Ekonomika i Organizacja Logistyki
2 (2), 2017, 69–76

DOI: 10.22630/EIOL.2017.2.2.16

Tomasz Nowakowski
Politechnika Wrocławska

Podatność na zagrożenia procesów logistycznych – problem oceny

Vulnerability of logistic process – evaluation problems

Synopsis. Główne kierunki rozwoju współczesnej teorii niezawodności dotyczą zarówno codziennych działań inżynierskich, takich jak np. kontrola jakości w produkcji masowej czy „czysta" analiza niezawodności, jak i nowych wyzwań, np. efektywności, odporności czy bezpieczeństwa złożonych systemów i procesów technicznych lub antropotechnicznych. Są one obecnie przedmiotem wielu prac koncepcyjnych, modelowania i badań. Celem artykułu jest pokazanie jak wymagania w stosunku do osiągów obiektu technicznego były poszerzane o oczekiwania klienta (jakość), zdolność do zapobiegania utracie właściwości przez obiekt podczas eksploatacji (nieuszkadzalność i obsługiwalność), skutki niepożądanych zdarzeń i ochrona przed nimi (bezpieczeństwo) oraz zdolność do odtworzenia osiągów (odporność na zagrożenia). Skoncentrowano uwagę na problemie oceny podatności procesu logistycznego na zagrożenia w rzeczywistych warunkach eksploatacji systemu logistycznego. Odniesiono się do modeli i metod oceny znanych i stosowany w zagadnieniach oceny niezawodności i bezpieczeństwa różnych obiektów technicznych.

Słowa kluczowe: podatność, zagrożenie, proces logistyczny, ocena

Abstract. There are several trends of development of modern reliability theory; some of them are subjects of everyday engineering activity, like: quality control of mass production or "pure" reliability. But most of these issues, such as: effectiveness, survivability, safety, security, are currently the subject of many works of conceptual, modeling, case study or survey nature. The aim of this article is show how the performance requirements of technical objects were supplemented with: customer expectations (quality), abilities to prevent the loss of the object properties in operation time (reliability and maintainability), the effects of undesirable events and protection against them (safety and security) and the ability to restore performance (resilience). The focus was on the problem of assessing the vulnerability of the logistics process to hazards in the actual operating conditions of the logistics system. It refers to models and evaluation methods known and used in the assessment of the reliability and safety of various technical objects.

Key words: vulnerability, logistic process, evaluation

Wstęp

W literaturze naukowej z obszaru niezawodności, bezpieczeństwa i zarządzania ryzykiem pojawia się coraz więcej artykułów poświęconych własnościom złożonych systemów technicznych i antropotechnicznych (szczególnie tzw. infrastruktury krytycznej, w tym systemów logistycznych) nazywanych w języku angielskim *vulnerability* oraz *resilience*. Jednocześnie w publikacjach w języku angielskim używa się dużej liczby pojęć o zbliżonym znaczeniu [IPCC 2001, Burton i in. 2002], np.: *vulnerability, sensitivity, resilience, adaptation, adaptive capacity, risk, hazard, coping range, adaptation baseline*. Relacje między tymi określeniami są często niejasne, a sam termin może mieć różne znaczenia, gdy jest stosowany w różnych kontekstach i przez różnych autorów [Buchon 2006].

Zgodnie ze słownikiem, *vulnerability* oznacza podatność na zagrożenia, a *vulnerable* – nieodporny, wrażliwy, niezabezpieczony przed atakami. Pojęcie podatności na zagrożenie (*vulnerability*) wprowadzono w celu poszerzenia możliwości analizy zdarzeń katastroficznych ze względu na ograniczony zakres wnioskowania z powszechnie używanej miary jaką jest ryzyko. Wartość ryzyka dla zdarzenia o małym prawdopodobieństwie wystąpienia i poważnych konsekwencjach oraz zdarzenia o dużej intensywności występowania i pomijanych skutkach jest taka sama. Pojawia się zatem problem jak rozumieć i jak zmierzyć podatność na zagrożenia systemów i procesów logistycznych.

Definicje pojęcia podatność na zagrożenia

Pojęcie podatności na zagrożenia (*vulnerability*) jest definiowane przez wielu autorów [Tixier i in. 2012] w zależności od dyscypliny badań i obszaru kulturowego, z którego pochodzą autorzy. Definicje mogą być klasyfikowane według trzech głównych kryteriów:

- kryterium wrażliwości,
- kryterium skutków,
- kryterium ujmującego oba poprzednie.

Definicje podatności mogą być także klasyfikowane ze względu na sposób badania:

- definicje jakościowe,
- definicje ilościowe,
- definicje półilościowe.

Podsumowując, podatność na zagrożenia charakteryzuje się trzema aspektami [Kröger i Zio 2011]:

- stopniem strat lub zniszczeń wynikających z działania zagrożenia,
- stopniem narażenia – możliwością wystawienia się na niepożądane oddziaływania różnego stopnia i wrażliwości obiektu na znoszenie strat lub zniszczeń (zagrożony obiekt może być systemem technicznym),
- stopniem odporności – zdolności systemu do przewidywania, radzenia sobie/przyswajania, przeciwstawiania się i odzyskiwania stanu pierwotnego po wystąpieniu zagrożenia lub katastrofy.

Analizując historyczną ewolucję rozumienia pojęcia wyróżniono trzy główne etapy [Tixier i in. 2012]:

I. Definicje podatności skupiają się na stopniu strat i szkód powstałych pod wpływem zagrożenia, tj. na technicznych aspektach podatności. Skutki w sferze społecznej lub historycznej nie są brane pod uwagę. Proponowane sposoby przeciwdziałania są ukierunkowane na zmniejszenie czułości (*sesitivity*) obiektu na możliwość oddziaływania danego zagrożenia;
II. W latach 80. XX wieku uznano, że stopień strat i zniszczeń jest także determinowany przez stopień narażania na wystąpienie zagrożenia. Podatność została zatem zdefiniowana przez wrażliwość obiektu na możliwość narażenia na zagrożenie oraz wrażliwość obiektu na możliwość wystąpienia strat i zniszczeń w funkcji stopnia jego narażenia na dane źródło zagrożenia. Nie wszystkie zagrożone elementy systemu wykazują ten sam poziom ekspozycji na zagrożenie (np. przez różne rozmieszczenie przestrzenne), więc ich podatność będzie różna.
III. W wyniku syntezy tych dwóch podejść proponuje się obecnie trzeci rodzaj definicji:
   – z jednej strony w naukach stosowanych podkreśla się, że stopień strat i zniszczeń zależy od wewnętrznych charakterystyk narażonego elementu. Podatność jest więc rozumiana jako wewnętrzny czynnik ryzyka związany ze zdolnością do oporu zagrożonego elementu. Po przekroczeniu danego poziomu odporności zagrożony element może ulec uszkodzeniu;
   – z drugiej strony, w dziedzinie nauk społecznych, zdefiniowano [Adger 2000] problem zdolności populacji do radzenia sobie z katastrofą, pochłaniania skutków i regeneracji własności jako miarę ich podatności. Występują czynniki wyzwalające katastrofy naturalne, ale w odpowiedzi systemy domowe lub społeczne albo im ulegają albo potrafią się ochronić. Taką zdolność do adaptacji określono jako zdolność społeczeństwa do przetrwania (żywotność). Zdefiniowana według Allen [2003] podatność odnosi się do „cech osoby lub grupy zależnych od ich zdolności do przewidywania, radzenia sobie, odpierania i regeneracji zdarzeń zachodzących pod wpływem naturalnych lub wywołanych przez człowieka katastrof, biorąc pod uwagę, że na podatność oddziaływuje wiele czynników polityczno-instytucjonalnych, ekonomicznych i społeczno-kulturowych".

Przedstawiony podział został także przeanalizowany w artykule Nowakowskiego, Werbińskiej-Wojciechowskiej i Chlebusa [2015] dotyczącym współczesnych wyzwań stojących przed teorią i inżynierią niezawodności. Podsumowaniem analizy może być schemat pokazany na rysunku 1. Biorąc pod uwagę skalę czasu, wyróżniono cztery etapy:

- etap 0 – zdefiniowanie oczekiwań klienta, ocena jakości;
- etap 1 – uwzględnienie w ocenie możliwości utraty jednej właściwości obiektu wraz z upływem czasu eksploatacji – nieuszkadzalność;
- etap 2 – uwzględnienie dwóch właściwości obiektu, uszkadzalności i skutków uszkodzenia obiektu – bezpieczeństwo lub nieuszkadzalności i naprawialności/obsługiwalności obiektu – niezawodność w sensie szerszym,
- etap 3 – uwzględnienie trzech właściwości obiektu, bezpieczeństwo i naprawialność lub naprawialność i skutki uszkodzenia – podatność na uszkodzenie.

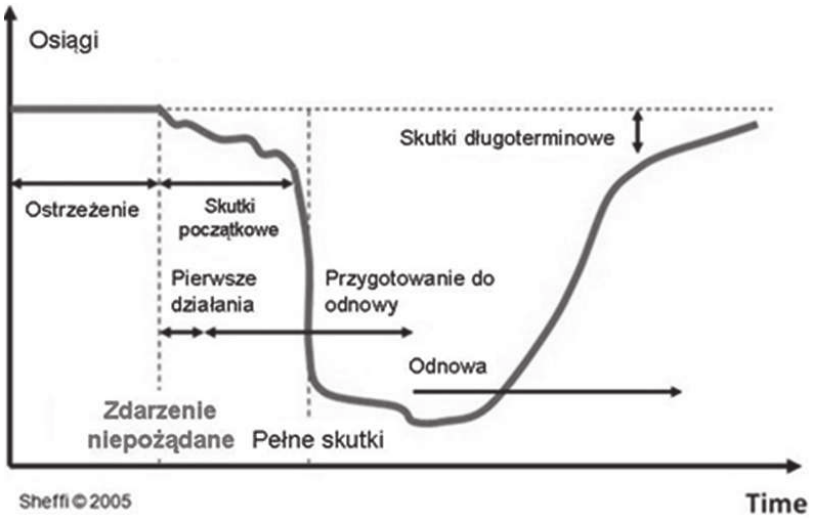
3	PODATNOŚĆ naprawialność *i*	skutek *i*
2	BEZPIECZEŃSTWO skutek *i*	NIEZAWODNOŚĆ *i* naprawialność
1	NIEUSZKADZALNOŚĆ czas *i*	
0	JAKOŚĆ	

Rysunek 1. Schemat relacji między niezawodnością i podatnością na uszkodzenia
Figure 1. Schema of relations between reliability and vulnerability

Źródło: opracowano na podstawie [Nowakowski, Werbińska-Wojciechowska i Chlebus 2015]

Model podatności na zagrożenia

Jednym z powszechnie cytowanych przebiegów utraty własności przez złożony system jest tzw. profil Sheffi'ego i Rice [2005]. Został on zaproponowany do opisu podatności systemów logistycznych – uszkodzeniem jest przerwanie łańcucha dostaw (rys. 2).



Rysunek 2. Schemat procesu reakcji na zagrożenie
Figure 2. Schema of disruption process

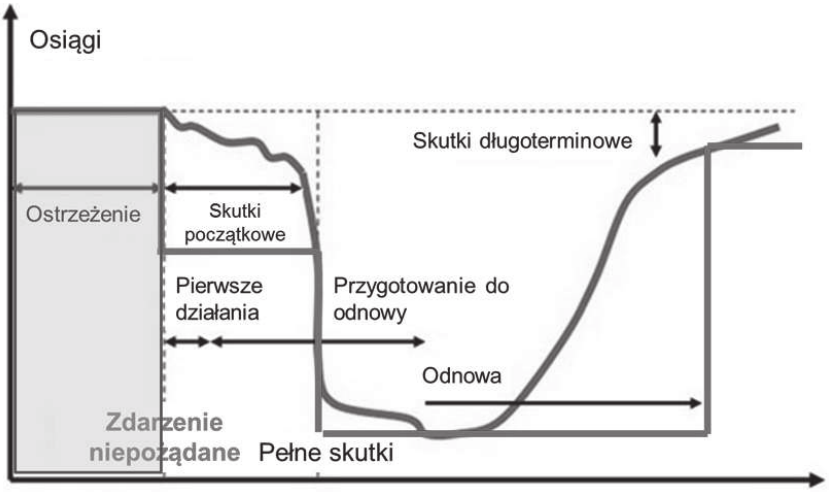
Źródło: opracowano na podstawie [Schaffi i Rice 2005].

Wyróżniono kolejne fazy tego procesu:

- *warning* – ostrzeżenie – okres oczekiwania na wystąpienie zagrożenia; czasem możliwe jest przewidzenie wystąpienia niepożądanego zjawiska i przygotowanie się na nie;
- *distruptive event* – przerwanie – zdarzenie niepożądane, katastrofa;
- *first response* – pierwsza odpowiedź – pierwsze działania związane z oceną sytuacji, ratowaniem i zabezpieczaniem życia ludzkiego, wyłączeniem działającego systemu, zapobieganiem dalszym zniszczeniom;

- *delayed impact* – opóźnione uderzenie – kumulujące się w czasie efekty katastrofy;
- *full impact* – pełne uderzenie – wystąpienie pełnych efektów zdarzenia niepożądanego;
- *prepare for recovery* – przygotowanie do regeneracji/powrotu do normalnego stanu;
- *long term imapact* – długoterminowe skutki uderzenia/katastrofy.

Biorąc pod uwagę dyskusję dotyczącą pojęć i ich klasyfikacji, Buchon [2006] zaproponował model podatności bazujący na danych uzyskanych z obserwacji zgromadzonych po wystąpieniu zdarzenia niepożądanego. Odnosząc się do znanych z teorii niezawodności modeli, na rysunku 3 pokazano, że wszystkie fazy procesu reakcji na zagrożenie można próbować opisać modelami wielofazowymi niezawodności systemu technicznego z rezerwą czasową [Nowakowski 2013]. Oczywiście pojawiają się problemy teoretyczne związane ze spełnieniem założeń modeli niezawodnościowych, ale ich aplikacja jest ograniczona przede wszystkim dostępnością wystarczająco wiarygodnych danych z eksploatacji rzeczywistych systemów logistycznych.



Rysunek 3. Proces reakcji na zagrożenie a modele niezawodności
Figure 3. Disruption process vs. dependability models
Źródło: opracowano na podstawie [Nowakowski 2013].

Ocena podatności procesu logistycznego

Podatność procesu logistycznego jest charakteryzowana na kilka sposobów. Przykłady są następujące [Valis i Nowakowski 2013]:

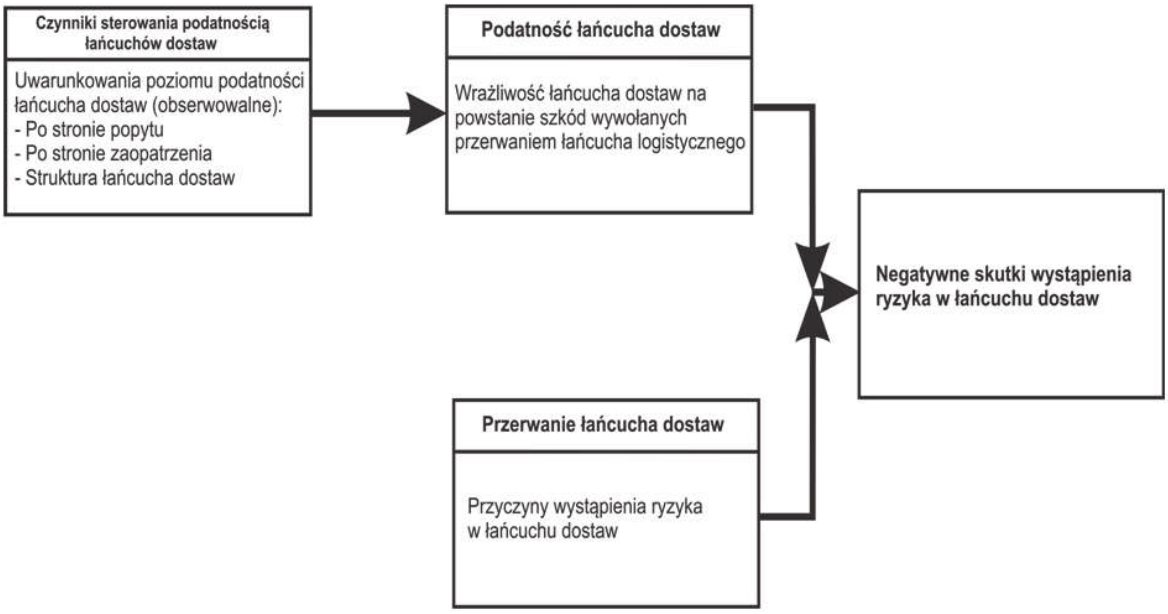
- „Narażenie na poważne zakłócenia" [Christopher i Peck 2004];
- „Zdolność źródeł i czynników ryzyka, aby przeważyć strategie łagodzące ryzyko, powodując negatywne skutki w łańcuchu dostaw" [Jutner, Pecki Christopher 2003];
- „Podatność łańcucha dostaw jest funkcją niektórych cech łańcucha dostaw i tego, że straty, które ponosi firma są wynikiem podatności jej łańcucha dostaw na przerwanie danego łańcucha dostaw" [Wagner i Bode 2006].

Możliwe uwarunkowania oceny podatności na zakłócenia i przerwania łańcucha dostaw pokazano na rysunku 4. Analiza różnych proponowanych metod oceny podatności wskazuje, że [Valis i Nowakowski 2013]:

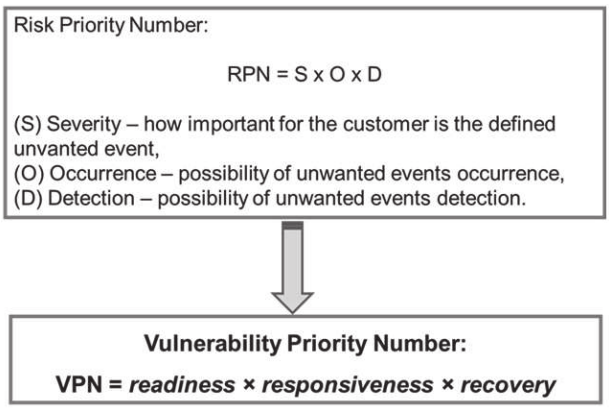
- większość metod bazuje na opinii eksperta,

- konieczne jest pozyskiwanie danych od zainteresowanych stron,
- większość metod daje oceny (rangowanie) jakościowe pozwalające na mapowanie podatności,
- tylko mała część metod jest w stanie oszacować ilościowe wskaźniki podatności [Valis 2013].

Dla złożonych łańcuchów dostaw można znaleźć wyniki oszacowanych wskaźników podatności; np. indeksu podatności łańcucha dostaw (SCVI – *Supply Chain Vulnerability Index*) [Wagner i Bode 2006] lub wskaźnik ważności podatności (VRN – *Vulnerability Priority Number*) [Nowakowski, Werbińska-Wojciechowska i Chlebus 2015].



Rysunek 4. Podatność na zakłócenia i przerwania procesu logistycznego
Figure 4. Vulnerability of logistic proces
Źródło: opracowano na podstawie [Wagner i Bode 2006].



Rysunek 5. Schemat koncepcji utworzenia wskaźnika VPN
Figure 5. Schema of VPN index conception
Źródło: opracowano na podstawie [Nowakowski, Werbińska-Wojciechowska i Chlebus 2015].

Algorytm obliczeń wskaźnika SCVI bazuje na teorii grafów [Wagner i Bode 2006]. Kolejne kroki tego algorytmu dotyczą:

- zdefiniowania węzłów grafu jako czynników stanowiących zagrożenia dla analizowanego procesu logistycznego,
- zidentyfikowanie wag i łuków w grafie w celu określenia zależności i korelacji,
- budowa macierzy zależności, obliczenia wskaźnika SCVI,
- analiza porównawcza grafów/wskaźników dla różnych procesów.

Przeprowadzone obliczenia pozwoliły na zróżnicowanie różnych grup gospodarki, np. przy wartości średniej wskaźnika SCVI = 24,14; dla przemysłu motoryzacyjnego SCVI = 28,85, a dla przemysłu hurtowego i detalicznego SCVI = 20,67. Można uznać, że metoda działa na tyle poprawnie, że pozwala różnicować podatność na zagrożenia różnych interesariuszy.

Podsumowanie i wnioski

Artykuł prezentuje możliwe podejścia i wybrane sposoby oceny podatności na zagrożenia procesu logistycznego. Nie ma jedynego możliwego podejścia – występuje szerokie spektrum różnych metod badania, modelowania i oceniania obszarów badawczych dotyczących oceny podatności systemu. Kwestia wrażliwości/podatności jest obecnie szczególnie istotne dla takich systemów jak środowisko naturalne, łańcuchy dostaw czy infrastruktura budowlana. Również metody oceny są zróżnicowane – od standardowych metod statystycznych do zaawansowanych metod takich jak np. sieci Petriego lub logika rozmyta.

Istnieją systemy i procesy logistyczne szczególnie narażone na działania zewnętrzne, których odporność na zagrożenia ma decydujące znaczenia dla warunków życia społeczeństwa. Nazywa się je często infrastrukturą krytyczną, do której należą także łańcuchy dostaw żywności, systemy dostaw produktów łatwo psujących się.

Literatura

Adger W.N., 2000: Social and Ecological Resilience: Are They Related? Progress in Human Geography, 24(3).

Allen K., 2003: Vulnerability reduction and the community-based approach, [w]: Pelling M. (red.), Natural Disasters and Development in a Globalising World, Routledge, New York.

Bouchon S., 2006: The Vulnerability of interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the-Art., European Commission Directorate-General Joint Research Centre Institute for the Protection and Security of the Citizen.

Burton I., Huq S., Lim B., Pilifosova O., Schipper E.L., 2002: From impacts assessment to adaptation priorities: the shaping of adaptation policies, [w:] Climate Policy 2.

Christopher M., Peck H., 2004: Building the resilient supply chain. International Journal of Logistics Management. 15(2), 1–13.

IPCC (Intergovernmental Panel on Climate Change), 2001, Climate Change: Impacts, Adaptation and Vulnerability. Contribution to the Working Group II to the Third Assessment Report of the IPCC, UNEP Publication.

Jüttner U., Peck H., Christopher M., 2003: Supply chain risk management: outlining the agenda for future research, International Journal of Ligistics: Research and Application, 6(4).

Kröger W., Zio E., 2011: Vulnerable Systems. Springer-Verlag, London Limited.

Nowakowski T., 2013: Vulnerability vs. dependability of logistic systems. Proceedings of Carpathian Logistics Congress CLC.

Nowakowski T., Werbińska-Wojciechowska S., Chlebus M., 2015: Supply chain vulnerability methods – possibilities and limitations, Proc. of the European Safety and Reliability Conference, ESREL 2015, Zurich, Switzerland.

Scheffi Y., Rice J.B. Jr., 2005: A Supply Chain View of the Resilient Enterprise. MIT Sloan Management Review, 47, 1.

Tixier J., Tena-Chollet F., Dusserre G., Lapébie E., Munier L., Osmont A., 2012: Development of a GIS-based approach for the vulnerability assessment of a territory exposed to a potential risk, [w:] Land Use Planning and Risk-Informed Decision Making. Proceedings of ESReDA Seminar 2012.

Valis D., Nowakowski T., 2013: Stan wiedzy na temat wybranych możliwości oceny podatności na zagrożenia – przegląd literatury, Materiały Zimowej Szkoły Niezawodności PAN.

Wagner S.M., Bode C., 2006: An empirical investigation into supply chain vulnerability, Journal of Purchasing & Supply Management, 12(6).

Adres do korespondencji:
prof. dr hab. inż. Tomasz Nowakowski
Politechnika Wrocławska
Wydział Mechaniczny
Wyb. Wyspiańskiego 27
50-370 Wrocław
tel.: (+48) 71 320 11
e-mail: tomasz.nowakowski@pwr.edu.pl