ryzyka krytycznego powodującego niemożność dalszego wykorzystania badanego systemu infrastruktury krytycznej. Jednocześnie, w kontekście praktyki oceny ryzyka aplikacji przemysłowych, do jakich zaliczyć można budowę i funkcjonowanie infrastruktury krytycznej sektora energii, zauważyć można, że to konsekwencje ryzyka mają znaczenie decydujące. W rzeczywistości trudno bowiem oczekiwać, że badający ryzyko jest w stanie analizować wszystkie możliwe scenariusze zdarzeń, bo liczba możliwych ścieżek prowadzących do zaburzeń funkcjonowania danego systemu może być wręcz nieskończona. W praktyce oceniający odwołuje się jedynie do skończonej liczby wariantów rozwoju sytuacji. W takim przypadku ryzyko dowolnego układu jest przybliżane za pomocą skończonej liczby scenariuszy ryzyka. To implikuje, że celem analizy ryzyka nie jest precyzyjny pomiar prawdopodobieństwa wszystkich wybranych scenariuszy. Brak precyzji szacunku prawdopodobieństwa jest zastępowany rangowaniem i wyborem właściwych (bardziej prawdopodobnych) scenariuszy. Trafność tego wyboru jest wprost zależna od kompetencji dokonujących ich ekspertów, co wskazuje na kluczową rolę doboru osób, które

[7] S. Kaplan, B.J. Garrick, *On the quantitative definition of risk*, „Risk Analysis", vol. 1, no. 1/1981, s. 11-27.

analizę ryzyka będą prowadziły. Obecna w tym rozumowaniu krytyka klasycznego sposobu analizy ryzyka wywodząca się z ekonomik sektorowych podkreśla, że błędem jest nadmierne uwypuklanie znaczenie prawdopodobieństwa[8]. W odniesieniu do oceny ryzyka infrastruktury krytycznej oceniający wręcz będzie obserwował raczej skutki ryzyka niż szansy jego realizacji. Wynika to z samej istoty terminu infrastruktura krytyczna. Z punktu widzenia podmiotów za nią odpowiedzialnych kalkulacja szansy wystąpienia ryzyka jest drugorzędna, bo pierwszoplanowe jest zapewnienie nieprzerwanego jej funkcjonowania. Ważne jest więc także jak dobrze system podlegający oddziaływaniu ryzyka jest w stanie wytrzymać jego skutki. W takim razie praktycznym celem analizy ryzyka infrastruktury krytycznej powinno być zidentyfikowanie obszarów wrażliwych i doprowadzenie do ich immunizacji na ryzyko. Co więcej spośród wszystkich prawdopodobnych scenariuszy ryzyka rozpatrywane winny być tylko te na które dany system w ogóle jest wrażliwy[9]. Wrażliwość systemu na ryzyko dotyczy jedynie tej grupy zdarzeń, która może wpłynąć negatywnie na system. System zatem może być wrażliwy na pewne zdarzenia (i jest to wówczas ryzyko) i niewrażliwy na inne (wówczas mimo, że występują czynniki ryzyka samego ryzyka nie ma). Podkreślić należy, że takie podejście odbiega od popularnej (głównie w kręgu badaczy anglosaskich) koncepcji ryzyka jako wszelkich, a więc także pozytywnych, odchyleń od funkcji celu.

W tej sytuacji obiektywnie najistotniejszym etapem analizy ryzyka staje się identyfikacja zagrożeń (ang. *threats*). Ryzyko będzie więc efektem realizacji zdarzeń niezależnych (losowych) powstałych jako wynik przypadkowego zdarzenia, lub zagrożeń postrzeganych jako wynik celowego działania. Dla określenia połączonego efektu obu rodzajów zdarzeń, w aplikacjach przemysłowych (także w sektorze energetycznym) używa się terminu zaburzenia (ang. *disturbances*) lub perturbacje (ang. *perturbations*)[10]. Mowa więc o ocenie ryzyka przez pryzmat oceny wrażliwości danego obiektu infrastruktury technicznej na zaburzenia. Proces identyfikacji i zarządzania ryzykiem musi zatem wskazywać na konsekwencje wystąpienia zaburzenia, prawdopodobieństwo ujawnienia się efektów zaburzenia w przypadku, gdy do zaburzenia dojdzie, oraz konsekwencje efektów realizacji ryzyka zainicjowanego zaburzeniem: Warto zwrócić uwagę na rozróżnienie między efektami samego zaburzenia a konsekwencjami efektów jego realizacji. Efekt wystąpienia zaburzenia może być żaden (system charakteryzował się wystarczająca odpornością na zaburzenie) lub może uruchomić ryzyko, dopiero wówczas pojawią się niekorzystne efekty zaburzenia. Przykładowo w energetyce obowiązuje tzw. zasada N-1[11] wedle której każdy z podsystemów infrastruktury powinien być w stanie przetrwać każdorazową awarię jednego elementu, niezależnie od źródła zaburzenia i utrzymać swą sprawność. Jest to koncepcja „uninterruptible power supply" stosowana powszechnie w odniesieniu do instalacji elektrycznych wrażliwych na przerwę w dostawie energii (np. w szpitalach). W powyższym przykładzie zaburzeniem jest zdarzenie, które prowadzi do tego, że jeden z komponentów systemu przestaje działać. Wrażliwość jest następnie definiowana przez możliwe scenariusze. Jeżeli w żadnym z nich nie ma dalszych konsekwencji (dla przytoczonego przykładu oznacza to utrzymanie zasilania), oznacza to, że system nie jest wrażliwy na zaburzenie. Jeżeli system jest wrażliwy (czyli wystąpiła przerwa w zasilaniu), ryzyko jest realizowane i występują efekty negatywne.

Analizując ryzyko dla infrastruktury krytycznej przyjąć należy, że wystąpić może dowolna liczba czynników inicjujących to samo ryzyko (np. zła pogoda, atak terrorystyczny, awaria

[8] M. Dilley, T. Boudreau, *Coming to terms with vulnerability: a critique of the food security definition*, „Food Policy", vol. 26, no. 3/2001, s. 229-247.

[9] P. Buckle, G. Mars, S. Smale, *New approaches to assessing vulnerability and resilience*, „Australian Journal of Emergency Management", vol. 15, no. 2/2000, s. 8-14.

[10] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovic, C. Taylor, T. Van Cutsem, V. Vittal, *Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions*, IEEE Transactions on Power Systems, vol.19, iss.3/2004.

[11] Zob. np.: N.Hadjsaid, J.C.Sabonnadiere, *Power Systems and Restructuring*, Wiley , Hoboken 2009, rozdz.16.6.

urządzenia), które mogą prowadzić do określonych konsekwencji. Pomiędzy zdarzeniem inicjującym a konsekwencjami ryzyka występują zdarzenia lub łańcuchy zdarzeń – stany pośrednie (ang. *middle states*). Dla każdego systemu infrastruktury krytycznej może wystąpić dowolna liczb zdarzeń inicjujących i konsekwencji tych zdarzeń oraz dowolna liczba dróg pośrednich do nich prowadzących. Może też wystąpić kilka zdarzeń inicjujących prowadzących do tego samego stanu końcowego. Analiza ryzyka skupia się więc na zdarzeniach inicjujących oraz stanach końcowych (konsekwencjach). Scenariusze ryzyka powinny zatem opisywać transformację stanu wyjściowego (pożądanego) przez serię stanów pośrednich, aż do stanu końcowego (niepożądanego). Natomiast z punktu widzenia oceny odporności systemu na ryzyko kluczowe stają się stany pośrednie. Droga przejścia od zdarzenia inicjującego do stanu końcowego w teorii systemów określana jest jako odporność systemu (ang. *robustness*) i odzwierciedla pogląd, że idealnym stanem końcowym jest stan początkowy. Odporność systemu pokazuje więc, jak bardzo system potrafi pozostać niezmieniony (lub prawie niezmieniony) pomimo wystąpienia zaburzenia.

Dla wielu systemów infrastruktury idealnym byłoby powrócić do stanu wyjściowego po wystąpieniu zaburzenia, nie jest to jednak zazwyczaj możliwe. W praktyce częściej dojdzie do przekształcenia systemu. Chodzi jednak o to, by możliwe ujemne konsekwencje zdarzeń nie wpłynęły nań negatywnie. Ma się on znaleźć w stanie końcowym odmiennym od początkowego, ale wciąż w stanie pożądanym. Z tym wiąże się pojęcie odzyskiwania równowagi (ang. *resilience*) określające zdolność do przywrócenia funkcji po zaburzeniu[12].

4. Wielowymiarowy model oceny ryzyka w infrastrukturze krytycznej

Teoria systemów odgrywa dla budowy modelu oceny ryzyka w inwestycjach infrastrukturalnych ważną rolę – daje podstawy do przedstawienia go jako funkcji zbioru składowych i odejście od szeroko stosowanych generalizacji na rzecz modelu ryzyka wielopłaszczyznowego. Identyfikacja ryzyka dotyczącego funkcjonowania infrastruktury krytycznej powinna być bowiem prowadzona na kilku płaszczyznach. Bezpośrednie przejawy realizacji danego ryzyka w odniesieniu do danego obiektu infrastrukturalnego będą identyczne, ale ich oddziaływanie będzie odmienne na poziomie strategicznym i operacyjnym. Poziom strategiczny to analiza ryzyka jakie niesie brak działającej infrastruktury krytycznej dla kraju, regionu, gałęzi gospodarki. Poziom operacyjny odnosi się do konsekwencji ponoszonych przez konkretne przedsiębiorstwo. W ocenie ryzyka na poziomie strategicznym zwarty jest więc także wymiar społeczny konsekwencji ryzyka. Przykładowo awaria sieci dystrybucyjnej energii elektrycznej powoduje brak dostępu do energii zarówno gospodarstw domowych jak i przedsiębiorstw. Skutki przerw w dostawach energii elektrycznej na duża skalę w obszarze gęsto zaludnionym i o dużej aktywności gospodarczej zaobserwować można było w amerykańskim stanie Kalifornia w latach 2000-2002. Na poziomie strategicznym było to ryzyko w wymiarze regionalnym. Seria awarii w kluczowych dla dystrybucji energii obiektach uruchomiła mechanizm, który uaktywnił inne rodzaje ryzyka (popytu, finansowe) powodując wzrost cen z 30 USD za megawatogodzinę w kwietniu 2000 r. do 450 USD w listopadzie. W rezultacie nastąpiła seria upadłości przedsiębiorstw energetycznych i konieczność zagwarantowania zakupów energii dla ludności przez władze stanowe, które w tym celu wydatkowały do sierpnia 2001 roku ponad 10 mld USD, podczas gdy od użytkowników końcowych uzyskały jedynie 3 mld USD[13]. Podobnie przykładowe uszkodzenie gazociągów, którymi dostarczany jest gaz do Europy z Rosji miałoby na poziomie strategicznym wymiar narodowy,

[12] E. Hollnagel, D.D. Woods, N. Leveson, *Resilience engineering concepts and precepts*, Ashby Publishing, Aldershot 2006.

[13] J.L. Sweeney, *The California Electricity Crisis*, „The Bridge", vol 32, no 2/ 2002.

a być może nawet transnarodowy, bowiem w przypadku wielu państw UE niemożliwym byłoby szybkie przestawienie się na alternatywne źródła dostaw.

Obie przykładowe awarie miałyby także wymiar operacyjny, mikroekonomiczny, rozpatrywany z punktu widzenia konkretnych przedsiębiorstw zaangażowanych w łańcuch dostaw paliwa gazowego czy dystrybucje energii elektrycznej. Z punktu widzenia przedsiębiorstw zarządzających infrastrukturą istotne byłyby koszty – związane z naprawą infrastruktury, związane z nowymi inwestycjami, czy wreszcie utracone korzyści (ograniczenie sprzedaży) lub koszty wynikające z kar umownych.

Oceniając ryzyko na płaszczyźnie strategicznej trzeba brać pod uwagę:

- ryzyko dotyczące zaburzeń w funkcjonowaniu infrastruktury uznawanej przez władze państwowe za istotne wymiarze ogólnokrajowym,
- ryzyko mające systematyczny, powtarzalny charakter i oddziałujące na inne sektory,
- ryzyko zagrażające lub uniemożliwiające osiągniecie zaplanowanych kluczowych celów rozwojowych,
- ryzyko uniemożliwiające realizację strategicznych celów polityki zagranicznej.

W przypadku pierwszym za kluczowy uznać należy wymiar społeczny ryzyka, a więc możliwość wystąpienia przerw w dostawach mediów do gospodarstw domowych. W drugim – najistotniejsze będą ograniczenia w produkcji zakładów przemysłowych wynikające z przerw w dostawach energii. Trzeci wymiar wynika z możliwego zablokowania rozwoju strategicznych gałęzi gospodarki na skutek niewystarczającego rozwoju infrastruktury krytycznej sektora. Czwarty wymiar dotyczy państw posiadających odpowiednią bazę surowcową i realizujących politykę eksportu surowców energetycznych w zamian za określone koncesje polityczne.

Proces identyfikacji ryzyka na szczeblu operacyjnym powinien natomiast wpisywać się w istniejące mechanizmy zarządzania przedsiębiorstwa odpowiedzialnego za budowę lub zarządzanie daną infrastrukturą krytyczną. Może on posługiwać się szczegółową metodologią dostarczaną przez jedną z aplikacyjnych metod zarządzania ryzykiem opracowanych przez różne ciała doradcze (zob. tabela 2). Niektóre z tych metodyk mają charakter dedykowany dla sektora energii, inne muszą zostać zaadaptowane do specyfiki konkretnych obiektów infrastruktury krytycznej. Alternatywą jest procedura opracowana w sposób autorski, bezpośrednio pod kątem funkcjonowania danego obiektu infrastruktury krytycznej.

Tablica 2. Standardy międzynarodowe zawierające wskazówki w zakresie analizy ryzyka w aplikacjach systemowych

Standard	Organizacja	Miejsce i data wydania
AS/NZS 4360:2004	Risk Management Standards Australia, Homebush NSW 2140, Australia, and Standards New Zealand	Wellington, Nowa Zelandia 2004
BS 6079-3:2000, Project Management. Part 3: Guide to the Management of Business-related Project Risk	British Standards Institution	Londyn, Wielka Brytania 2000
BS 8444-3: 1996 Risk Management. Part 3: Guide to Risk Analysis of Technological Systems	British Standards Institution	Londyn, Wielka Brytania 1996
CAN/CSA-Q850-97, Risk Management Guideline for Decision Makers	Canadian Standards Association	Ontario, Kanada 1997
CP142 Operational Risk Systems and Controls	Financial Services Authority	Londyn, Wielka Brytania 2002
IEEE 1540-2001, Standard for Software Life Cycle Processes. Risk Management	The Institute of Electrical and Electronic Engineers, Inc.	USA 2001

ISO 14001: 2004, Environmental Management Systems. Requirements with Guidelines for Use International Organization for Standardization	International Organization for Standardization	Genewa, Szwajcaria 2004
ISO/IEC 17799:2005, Information Technology. Security Techniques. Code of Practice for Information Security Management	International Organization for Standardization/International Electrotechnical Commission	Genewa, Szwajcaria 2005
IEC 62198:2001, Project Risk Management. Application Guidelines	International Electrotechnical Commission	Genewa, Szwajcaria 2001
JIS Q 2001:2001 (E), Guidelines for Development and Implementation of Risk Management System	Japanese Standards Association	Tokio, Japonia 2001
PAS 56:2003, Guide to Business Continuity Management	British Standards Institution	Londyn, Wielka Brytania 2003
PD 6668:2000, Managing Risk for Corporate Governance	British Standards Institution	Londyn, Wielka Brytania 2000
PD ISO/IEC Guide 73:2002, Risk Management. Vocabulary. Guidelines for Use in Standards	British Standards Institution	Londyn, Wielka Brytania 2002
A Guide to the Project Management Body of Knowledge	Project Management Institute	Filadelfia, USA 2004
A Risk Management Standard Institute of Risk Management (IRM)	Association of Insurance and Risk Managers (AIRMIC) and National Forum for Risk Management in the Public Sector (ALARM)	Londyn, Wielka Brytania 2002
Continuous Risk Management Guidebook	Software Engineering Institute (SEI)	Carnegie Mellon University, USA 1996
Enterprise Risk Management. Integrated Framework	The Committee of Sponsoring Organizations of the Treadway Commission, USA	2004
Guidelines for Environmental Risk Assessment and Management	DETR, Environment Agency and IEH/The Stationery Office	Londyn, Wielka Brytania 2000
Guidelines on Risk Issues The Engineering Council, Management of Risk. Guidance for Practitioners	UK Office of Government Commerce (OGC)/The Stationery Office	Londyn, Wielka Brytania 2002
Project Risk Analysis & Management (PRAM) Guide	Association for Project Management/APM Publishing	High Wycombe, Bucks, Wielka Brytania 2004
Risk Analysis and Management for Projects (RAMP)	Institution of Civil Engineers, Faculty of Actuaries and Institute of Actuaries/Thomas Telford	Londyn, Wielka Brytania 2005
NS 5814:1991, Krav til risikoanalyser	Norges Standardiseringsforbund	Oslo 1991
Association for Project Management Risk	Management Specific Interest Group (APM Risk SIG)	http://www.eurolog.co.uk/APMRiskSIG
Roads to Resilience	Association of Insurance and Risk Managers (AIRMIC)	http://www.AIRMIC.com
EIRM Risk Library	European Institute of Risk Management (EIRM)	http://www.EIRM.com

Professional Standards in Risk Management	Institute of Risk Management (IRM)	http://www.theIRM.org
Standard opublikowany w formie elektronicznej	International Association of Contract and Commercial Managers (IACCM) Business Risk Working Group	http://www.IACCM.com/risk.php
Risk Management Working Group Standard (INCOSE RMWG)	International Council on Systems Engineering	http://www.INCOSE.org
Development and Use of Probabilistic Risk Assessments In Department Of Energy Nuclear Safety Applications	US Department of Energy	Washington 2010
Operational Risk Management in the Energy Industry	Management Solutions	http://www.managementsolutions.com
Risk Assessment Software: Enterprise Risk Management (ERM) in Energy and Utility Industry	MetricStream	http://www.metricstream.com
Electricity Subsector Cybersecurity Risk Management Process	US Department of Energy	Washington 2012

Źródło: opracowanie własne.

Implementacja takiego procesu do specyfiki danej jednostkowo rozpatrywanej infrastruktury krytycznej powinna spełniać założenia przedstawione w normie ISO 31000[14], którą uznać można za ogólną, ale elastyczną platformę oferującą metodologiczne podstawy przygotowania takiego systemu. Po implementacji do infrastruktury krytycznej procedura identyfikacji, oceny i zarzadzania ryzykiem powinna zapewniać:

- aktywne zarządzanie ryzykiem,
- identyfikację zagrożeń,
- identyfikację elementów wrażliwych ujawniających się na skutek interakcji różnych procesów,
- zgodność z normami krajowymi i międzynarodowymi,
- zwiększone zaufanie interesariuszy,
- narzędzie podejmowania decyzji zarządczych
- efektywną alokacje zasobów przeznaczonych na działania ochronne,
- zwiększoną efektywność systemów prewencji zagrożeń i minimalizacji strat
- zwiększoną zdolność systemu do samo naprawy.

Aktywne zarządzanie ryzykiem oznacza koncentrację na wyprzedzającym rozpoznaniu ryzyka i niedopuszczeniu do jego realizacji, w przeciwieństwie do strategii pasywnego – reaktywnego odnoszenia się do istniejącego ryzyka. Dobra identyfikacja zagrożeń oznacza umiejętność trafnej identyfikacji zdarzeń, które potencjalnie prowadzić mogą do powstawania ryzyka. System powinien charakteryzować się zdolnością analizowania ryzyka pojawiającego się na skutek nakładania się procesów. Procesy mogą mieć charakter niezależny (wówczas ryzyko procesów cząstkowych nie będzie podlegało interakcji), mogą mieć charakter synergiczny (wówczas suma ryzyka procesów cząstkowych jest niższa niż ryzyko procesu wynikającego z interakcji) – to właśnie te rodzaje zagrożeń muszą być sprawnie identyfikowane przez wprowadzany system. Wreszcie suma ryzyka procesów podlegających interakcji może być niższa niż ryzyko każdego z tych procesów istniejących niezależnie, te interakcje uznać należy za pozytywne i zmniejszające ogólne ryzyko funkcjonowania infrastruktury krytycznej.

[14] *ISO 31000: Risk management - Principles and guidelines*, International Organization for Standardization, Geneva 2009.

Zgodność z normami zapewnia minimum niezbędnych zabezpieczeń przed ryzykiem (są to np. przepisy p-ppoż., BHP itp.). Z reguły przestrzeganie norm zapewnia jedynie podstawowy, minimalny poziom bezpieczeństwa, a ich działanie musi być wzmocnione procedurami kontroli wewnętrznej. Zwiększone zaufanie interesariuszy dotyczy zarówno interesariuszy wewnętrznych jak i zewnętrznych. Interesariusze wewnętrzni to zarząd, właściciele oraz pracownicy firmy zarządzającej infrastrukturą krytyczną. Zwiększenie ich zaufania prowadzi do poprawy finansowania, lepszego zarzadzania, większej sprawności pracowników (np. dzięki większej wierze w poprawność funkcjonujących procedur zmniejszających ich osobiste narażenie na utratę zdrowia). Interesariusze zewnętrzni reprezentują szerszą grupę. W jej skład wchodzić mogą władze wszystkich szczebli, społeczeństwo, w szczególności mieszkańcy obszarów przyległych do infrastruktury, media. Zapewnienie ich współdziałania ma kluczowe znaczenie dla kwestii związanych z bezpieczeństwem już istniejących obiektów (np. nakłonienie mieszkańców do przestrzegania zasad obowiązujących w strefach ochronnych), może mieć też znaczenie dla lokowani nowych obiektów. Np. częste są protesty mieszkańców wobec planów realizacji dużych inwestycji sektora energii – lokacji nowych elektrowni (zwłaszcza atomowych), prowadzenia napowietrznych linii przesyłowych itd. Wzrost efektywności alokacji zasobów przeznaczanych na ochronę przed ryzykiem powinien prowadzić do maksymalizacji wskaźnika redukcji potencjalnych strat do kosztów tej redukcji. Ta cecha implementowanej platformy zarządzazarządzania ryzykiem powinna więc prowadzić do eliminacji tych działań w przypadku których koszty ochrony przed ryzykiem są wyższe niż koszty realizacji ryzyka. Podobny rachunek efektywności powinien odnosić się do proponowanych mechanizmów prewencji i redukcji strat. Pierwsza grupa narzędzi koncentruje się na niedopuszczeniu do realizacji ryzyka, podczas gdy druga na usuwaniu skutków ryzyka zrealizowanego. Niekiedy tańszym rozwiązaniem może okazać się usuwanie skutków ryzyka niż prewencja. Przykładowo zapewnienie wytrzymałość napowietrznej trakcji elektrycznej na wichury jest sensowne ekonomicznie tylko do pewnego poziomu siły wiatru, powyżej którego inwestycja ze względu na konieczność stosowania bardzo trwałych materiałów nie jest opłacalna w zestawieniu z kosztami napraw zerwanej sieci. Wreszcie promowane powinny być te rozwiązania, które pozwalają na automatyzm reakcji na ryzyko i pozwalają na przerwanie procesu narastania strat. Do takich mechanizmów należą np. rozmaite urządzenia techniczne wyłączające elementy danej infrastruktury w przypadku jej przeciążenia.

Szczegółowa metodologia służąca rozpoznaniu ocenie i wreszcie sformułowaniu rozwiązań redukujących ryzyko w zakresie funkcjonowania infrastruktury krytycznej musi adresować wszystkie wyżej sygnalizowane problemy (zob. tablica 3).

Tablica 3. Obszary kluczowe procedury zarządzania ryzykiem w infrastrukturze krytycznej

Problem	Narzędzia	Aplikacje
Identyfikacja zdarzenia negatywne (co może pójść źle?)	Identyfikacja scenariuszy	Identyfikacja zagrożeń Lista obiektów
Jakie jest prawdopodobieństwo zaistnienia zdarzenia negatywnego? Jakie mogą być konsekwencje zaistnienia zdarzenia negatywnego?	Ocena ilościowa Ocena jakościowa Ocena wielokryteriowa	Procedura zagrożenie – strata Identyfikacja kluczowych elementów infrastruktury Ranking / baza danych zagrożeń Ranking / baza danych skutków Kategoryzacja strat
Co można zrobić? Jakie są efekty uboczne? Jakie są skutki? Jakie zmiany można wprowadzić?	Instrumenty zarządzania ryzykiem	Procedury bezpieczeństwa Analiza kosztów Środki zapobiegawcze Środki ograniczające skutki
Informacja zwrotna	Kontrola	Zmiany procedur/narzędzi

Źródło: opracowanie własne na podstawie: Y.Y. Haimes, J.H.Lambert, S. Kaplan, I. Pikus, F. Leung, A risk assessment methodology for critical infrastructure, VTRC, Charlottensville 2002; Y.Y. Haimes, Total risk management, Risk analysis 19(2)/2001.

Procedury te powinny być wpisane w klasyczny cykl zarządzania ryzykiem, natomiast rozwiązania szczegółowe stają się specyficzne dla konkretnego podsektora w którym mają być zastosowane. Taki system zapewnia z jednej strony wielopłaszczyznowość, z drugiej mieści się w funkcjonalnych i kompatybilnych ramach umożliwiających szybkie tworzenie planów ryzyka na styku dwóch podmiotów. W fazie pierwszej generowane powinny być scenariusze ryzyka przedstawiające możliwe niekorzystne zdarzenia. W praktyce procedura taka prowadzić musi do wyodrębnienia z jednej strony listy zdarzeń, które mogą niekorzystnie wpływać na infrastrukturę, z drugiej pozwala na sporządzenie listy obiektów infrastrukturalnych narażonych na te zdarzenia. Nie każde zdarzenie można powiązać z każdym z obiektów. Lista zdarzeń będzie zapewne szersza niż lista obiektów, niektóre zdarzenia mogą mieć specyficzny, związany z warunkami danej lokalizacji, charakter (np. lokalizacja na obszarze dużej aktywności sejsmicznej, terenach zalewowych itp.), podczas, gdy inne mogą być bardziej uniwersalne.

Scenariusze ryzyka powinny uwzględniać przynajmniej trzy rodzaje konsekwencji (dla płaszczyzny strategicznej jak i operacyjnej):

- mające duże znaczenie ekonomiczne lub społeczne (wpływ na społeczeństwo i gospodarkę),
- mające duży wpływ na podmiot zarządzający lub właściciela infrastruktury,
- wymagające współdziałania wielu podmiotów (np. konieczność zaangażowania różnych służb państwowych w celu likwidacji skutków ryzyka).

Ponieważ liczba możliwych scenariuszy może być dość znaczna, należałoby dokonać ich wstępnej selekcji w oparciu o powszechnie używane narzędzia oceny. Lista możliwych narzędzi jest bardzo rozbudowana i może zawierać różnorodne metody ewaluacji ryzyka takie jak: jakościowe (np.: rankingi, benchmarking, listy, macierze i mapy ryzyka, HAZOP, rating i inne) oraz ilościowe (np.: Monte Carlo, ocena wrażliwości zmiennych krytycznych, VaR i inne)[15].

W procedurach oceny ryzyka dotyczących infrastruktury krytycznej należy wprowadzić dodatkowy etap, który nie jest niezbędny w normalnych procedurach oceny ryzyka np. ekonomicznego, pozwalający na zestawienie siły oddziaływania ryzyka i siły istniejących zabezpieczeń. Wynika to wprost z wymogów bezpieczeństwa. Należy pamiętać, że ocena ryzyka w zakresie infrastruktury krytycznej zawiera w sobie wymiar bezpieczeństwa, który nie jest uwzględniany np. w szacunkach ryzyka finansowego, czy szerzej ekonomicznego. Wymaga to więc wprowadzenia etapu ewaluacji na ile realizacja ryzyka przewidzianego w danym scenariuszu może być ograniczona poprzez istniejące procedury zabezpieczające.

Przykładowo ryzyko zamachu terrorystycznego z użyciem ładunku bombowego może być w takim przypadku odniesione do następujących parametrów wpływających na działanie istniejącego mechanizmu ochrony przed tym ryzykiem:

- niewykrywalność,
- niekontrolowalność,
- możliwe ścieżki zdarzeń prowadzące do unieszkodliwienia mechanizmów ochronnych,
- nieodwracalność,
- czas trwania efektów,
- efekty wtórne,
- środowisko w jakim system funkcjonuje,
- zużycie,
- interfejsy użytkownika (sprzętowe/programowe/osobowe)

[15] P. Borkowski, *Metody obiektywizacji oceny ryzyka w inwestycjach infrastrukturalnych w transporcie,* Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2012, rozdz. 5.1.2 i 5.1.3.

Kryteria powyższe należy traktować jako przykładowe. W zależności od skonkretyzowanego rodzaju ryzyka mogą być one zastąpione innymi lepiej opisującymi możliwe interakcja na linii: istniejące procedury bezpieczeństwa – zagrożenia. Niemniej istotnym jest jak bardzo realizacja ryzyka wpływa na te elementy. Jeżeli oddziaływanie na poszczególne parametry określone zostało jako „wysokie", wówczas dane ryzyko powinno znaleźć się wyżej w rankingu zagrożeń.

Wreszcie faza zarządzania ryzykiem służyć ma wprowadzeniu procedur umożliwiających zapobieganie realizacji scenariusza ryzyka, albo niwelujących jego skutki. Jest to klasyczny element procedury ryzyka znany także z aplikacji dotyczących ryzyka ekonomicznego, ale w przypadku infrastruktury krytycznej większość proponowanych narzędzi opierała będzie się na wprowadzaniu procedur kontrolnych czy fizycznych ulepszeń, rzadko stosowane będą zaś typowo ekonomiczne instrumenty natury finansowej. Zakres i wybór konkretnych narzędzi powinien być zindywidualizowany i dostosowany do wymogów wynikających z charakteru konkretnego obiektu infrastruktury krytycznej.

Podsumowanie

Celem wprowadzenia procedury analizy i zarządzania ryzykiem w zakresie infrastruktury krytycznej powinno być minimalizowanie prawdopodobieństwa realizacji tego ryzyka oraz ograniczenie jego skutków. Metodologia identyfikacji i analizy ryzyka w stosunku do infrastruktury krytycznej może być zróżnicowana i najczęściej odpowiada lokalnym planom i potrzebom zamawiających takie procedury jednostek. Każda tego typu metodologia powinna jednak charakteryzować się kilkoma nieodzownymi cechami.

Po pierwsze system identyfikacji ewaluacji ryzyka w odniesieniu do infrastruktury krytycznej powinien opierać się na narzędziach umożliwiających uwzględnienie zróżnicowanych perspektyw różnych podmiotów zaangażowanych w funkcjonowanie danego rodzaju infrastruktury krytycznej. Jeżeli firmy z sektora energetycznego opracowują własne plany ryzyka, powinny one być sporządzane w sposób gwarantujący porównywalność oraz w sposób umożliwiający współdziałanie na styku ich operacji. W szczególności w odniesieniu do infrastruktury krytycznej takiej jak infrastruktura przesyłowa w miejscach, gdzie łączą się obiekty różnych operatorów. Z tego względu wskazać można na walory podejścia opartego o modele wielowymiarowe w modelowaniu ryzyka infrastruktury.

Po drugie ważne jest rozróżnienie pomiędzy poziomem strategicznym, na którym ryzyko oceniane jest w kontekście interesów państwa oraz mikroekonomicznym, dotyczącym konkretnych podmiotów gospodarczych funkcjonujących w poszczególnych łańcuchach dostaw sektora energii. Po trzecie istotnym ograniczeniem tworzenia procedur dotyczących ryzyka w sektorze jest przeniesienie punktu ciężkości z oceny prawdopodobieństwa wystąpienia danego ryzyka na ocenę skutków jego realizacji oraz zdolność systemu infrastruktury do absorbcji tych niekorzystnych efektów. Implikuje to konieczność dostosowania typologii ryzyka oraz metodologii rozpoznawania zagrożeń. Po czwarte, w zakresie zarządzania ryzykiem istotna będzie specyfika przypadku dla wyboru konkretnych działań, ale procedury nastawione będą przede wszystkim na bezpieczeństwo i zarządzanie kryzysowe.

Literatura

1. Borkowski P., *Kluczowe czynniki ryzyka w sektorze energetycznym*, [w:] *Zarządzanie ryzykiem w działalności gospodarczej: InfoGlobMar 2015*, red. J. Winiarski, D. Wach, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2015
2. Borkowski P., *Metody obiektywizacji oceny ryzyka w inwestycjach infrastrukturalnych w transporcie,* Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2012

3. Buckle P., Mars G., Smale S., *New approaches to assessing vulnerability and resilience*, „Australian Journal of Emergency Management", 2000, vol. 15, no. 2
4. Dilley M., Boudreau T., *Coming to terms with vulnerability: a critique of the food security definition*, „Food Policy", 2001, vol. 26, no. 3
5. *Dyrektywa Rady UE z 8 grudnia 2008 roku w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz potrzeb w zakresie poprawy jej ochrony*, Dziennik Urzędowy Unii Europejskiej L 345 z 23.12.2008.
6. Hadjsaid N., Sabonnadiere J.C.,*Power Systems and Restructuring*, Wiley, Hoboken 2009
7. Haimes Y.Y., Lambert J.H., Kaplan S., Pikus I., Leung F., *A risk assessment methodology for critical infrastructure*, VTRC, Charlottensville 2002
8. Haimes Y.Y., *Total risk management*, „Risk analysis", 2001, vol.19, no. 2.
9. Hollnagel E., Woods D.D., Leveson N., *Resilience engineering concepts and precepts*, Ashby Publishing, Aldershot 2006.
10. *ISO 31000: Risk management - Principles and guidelines*, International Organization for Standardization, Geneva 2009.
11. Kaplan S., Garrick B.J., *On the quantitative definition of risk*, „Risk Analysis", 1981, vol. 1, no. 1.
12. Kundur P., Paserba J., Ajjarapu V., Andersson G., Bose A., Canizares C., Hatziargyriou N., Hill D., Stankovic A., Taylor C., Van Cutsem T., Vittal V., *Definition and classification of power system stability. IEEE/CIGRE joint task force on stability terms and definitions*, „IEEE Transactions on Power Systems", 2004, vol.19, iss.3
13. *Lista Projektów Strategicznych dla infrastruktury energetycznej w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020*, Ministerstwo Gospodarki, Warszawa 2015.
14. Sweeney J.L., *The California Electricity Crisis*, „The Bridge", 2002, vol 32, no. 2
15. *Ustawa z dnia 18 marca 2010 roku o szczególnych uprawnieniach ministra właściwego dla spraw Skarbu Państwa oraz ich wykonywaniu w nie-których spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych*, Dz.U. 2010 nr 65 poz. 404.
16. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*, Dz.U. 2007 Nr 89 poz. 590.
17. Wade W., *Scenario planning. A field guide to the future*, Wiley, Hoboken 2012

DETERMINANTS OF RISK ASSESSMENT PROCESS IN CRITICAL ENERGY INFRASTRUCTURE

Summary

Article deals with the problem of risk assessment in critical energy infrastructure. Firstly the critical infrastructure in energy sector is discussed than risk identification methodology for application to critical infrastructure is proposed. Specific conditions resulting from features of critical infrastructure are addressed in the context of risk assessment procedure. The limits of such a procedure are outlined and critical factors influencing different stages of risk assessment process are researched in view of specificity of the sector.

Keywords: risk assessment for critical energy infrastructure, critical infrastructure, risk in energy sector

Prof. UG, dr hab. Przemysław Borkowski
Uniwersytet Gdański
Armii Krajowej 119/121, 81-824 Sopot
e-mail: przemyslaw.borkowski@univ.gda.pl