RISK ASSESSMENT IN TRANSPORTATION SYSTEMS

OCENA RYZYKA W SYSTEMACH TRANSPORTOWYCH

Marek Młyńczak

Politechnika Wrocławska, Wydział Mechaniczny

e-mail: marek.mlynczak@pwr.wroc.pl

Abstract: *The paper presents problems of hazard identification in transportation systems, where not only field of action is large but also cause-consequences relations between failure causes and losses are distant in time and space. It is observed in transportation systems of goods and passengers, systems of water, gas, oil distribution and electro-energetic nets. Proposed systemic approach based on system elements classification on active (casual) and passive ones (affected). There are described concepts of vulnerability (damageability), resilience (ability of recovering and risk controlling by introducing safety measures to undesired event chain.*

Keywords: *technical system, hazard identification, risk analysis and assessment*

Streszczenie: *W pracy omówiono problemy identyfikacji zagrożeń w systemach transportowych, w których nie tylko obszar działania jest duży, ale też związki przyczynowo - skutkowe pomiędzy przyczynami uszkodzeń, a stratami są odległe w czasie i przestrzeni. Ma to miejsce w systemach transportowych osób i towarów, systemach dystrybucji wody, gazu, ropy naftowej, czy w sieciach elektro-energetycznych. Zaproponowano systemowe podejście bazujące na kategoryzacji systemu na elementy aktywne (przyczynowe) i pasywne (skutkowe). Omówiono pojęcie podatności na zagrożenie (vulnerability), zdolności zdrowienia (resilience) oraz możliwość sterowania ryzykiem poprzez wprowadzanie środków bezpieczeństwa w łańcuchach zdarzeń niepożądanych.*

Słowa kluczowe: *system techniczny, identyfikacja zagrożeń, analiza i ocena ryzyka*

OCENA RYZYKA W SYSTEMACH TRANSPORTOWYCH

1. Wstęp

Bezpieczeństwo systemu transportowego jest stanem tego systemu, w którym ryzyko wynikające ze wszystkich zagrożeń, zarówno zidentyfikowanych jak i ukrytych, jest na poziomie akceptowalnym. System eksploatacji środka transportu, oprócz obiektów technicznych, obejmuje także ludzi i otoczenie, stąd analiza i ocena ryzyka jest złożonym problemem o wielopłaszczyznowym postrzeganiu. W rozpoznawaniu zagrożeń konieczne jest uwzględnienie uszkodzalności obiektów technicznych, błędów ludzi w obszarze użytkowania i obsługi oraz wpływu otoczenia, w którym wyróżnia się zjawiska środowiska naturalnego, jak również osoby postronne i obiekty techniczne w otoczeniu systemu eksploatacji. Można uznać, że zagrożenia są skojarzone z niepoprawnym stanem tych elementów systemu, lub tzw. zdarzeniami niepożądanymi powodującymi przejście systemu do takiego stanu. Wymaga to wówczas wykonania działań przerywających taki łańcuch wypadkowy, które jednak w pewnych sytuacjach mogą być nieskuteczne. Z drugiej strony, końcowe straty w wyniku zaistnienia wypadku obserwuje się w tym samym zbiorze elementów systemu (człowiek, technika, otoczenie). W opracowaniu proponuje się metodę identyfikacji zagrożeń poprzez systemową dekompozycję elementów na aktywne i pasywne ze względu na bezpieczeństwo i kojarzenie możliwości zdarzeń niepożądanych z elementami aktywnymi, a straty z pasywnymi. Macierz relacji wzajemnego wpływu elementów na siebie pozwala na wyznaczenie ryzyka dla wydzielonych elementów systemu. Przedstawione zagadnienie powinno stanowić element wartościowania zmiennych sterujących w metodach utrzymania systemów technicznych i zarządzania ryzykiem.

2. Bezpieczeństwo w systemach transportowych

Bezpieczeństwo w systemach transportowych jest złożonym zagadnieniem, które powinno być postrzegane wielopłaszczyznowo, głównie ze względu na obecność i udział człowieka w funkcjonowaniu takich systemów. Nie bez znaczenia jest także otoczenie systemu obejmujące zarówno środowisko naturalne, jak też „obcą”, niezwiązaną z analizowanym systemem infrastrukturę i ludzi w otoczeniu systemu technicznego.

W literaturze występuje wiele definicji opisujących bezpieczeństwo odnoszących się do obszarów technicznych jak np. [19]: „Bezpieczeństwo jest względnym sposobem oddzielenia od zagrożenia, jest antonimem niebezpieczeństwa” [10], „Bezpieczeństwo jest miarą względnej wolności od zagrożeń... Bezpieczeństwo jest stopniem wolności od zagrożeń w każdym środowisku” [9], „Bezpieczeństwo jest takim sterowaniem zagrożeniami, aby osiągnąć akceptowalny poziom ryzyka” [27], czy też: „Bezpieczeństwo w sensie opisowym jest to stan układu, w którym żaden ze składników (obiekt, człowiek, otoczenie) nie zagraża żadnemu innemu składnikowi tego układu” [25].

Można więc przyjąć, że bezpieczeństwo jest subiektywnym odczuciem, stanem systemu lub umysłu, w którym nie zauważa się lub nie odczuwa potencjalnych, możliwych do zaistnienia strat.

Jako pewną miarę bezpieczeństwa przyjęto w nauce pojęcie ryzyka, jednak zdefiniowaną niezbyt precyzyjnie, równie miękko jak samo bezpieczeństwo. Ryzyko nie jest także ściśle zdefiniowane w podstawowej normie poświęconej zarządzaniu ryzykiem [21]. Definicję ryzyka przyjęto w postaci liczbowej „kombinacji”, najczęściej iloczynu, możliwości wystąpienia strat i ich wielkości.

Ryzyko odnosi się do tzw. zdarzeń niepożądanych, tj. takich, których następstwem są straty, szkody, ujemne skutki, zwykle określanych jako wypadek, katastrofa, awaria, itp. Wypadki są zdarzeniami nagłymi, niezamierzonymi, powodującymi śmierć, zranienia, straty materialne, straty ekonomiczne, straty moralne, wizerunkowe, skażenie środowiska naturalnego, itp.

3. Metodyka badania bezpieczeństwa

Badanie bezpieczeństwa, a właściwie ocena ryzyka w systemach technicznych została wszechstronnie opisana w literaturze i opracowaniach normowych [21, 23, 31]. Na rys. 1 przedstawiono rozwój zdarzeń prowadzących od zagrożenia do wystąpienia strat. W odniesieniu do kolejnych etapów analizy takiego procesu opracowano wiele wspomagających metod analitycznych odnoszących się do identyfikacji zagrożeń, rozwoju zdarzeń, analizy i oceny ryzyka oraz oceny strat [12].

Rys. 1. Rozwój zdarzenia niepożądanego

Duże znaczenie zaczęto także przywiązywać w technice do pojęcia podatności na uszkodzenie, „zranialności” czy „wrażliwości” (vulnerability) [22] oraz zdolności powrotu do stanu zdolności funkcjonalnej, tj. „odporności, zdolności zdrowienia” (resilience) [1, 11]. Pojęcia te wywodzące się z nauk socjologicznych zaczęto wdrażać do nauk technicznych w odniesieniu do wielostanowego podejścia do bezpieczeństwa systemów socjo-technicznych. Na rys 2. pokazano sytuacje systemów o różnym poziomie jakości (wyższym potencjale) i ich stanie po wystąpieniu zakłócenia. System o wyższej jakości jest bardziej odporny na zakłócenia, łatwiej powraca do poprawnego stanu działania, szybciej odparowuje zakłócenia.

Rys. 2. Ilustracja podatności i odporności [opracowanie własne na podstawie <http://practicalaction.org/from-vulnerability-to-resilience>]

Klasyfikacja różnych systemów pod względem ich podatności na zakłócenie i odporność (dwuwartościowo) (rys. 3) pozwala na wyodrębnienie i ocenę systemów w czterech grupach. Najlepszy jest system o dużej odporności i małej podatności na zakłócenia (I), najgorszy, odwrotnie o dużej podatności i małej odporności (IV). Przypadek II odnosi się do systemu z wykształconą odpornością przygotowanego na przetrwanie w przypadku pojawienia się zakłócenia. Przypadek III to „szczęśliwy” system o małej podatności na zakłócenia i bez wykształconej odporności z powodu braku zakłóceń (system nienarażany na zakłócenia). Uważa się, że podatność (vulnerability) jest wewnętrzną cechą systemu niezależną od tego czy zakłócenia pojawiają się, czy nie, natomiast odporność jest cechą dynamiczną, która wyzwala działania obronne po wystąpieniu zakłócenia.

Podatność (vulnerability) jest stopniem wrażliwości systemu i określane było jako: „ekonomiczna” kruchość systemu lub brak odporności w stosunku do sił zewnętrznych (resilience) [4, 20], stan bezbronności, brak zabezpieczeń i wystawienie na zakłócenia i wstrząsy [30]. Podatność zdefiniowano też jako odwrotność tolerancji uszkodzeń [16].

Rys. 3. Scenariusze rozwoju bezpieczeństwa systemów
Opracowanie własne na podst. [14]

Podatność jest skłonnością systemu do znaczących przekształceń (degradacji) w wyniku interakcji z wewnętrznymi lub zewnętrznymi zakłóceniami. Głównymi czynnikami wpływającymi na tą podatność są: narażenie, wrażliwość i wewnętrzna zdolność do obrony [8]. Narażenie (exposure) może być wyrażone przez: stopień, zasięg lub czas działania zakłócenia. Wrażliwość (sensitivity) jest wewnętrzną cechą systemu i odnosi się do stopnia jego transformacji pod wpływem zakłócenia. Im większa zmiana systemu tym większa jego wrażliwość.

Zdolność do obrony, odprowadzania zakłócenia (Adaptive Capacity), to zdolność systemu do przystosowania się do zakłócenia, pochłaniania i radzenia sobie ze skutkami zakłócenia, wreszcie zdolność wykorzystania zakłócenia. Zdolność ta charakteryzowana jest [6] jako zdolność systemu do odpowiedzi na zmiany w zewnętrznym otoczeniu i do odzyskania zdolności struktury wewnętrznej systemu. System może przejawiać tę zdolność poprzez [3]:

- wykorzystanie istniejących zasobów do rozwiązania problemu, w ujęciu technicznym np. rezerwowanie strukturalne,
- wykorzystanie istniejących sposobów działań ochronnych, ale w innym kontekście, w ujęciu technicznym np. przeniesienie „miękkich” środków bezpieczeństwa takich jak regulacje prawne, instrukcje, szkolenia, organizacja i zarządzanie do innych systemów,
- opracowanie nowych sposobów działania, w ujęciu technicznym np. modernizacja systemu eksploatacyjnego w zakresie techniki i zarządzania.

Odporność (resilience), w stosunku do systemów socjologicznych lub ekologicznych, określa się jako zdolność do pochłaniania zakłóceń poprzez utrzymanie struktury, sposobu i potencjału działania, możliwości działania pod wpływem zakłócenia [20].

Leveson [15] modyfikuje definicję tej odporności w ujęciu zdolności systemu do kontynuacji działania lub odzyskania stabilnego stanu po wystąpieniu znacznego zakłócenia lub zdarzenia niepożądanego poprzez uwzględnienie także zapobieganie zakłóceniom.

System, aby być bezpiecznym, powinien być odporny tj. unikać uszkodzeń i strat, jak również właściwie reagować na zakłócenia.

Odporność w odniesieniu do systemów logistycznych jest trójką $Res = \langle SE, SU, RE \rangle$ zdefiniowaną przez: zabezpieczenie systemu (security), zdolność przetrwania, zdolność do realizacji zadania (survivability) oraz zdolność odbudowy systemu (recovery) [5].

Odporność techniczna odnosi się do sposobu traktowania bezpieczeństwa, które odchodzi od konwencjonalnego zarządzania ryzykiem na rzecz poprawy zdolności systemu do monitorowania i usprawniania modeli ryzyka, tworzenia elastycznych i skutecznych procesów bezpieczeństwa oraz wykorzystania zasobów proaktywnie w stosunku do potencjalnych zakłóceń. Wypadki czy katastrofy nie są postrzegane w odporności technicznej, jako uszkodzenia systemu, a raczej jako brak adaptacji systemu w utrzymaniu działania. Stosownie do teorii sterowania, dynamiczna stabilność systemu, obiekty, organizacje, zespoły muszą zawsze dostosowywać ich działania do bieżących warunków. Ponieważ zasoby i horyzont działania jest skończony, to oczywiste jest, że takie dostosowywanie jest przybliżone i obciążone dodatkowym ryzykiem [7].

Odporność jest właściwością system do dostosowania funkcjonowania przed, w trakcie i po wystąpieniu zmian i zakłóceń tak, aby utrzymać wymagane działanie w przypadku zarówno oczekiwanych jak i nieoczekiwanych warunków zewnętrznych [1, 7, 11].

Generalne wnioski wynikające z przeglądu stanu pojęć PODATNOŚĆ (vulnerability) i ODPORNOŚĆ (resilience) wskazują, że:

- odporny system jest mniej podatny niż nie odporny, ale relacja odwrotna nie jest symetryczna (rys. 3),
- odporność odnosi się do zdolności do obrony (adaptive capacity) będącej cechą podatności, ale odporność zawiera się również w zdolności do obrony,
- odporność nie odnosi się ściśle do wrażliwości systemu, ponieważ wrażliwy system może być odporny lub nie,
- niewrażliwy system może przejawiać niską podatność jak również niską odporność („system uzbrojony”),
- wrażliwy system może być podatny na zakłócenia, ale niewrażliwy system może być niezdolny do odparcia zakłócenia,
- odporność nie obejmuje ekspozycji (narażenia), jednak znajomość historii zakłóceń może być istotna w tworzeniu resilience.

Poglądowo, można też wyrazić ryzyko, jako resztkową odporność systemu po wystąpieniu zakłócenia i pozostającą po wykorzystaniu na odparowanie zakłócenia (rys. 4). Propozycją miary vulnerability jest stosunek wydajności (efektywności) systemu po wystąpieniu zakłócenia do wydajności niezakłóconej.

Rys. 4. Ryzyko jako różnica podatności i odporności systemu na zakłócenie
[Opracowanie własne na podstawie [14]]

Formalnie, ryzyko jest miarą wyrażoną liczbowo wiążącą możliwość (intensywność) wystąpienia zdarzenia niepożądanego oraz wielkość strat wynikających z tego zdarzenia. Ponieważ ciąg postępujących po sobie zdarzeń prowadzących do wypadku jest w większości losowy, konieczne jest też uwzględnienie prawdopodobnych scenariuszy takiego łańcucha zdarzeń. Należy więc przyjąć, że zagrożenie pobudzone zdarzeniem inicjującym, w zależności od różnych scenariuszy spowoduje różne straty, a w konsekwencji będzie charakteryzowane ryzykiem obejmującym wszystkie potencjalne skutki. Ryzyko opisuje trójka [13, 28] (1):

$$RS = \langle S_i, L_i, C_i \rangle \quad (1)$$

gdzie:

- S_i – scenariusz rozwoju wydarzenia niepożądanego od zagrożenia do strat,
- L_i – możliwość wystąpienia i -tego scenariusza prawdopodobieństwo odniesione do czasu lub częstotliwość),
- C_i – potencjalne straty wynikające ze zdarzenia niepożądanego [18, 23].

Źródłem strat jest zwykle energia, której uwolnienie w wyniku uszkodzenia, błędu człowieka działania czynników środowiskowych. Straty wynikające z wypadków i katastrof mogą być klasyfikowane według wielu kryteriów związanych z systemowym podziałem analizowanego systemu i powinny obejmować:

- straty związane z życiem i zdrowiem człowieka: (śmierć: liczba ofiar, wiek ofiary), zranienie, kalectwo (utrata sprawności fizycznej), cierpienie,
- straty w środowisku naturalnym (np. równoważne karom administracyjnym): zniszczenie fauny, flory, zanieczyszczenie, skażenie wody, gleby, powietrza,
- straty ekonomiczne: uszkodzenie środków trwałych skutkujące w konieczności naprawy, wymiany (koszty napraw), strata potencjalnej produkcji, niewykonanych usług (np. koszt wynajmu środków zastępczych), straty informacji (koszt obniżonej efektywności działania, opóźnienia), straty renomy, reputacji, dobrego imienia (długotrwałe koszty obniżenia zysków).

4. Identyfikacja zagrożeń

Pełny i racjonalny opis scenariuszy wypadków jest kluczowym elementem zarządzania ryzykiem, bowiem rozpoznanie źródeł i możliwy rozwój i przebieg wydarzeń daje możliwość wprowadzenia środków bezpieczeństwa (podwyższenie vulnerability) lub przygotowania aktywnego odparowania (resilience). Scenariusz rozwoju wydarzenia niepożądanego wiąże zdarzenia bazowe ze zdarzeniem wypadkowym. Metoda klasyfikacji obiektów pozostających względem siebie w pewnej relacji ze względu na bezpieczeństwo pozwala na bardziej efektywną identyfikację zagrożeń, to jest taką, w której obok zagrożeń wcześniej opisanych, powszechnie znanych wynajduje się zagrożenia dotąd ukryte, nieujawnione, wymagające wprowadzenia barier ochronnych. To inne spojrzenie na identyfikację zagrożeń polega na skojarzeniu źródeł wypadków z obiektami, czy elementami systemu ponoszącymi straty. Wszystkie elementy systemu eksploatacji takie jak: analizowany obiekt, operator, obsługownik, specyficzna infrastruktura użytkowania i obsługiwanie, przewożona lub przetwarzana materia oraz otoczenie systemu mogą być zarówno przyczyną strat jak i ponosić straty w wyniku wypadku. Stąd obiekty te nazywa się aktywnymi (źródło strat) i pasywnymi (odbiorcy strat). Obiekty te mogą być znacznie oddalone od siebie, zarówno w przestrzeni (np. huraganowy wiatr – zerwanie sieci energetycznej – brak zasilania w szpitalu) jak i w czasie (np. wyciek radioaktywny – choroba popromienna). Identyfikacja zagrożeń może też penetrować najbliższe relacje konstrukcyjne, funkcjonalne w obrębie jednego obiektu (np. zerwanie śruby mocowania silnika-brak napędu). Stąd uszczegółowienie schematu pokazanego na rys. 1 i wyodrębnienie pojedynczej relacji przyczyna-skutek w scenariuszu utraty bezpieczeństwa. Na rys. 5 przedstawiono zdarzenie zmiany stanu bezpieczeństwa elementarnego systemu wywołanego zakłóceniem. Stanem bezpieczeństwa jest stan systemu, w którym parametrem krytycznym jest wielkość strat wynikających z dowolnego zakłócenia. W skali dwuwartościowej system może być bezpieczny (straty akceptowalne) lub niebezpieczny (straty nieakceptowalne). W dowolnym stanie procesu eksploatacji można wyróżnić własną odporność systemu na zakłócenia odpowiadającą pojęciu vulnerability (wbudowana, zaprojektowana, bariera fizyczna, informacyjna, itp.) oraz aktywne bariery inicjowane symptomami bezpieczeństwa (automatyczne systemy bezpieczeństwa, bezpieczniki, reakcja operatora, itp.). Zakłócenie (zewnętrzne, wewnętrzne) wpływa na stan systemu poprzez zmianę parametrów i, jeśli jest to możliwe, odbierane jest to w postaci symptomu bezpieczeństwa (alarm, obserwowalna zmiana przebiegu procesu, dezaktywacja funkcji). W przypadku, jeśli odporność systemu na zakłócenie jest nieskuteczna lub reakcja w postaci uruchomienia aktywnej bariery jest opóźniona lub niewystarczająca, dochodzi do kolejnej zmiany stanu bezpieczeństwa (system nie jest wystarczająco odporny – nie jest resilient).

Proces zmiany stanu bezpieczeństwa zależy więc od:

- bieżącego stanu systemu (vulnerability),
- zakłócenia (postaci, zasięgu, wielkości),
- aktywnych podsystemów obrony (resilience),
- czasu (chwila wystąpienia zakłócenia, czas trwania, czas reakcji, itp.),
- możliwości pozyskiwania informacji, ich niepewności i przepływu (diagnostyka).

Rys. 5. Schemat zmiany stanu bezpieczeństwa systemu

Analiza eksploatacyjna dowolnego systemu działania identyfikuje: obiekt działania, podmiot działania (człowiek) oraz otoczenie eksploatacji [24]. Są to trzy grupy obiektów obejmujących: człowieka, system techniczny i otoczenie. Analiza obiektowa klasyfikuje w każdej z tych grup obiekty o różnej funkcji spełnianej w trakcie eksploatacji. Analiza obiektowa dzieli elementy systemu eksploatacji na dwie grupy:

- obiekty systemowe, ogólnie pojmowane encje bez określonego związku z systemem działania (człowiek, obiekt techniczny, otoczenie),
- obiekty eksploatacyjne mające istotne znaczenie dla eksploatacji (system eksploatacji, łańcuch eksploatacji, otoczenie eksploatacji).

Kryterium obiektowe wyróżnia w systemie eksploatacji różnego rodzaju obiekty (encje): obiekty techniczne oraz inne obiekty, w tym człowieka i elementy środowiska naturalnego. Zarówno człowiek, jak też obiekty techniczny i otoczenie, to nie pojedyncze elementy systemu eksploatacji, a zazwyczaj grupy obiektów.

Człowiek nie występuje w eksploatacji tylko jako użytkownik czy obsługownik, ale pojawia się tu także jako pasażer środka transportu, klient w punktach usługowych, przechodzień czy spacerowicz niezwiązany bezpośrednio z obiektami eksploatacji, jednak mogący wpływać na przebieg tej eksploatacji nieświadomie lub świadomie. Osoby postronne mogą być także potencjalnymi poszkodowanymi w przypadku uszkodzenia systemu technicznego lub też sprawcami awarii systemu. Podobnie, otoczenie eksploatacji należy zróżnicować jako aktywnie biorące udział w eksploatacji lub bierne otoczenie naturalne, także mogące wpływać na eksploatację [29, 32].

W najszerszym postrzeganiu eksploatacji należy wyróżnić następujące encje:

- człowiek: jako użytkownik, obsługownik, osoba postronna, ale biorąca udział w eksploatacji, osoba postronna nie związana bezpośrednio z eksploatacją, jednak potencjalnie wpływająca na eksploatację poprzez jego relację z otoczeniem eksploatacji,
- obiekt techniczny, jako: pośrednik lub przedmiot działania,
- otoczenie, jako: infrastruktura techniczna niezbędna do realizacji eksploatacji (infrastruktura użytkowania i obsługi), tzw. wsparcie logistyczne eksploatacji, infrastruktura techniczna nie biorąca udziału w eksploatacji, środowisko naturalne.

Szczegółowy wykaz elementów eksploatacji sklasyfikowanych wg powyższej zasady oraz powiązanych ze sobą przedstawia tab. 1.

Człowiek odgrywa tu szczególną, podmiotową rolę w procesie sterowania i zarządzania eksploatacją. Jest on także często przyczyną niepoprawnych działań i sprawcą błędnych decyzji powodujących w rezultacie uszkodzenia systemów, awarie i katastrofy [26]. Są to najczęściej błędy stanowiące reakcję na zdarzenia inicjujące wymagające tak zwanego „odparowania” przerywającego łańcuch przyczynowo-skutkowy (rys. 1).

Źródeł strat w analizie ryzyka można poszukiwać zgodnie z powyższą klasyfikacją obiektów (tab. 1). Wskazuje to na trzy obszary przyczyn zakłóceń, uszkodzeń czy awarii. Najważniejszą grupą przyczyn są błędy człowieka, drugą grupą są przyczyny natury technicznej (pierwotne, wtórne, degradacyjne, przypadkowe, itp.), a trzecią przyczyny generowane w środowisku naturalnym (zmienne zjawiska klimatyczne i pogodowe).

Tab. 1. Klasyfikacja encji w eksploatacji obiektu technicznego

Kryterium klasyfikacji		Obiekty w ujęciu eksploatacyjnym		
		Baza eksploatacyjna	Łańcuch eksploatacji	Otoczenie eksploatacji
Obiekty w ujęciu systemowym	Człowiek	uczestnik eksploatacji, np. pasażer jako ładunek	użytkownik, obsługownik	osoba postronna związaną z eksploatacją poprzez jej relację z otoczeniem
	Obiekt techniczny	infrastruktura techniczna niezbędna do realizacji eksploatacji, materiał, ładunek	ANALIZOWANY OBIEKT TECHNICZNY	infrastruktura techniczna nie biorąca udziału w eksploatacji
	Otoczenie	środowisko (warunki geo-meteorologiczne)	otoczenie łańcucha eksploatacji	środowisko naturalne

Źródło: opracowanie własne

5. Przykład zastosowania metody oceny ryzyka w transporcie

Identyfikacja zagrożeń

Koncepcja aktywnych i pasywnych bezpieczeństwo elementów pozwala na wydzielenie z systemu dwóch grup elementów:

$$OEA = \langle EA, W(EA), R_{AW} \rangle, \quad OEP = \langle EP, W(EP), R_{PW} \rangle.$$

gdzie:

- EA, EP – zbiory aktywnych i pasywnych elementów systemu,
- $W(.)$ – zbiór atrybutów elementów,
- RAW, RWP – zbiór relacji między elementami.

Przykładowa lista obiektów tworzących wydzielony fragment systemu transportowego (przejazd kolejowy) może obejmować takie elementy systemu jak: dróżnik przejazdowy, zapory, układ ostrzegawczy świetlny, układ ostrzegawczy dźwiękowy, przejeżdżające pojazdy drogowe i kolejowe, piesi, budowle inżynieryjne tworzące infrastrukturę przejazdu, roślinność, budowle w pobliżu przejazdu, urządzenia energetyczne w pobliżu przejazdu, itp. Identyfikację zagrożeń rozpoczyna intuicyjna analiza dwustronnych relacji między aktywnymi i pasywnymi obiektami. Pomocne mogą tu być takie narzędzia analityczne jak: FTA, ETA, CCA i inne [12,18,19]. Przykład macierzy relacji między elementami aktywnymi i pasywnymi pokazano w tabeli 2.

Tab. 2. Tabela możliwości wpływu elementów aktywnych na pasywne

		Obiekty pasywne						
		Zapory	Dróżnik	Piesi	Pojazdy drogowe	Pojazdy kolejowe	Obiekty inżynieryjne	Roślinność (drzewa)
Obiekty aktywne	Zapory	0	0	1	1	1	0	0
	Dróżnik	0	0	1	1	1	0	0
	Piesi	0	0	0	1	1	0	0
	Pojazdy drogowe	1	0	1	1	1	1	1
	Pojazdy kolejowe	0	0	1	1	1	1	1
	Obiekty inżynieryjne	0	0	0	1	1	0	0
	Roślinność (drzewa)	1	1	1	1	1	1	1

Macierz ryzyka

Na podstawie relacji przedstawionych w tab. 2 można utworzyć dwie macierze stanowiące podstawę miary ryzyka, tj. macierz możliwości wystąpienia strat (L(EA)) oraz macierz wielkości możliwych strat (C(EA)). Macierze te mogą być wypełnione zarówno wielkościami bezwzględnymi jak i względnymi (punktowymi) jak to mam miejsce w metodzie PHA [12]. W niniejszym przykładzie przyjęto czterostopniową skalę możliwości:

- 1 – mało prawdopodobne ($>0,001$),
- 2 – rzadkie ($>0,01$),
- 3 – prawdopodobne ($>0,1$),
- 4 – bardzo prawdopodobne ($>0,2$)

oraz czterostopniową skalę strat:

- 1 – nieistotne (bez wpływu na funkcję obiektu i zdrowie),
- 2 – znaczne (utrata funkcji obiektu, zanieczyszczenie środowiska naturalnego),
- 3 – bardzo duże (utrata zdrowia, zniszczenie obiektu),
- 4 – katastrofalne (utrata życia, obiektu).

W tabelach 3 i 4 pokazano przykładowe wartości czynników ryzyka, a w tab. 5 wartości punktowe oszacowanego ryzyka.

Tab. 3. Macierz możliwości spowodowania strat w elementach pasywnych

		Obiekty pasywne						
		Zapory	Dróżnik	Piesi	Pojazdy drogowe	Pojazdy kolejowe	Obiekty inżynieryjne	Roślinność (drzewa)
Obiekty aktywne	Zapory	0	0	3	3	3	0	0
	Dróżnik	0	0	3	3	3	0	0
	Piesi	0	0	0	1	1	0	0
	Pojazdy drogowe	1	0	1	1	2	1	1
	Pojazdy kolejowe	0	0	1	3	0	0	0
	Obiekty inżynieryjne	0	0	0	1	1	0	0
	Roślinność (drzewa)	1	1	1	1	1	1	1

Tab. 4. Macierz wielkości strat elementów pasywnych wywołanych przez element aktywne

		Obiekty pasywne						
		Zapory	Dróżnik	Piesi	Pojazdy drogowe	Pojazdy kolejowe	Obiekty inżynieryjne	Roślinność (drzewa)
Obiekty aktywne	Zapory	0	0	3	3	2	0	0
	Dróżnik	0	0	3	3	2	0	0
	Piesi	0	0	0	3	4	0	0
	Pojazdy drogowe	2	0	3	2	2	1	1
	Pojazdy kolejowe	0	0	4	4	0	0	0
	Obiekty inżynieryjne	0	0	0	1	1	0	0
	Roślinność (drzewa)	2	3	3	2	2	2	1

Tab. 5. Macierz ryzyka

		Obiekty pasywne						
		Zapory	Dróżnik	Piesi	Pojazdy drogowe	Pojazdy kolejowe	Obiekty inżynieryjne	Roślinność (drzewa)
Obiekty aktywne	Zapory	0	0	9	9	6	0	0
	Dróżnik	0	0	9	9	6	0	0
	Piesi	0	0	0	3	4	0	0
	Pojazdy drogowe	2	0	3	2	4	1	1
	Pojazdy kolejowe	0	0	4	12	0	0	0
	Obiekty inżynieryjne	0	0	0	1	1	0	0
	Roślinność (drzewa)	2	3	3	2	2	2	1

Ocena ryzyka

Na podstawie wartości ryzyka różnych od 0 pokazanych w tab. 5, sporządzono wykaz zagrożeń w porządku malejącego ryzyka (tab. 6). Zagrożenia te poddano ocenie pod względem akceptowalności ryzyka porównując odpowiednie wartości ryzyka z wartościami zestawionymi w tab. 7.

Tab. 6. Wykaz zagrożeń

lp.	Opis zagrożenia	Ryzyko	lp.	Opis zagrożenia	Ryzyko
1.	Pociąg uderza w pieszego	12	14.	Pojazd drogowy uderza w zapory	2
2.	Uszkodzona roгатka, pieszy wkracza na otwarty przejazd	9	15.	Pojazd drogowy uderza w inny pojazd drogowy	2
3.	Uszkodzona roгатka, pojazd drogowy wjeżdża na otwarty przejazd	9	16.	Uszkodzony obiekt inżynieryjny zakłóca bieg pociągu	2
4.	Dróżnik nie opuścił zapór, kolizja pieszy-pociąg	9	17.	Drzewo uszkadza pieszego	2
5.	Dróżnik nie opuścił zapór, kolizja pojazd-pociąg	9	18.	Drzewo uszkadza pociąg	2
6.	Uszkodzona roгатka, pojazd kolejowy wjeżdża na otwarty przejazd	6	19.	Drzewo uszkadza pojazd drogowy	2
7.	Dróżnik nie opuścił zapór, kolizja pociągu z innym obiektem	6	20.	Pojazd drogowy uderza w obiekt inżynieryjny	1
8.	Pieszy narusza roгатki, kolizja z pojazdem kolejowym	4	21.	Pojazd drogowy uderza w drzewo	1
9.	Pojazd drogowy uderza w pociąg	4	22.	Uszkodzony obiekt inżynieryjny zakłóca ruch poj. drogowego	1
10.	Pieszy narusza roгатki, kolizja z pojazdem kołowym	3	23.	Pociąg uderza w pojazd drogowy	1
11.	Pojazd drogowy uderza w pieszego	3	24.	Drzewo uszkadza obiekt inżynieryjny	1
12.	Drzewo uszkadza zapory	3	25.	Drzewo uszkadza inne drzewa	1
13.	Drzewo uszkadza dróżnika	3			

Tab. 7. Macierz akceptacji ryzyka

MOŻLIWOŚĆ	STRATY				
		1	2	3	4
	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Zagrożenia scharakteryzowane ryzykiem wyższym niż 6 są nieakceptowalne, natomiast mające wartości 4 i 6 odpowiadają obszarowi ALARP tj. możliwa jest ich bardziej wnikliwa analiza i przyjęcie lub odrzucenie w zależności od nadrzędnych kryteriów takich jak opłacalność czy niemożność wpływania na ryzyko.

W przedstawionym przykładzie zarządzanie ryzykiem powinno być ukierunkowane na zdarzenia 1-5 jako nieakceptowalne, a zdarzenia 6 i 7 mogą być tolerowane po wykonaniu dodatkowej, bardziej wnikliwej analizy kosztów środków bezpieczeństwa i potencjalnych zysków.

6. Podsumowanie

Odporność techniczna (Engineering Resilience) jest narzędziem umożliwiającym w miarę możliwości autonomiczne „radzenie” sobie z przeciwnościami (zakłóceniami), sposobem przewidywania efektów ubocznych w przypadku zmiany ryzyka, celowym zarządzaniem środkami/zasobami, głównie technicznymi dla poprawy dostosowania systemu do potencjalnych zakłóceń. Odporność w sensie technicznym odnosi się do przygotowania systemu działania na zakłócenia i utrzymania funkcjonowania w sensie nadrzędnego kryterium, np. zdolności, wydajności, efektywności, sprawności, na wymaganym poziomie. Wymaga więc opracowania miar odporności systemu na zakłócenia, narzędzi organizacyjnych i technicznych do odparcia zakłócenia oraz sposobów przewidywania ewentualnych niepoprawnych stanów systemu i możliwości powrotu do stanu stabilnego. Oryginalna metoda identyfikacji zagrożeń oparta na podziale obiektów na aktywne i pasywne ułatwia ten proces i odkrywa dodatkowe obszary poszukiwań zagrożeń.

7. Literatura

- [1] A White Paper on Resilience Engineering for ATM. European Organisation for the Safety of Air Navigation (EUROCONTROL). September 2009
- [2] Adolph L., Lafrenz B., Grauel B., Safety Management Systems, Safety Culture and Resilience engineering: Comparison of Concepts. Proceedings of the Human Factors and Ergonomics Society Europe Chapter 2015 Annual Conference. Groningen. 2015.
- [3] Bernard St. G., Social Vulnerability Measurement in the Caribbean Sub-Region – A Pilot Test. XXV IUSSP International Population Conference. Tours, 2005.
- [4] Briguglio L., Small Islands State and their Economic Vulnerabilities. World Development no. 23(9), 1993.
- [5] Bukowski L.A., Feliks J., Fuzzy logic expert system for supply chain resilience modelling and simulation. Proceedings of Critical Infrastructures Preparedness: Status of Data for Resilience Modelling, Simulation and Analysis (MS&A). ESReDA 48. Wrocław, 2015.
- [6] Dalziel E.P., McManus S.T., Resilience, Vulnerability, and Adaptive Capacity: Implications for System Performance.
- [7] Dekker S., Hollnagel E., David Woods, Cook R., Resilience Engineering: New directions for measuring and maintaining safety in complex systems. Final Report. Lund University School of Aviation. 2008.
- [8] Gallopin G., Linkages Between Vulnerability, Resilience, and Adaptive Capacity. Workshop “Formal Approach To Vulnerability”. Potsdam Institute for Climate Impact Research. Potsdam, 2007.
- [9] Gloss D.S., Wardle M.G., Introduction to Safety Engineering. John Wiley & Sons, 1984
- [10] Hammer W., Occupational Safety Management and Engineering, Prentice-Hall, New York, 1989.
- [11] Hollnagel E., Human Reliability Analysis; Context and Control. Academic Press, London, 1993.
- [12] ISO/IEC 31010:2009 Ed. 1.0: Risk Management – Risk Assessment Techniques.
- [13] Kaplan, S., Garrick, B.J., On the quantitative definition of risk. Risk Analysis 1 (1), 1981.
- [14] Laguardia J.M., Vulnerability and Resilience. Small States in the Global System. Institute of International Relations, University of The West Indies. Kingston, 2014

- [15] Leveson N., Dulac N., Zipkin D., Cutcher-Gershenfeld J., Carroll J., Barrett B. Engineering resilience into safety-critical systems. Resilience Engineering—Concepts and Precepts. Ashgate Aldershot, MIT. 2006.
- [16] Lind N.C., A measure of vulnerability and damage tolerance. Reliability Engineering and System Safety (48), 1995.
- [17] Młyńczak M., Basics of risk assessment in land transportation. in: „Analiza ryzyka w transporcie i przemyśle”, Navigator no. 6, Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław 1997.
- [18] Młyńczak M., Methodology of field test of mechanical objects. Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław 2012.
- [19] Młyńczak M., Metodyka analizy ryzyka transportowego w przestrzeni miejskiej. w: Transport zrównoważony. Jako czynnik tworzący przestrzeń miejską. Monografia Texter. Warszawa 2011.
- [20] Parry M., Canziani O., Palutikof J.: Climate Change Vulnerability and Resilience: Current Status and Trends for Mexico. Climate Change 2007: Impacts, Adaptation and Vulnerability. Workgroup II Contribution to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press, 2008.
- [21] PN-ISO 31000:2012. Zarządzanie ryzykiem Zasady i wytyczne
- [22] Principles, System Representation & Risk Criteria. JCSS (Joint Committee on Structural Safety)
- [23] Rausand M., System Reliability Theory. John Wiley & Sons, Inc. New York 2004.
- [24] Sadowski W., Basics of General System Theory (in Polish). PWN. Warszawa 1978.
- [25] Smalko Z., Studium terminologiczne inżynierii bezpieczeństwa transportu. Navigator nr 21. Oficyna Wydawnicza Politechniki Wrocławskiej. Wrocław, 2010.
- [26] Todinov M.T., Risk-Based Reliability Analysis and Generic Principles for Risk Reduction. Elsevier Science & Technology Books. 2006.
- [27] U.S. National Safety Council (<http://www.nsc.org/>)
- [28] Wall K.D., The Kaplan and Garrick Definition of Risk and its Application to Managerial Decision Problems. Dudley Knox Library. Monterey, 2011.
- [29] Wasson C.S., System Analysis, Design and Development. John Wiley & Sons, Inc. Hoboken 2006.
- [30] Wratten, E., Conceptualizing Urban Poverty, Background Paper for the United Nations Centre for Human Settlements (Habitat), Global Report on Human Settlements. London School of Economics. London, 1994.

- [31] Zio E., Aven T., Industrial disasters: Extreme events, extremely rare. Some reflections on the treatment of uncertainties in the assessment of the associated risks. *Process Safety and Environmental Protection* (91), 2013.
- [32] Żurek J., Modelowanie nadążnych systemów bezpieczeństwa. Wydawnictwa Naukowe ITE. Radom 2010.

Dr hab. inż. Marek Młynczak, prof. nadzw. PWr., Politechnika Wrocławska, Wydział Mechaniczny, Katedra Logistyki, Systemów Transportowych i Układów Hydraulicznych. Zajmuje się metodami oceny ryzyka w systemach technicznych oraz badaniami eksploatacyjnymi różnorodnych obiektów, a w szczególności środków transportu i maszyn górnictwa odkrywkowego. Interesuje się eksploatacją techniczną, niezawodnością, degradacją i diagnostyką techniczną ukierunkowaną na ograniczanie uszkodzalności w systemach technicznych.