P R A C E N A U K O W E P O L I T E C H N I K I W A R S Z A W S K I E J
z. 115 Transport 2017

Adrian Gill, Adam Kadziński
Politechnika Poznańska, Wydział Maszyn Roboczych i Transportu

IDENTYFIKACJA ZAGROŻEŃ W DOMENACH ANALIZ SYSTEMU KOLEJOWEGO

Rękopis dostarczono, styczeń 2017

Streszczenie: Zgodnie z obowiązującymi przepisami (dokumentami CSM), na przedsiębiorstwach kolejowych, zarządcach infrastruktury oraz wszystkich podmiotach, które wprowadzają zmiany do systemu kolejowego Unii Europejskiej, ciąży odpowiedzialność za utrzymywanie ryzyka wszystkich zagrożeń na poziomach poniżej kategorii ryzyka nieakceptowanego. Aby to osiągnąć CSM przewiduje konieczność realizacji procesu zarządzania ryzykiem zagrożeń. Ogólne wskazania co do jego przeprowadzania znajdują się w załączniku do dokumentu CSM (rozporządzenie 402/2013) i co do idei, nie różnią się od klasycznych podejść do zarządzania ryzykiem zagrożeń. Kluczowa jest natomiast poprawna implementacja procedur, które należy zrealizować w ramach tego procesu, ale których nie przedstawia się (a nawet nie wymienia) we wspomnianych przepisach w szczegółowy sposób. W niniejszym artykule zaprezentowano zatem podstawy identyfikacji zagrożeń dedykowane domenom analiz w systemie kolejowym, obejmującą procedury: rozpoznawania źródeł zagrożenia, grupowania źródeł zagrożenia, formułowania zagrożenia i wstępnego wskazania wielkości strat/szkód, które mogą powstać w wyniku aktywizacji zagrożenia. Rezultatem tych procedur jest m.in. lista źródeł zagrożeń i lista sformułowanych zagrożeń. Proces identyfikacji zagrożeń jest odzwierciedleniem pewnych rodzajów rozumowania (indukcyjnego i obdukcyjnego) i w związku z tym zdefiniowano i przedstawiono odpowiednie sposoby jego realizacji.
Słowa kluczowe: zagrożenie, proces identyfikacji zagrożeń, zarządzanie ryzykiem zagrożeń

1. WPROWADZENIE

Zgodnie z obowiązującymi przepisami Unii Europejskiej (m.in. dokumentami CSM – *Common Safety Methods*) ujednolicającymi wymagania i metody związane z bezpieczeństwem na kolei, na przedsiębiorstwach kolejowych, zarządcach infrastruktury oraz wszystkich podmiotach, które wprowadzają zmiany do systemu kolejowego, ciąży odpowiedzialność za utrzymywanie ryzyka wszystkich zidentyfikowanych zagrożeń na poziomach poniżej kategorii ryzyka nieakceptowanego. Dla zmian mających znaczący wpływ na bezpieczeństwo (Systemu Kolejowego Unii Europejskiej lub/i jego podsystemów strukturalnych), CSM przewiduje konieczność realizacji procesu zarządzania ryzykiem zagrożeń. Ogólne wskazania co do jego przeprowadzania znajdują się w załączniku do dokumentu CSM (rozporządzenie 402/2013 [12]) i co do idei nie różnią się od klasycznych podejść do zarządzania ryzykiem zagrożeń. Głównymi celami procesu zarządzania ryzykiem zagrożeń

jest identyfikacja zagrożeń generowanych przez zmianę i utrzymywanie ich ryzyka na poziomach poniżej kategorii ryzyka nieakceptowanego.

Identyfikowanie zagrożeń jest to proces systematycznego postępowania przy identyfikacji zagrożeń, które w wyniku aktywizacji mogą być powodem strat/szkód we wskazanej domenie analiz. Rezultatem identyfikacji zagrożeń jest m.in. lista źródeł zagrożeń i lista sformułowanych zagrożeń. Przykłady realizacji tego procesu przedstawiają m.in. prace [2-5, 8-10].

Proces identyfikacji zagrożeń (*hazard identification process* – HIP) odbywa się na zasadach rozumowania ampliatywnego (twórczego), głównie indukcyjnego, a nawet abdukcyjnego, gdyż pojawia się w nim element twórczości, „kreatywnego skoku umysłu", „zdolności do trafnego zgadywania" [4, 13].

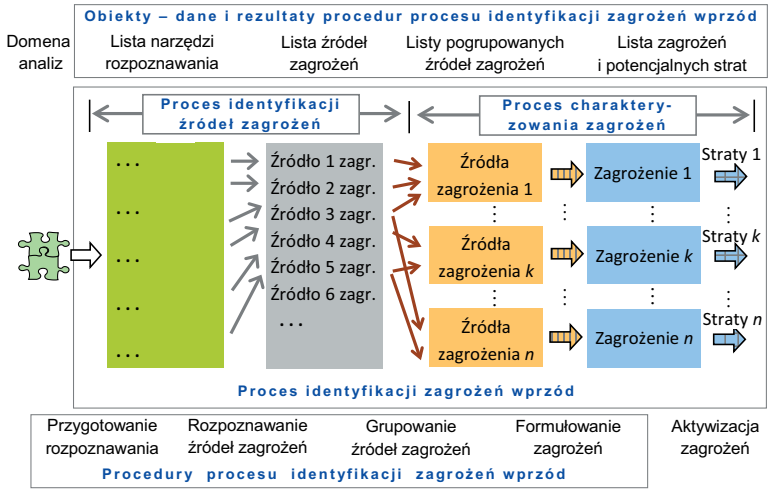
W HIP można wskazać pewien kierunek jego realizacji wynikający z kolejności identyfikowania składowych procesu. Aby to wyjaśnić, można posłużyć się pojęciami rozumowanie wprzód (*forward reasoning*) i rozumowanie wstecz (*backward reasoning*). Jak jednak wskazuje m.in. autor pracy [13], może być to pewnym nadużyciem, gdyż rozumowanie/wnioskowanie odbywa się zawsze w jednym kierunku – od przesłanek do wniosku. Wszędzie zatem gdzie powodowałoby to kontrowersje, autorzy niniejszej pracy proponują używać dwóch następujących pojęć: identyfikacja zagrożeń wprzód (*forward hazard identification*) i identyfikacja zagrożeń wstecz (*backward hazard identification*).

Celem artykułu jest przedstawienie metodycznych podstaw realizacji procesu identyfikacji zagrożeń wprzód i wstecz w domenach analiz systemu kolejowego Unii Europejskiej.

2. SPOSOBY REALIZACJI PROCESU IDENTYFIKACJI ZAGROŻEŃ

2.1. IDENTYFIKACJA ZAGROŻEŃ WPRZÓD

Rozumowanie wprzód dotyczy sytuacji, w której do znanych przesłanek próbuje się dobrać wniosek na ich podstawie uzasadniony. Umożliwia ono zatem formułowanie zagrożeń (*hazard* – H), rozpoczynając od pojedynczych przyczyn tj. od źródeł zagrożeń/czynników (*hazard sources* – HS). Stosowane jest zwykle wtedy, gdy pożądanym jest wskazanie konsekwencji dla znanych lub przewidywanych zdarzeń, stanów związanych z analizowanymi elementami podsystemów, systemów, domen/poddomen analiz. W uproszczonym rozumieniu, zastosowanie rozumowania wprzód w identyfikacji zagrożeń jest udzieleniem odpowiedzi na pytanie: Co się stanie gdy…? W odniesieniu do systemów technicznych, sprowadza się to do założenia występowania pewnych zdarzeń, głównie uszkodzeń jego elementów, a następnie analizy wpływu tych zdarzeń na funkcjonowanie systemu. Na rysunku 1 przedstawiono schemat ideowy procesu identyfikacji zagrożeń wprzód (*forward hazard identifiction process* – F-HIP), to jest HIP realizowanego z wykorzystaniem rozumowania wprzód.

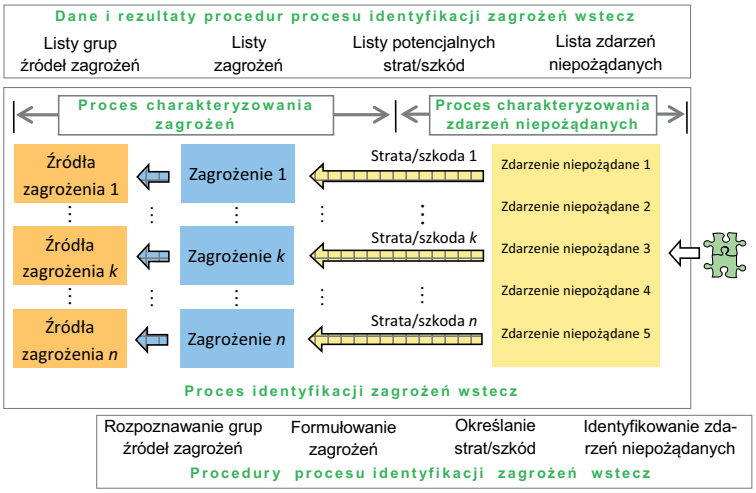


Rys. 1. Schemat ideowy procesu identyfikacji zagrożeń wprzód (F-HIP) [9]

2.2. IDENTYFIKACJA ZAGROŻEŃ WSTECZ

Rozumowanie wstecz zwykle odnosi się do sytuacji, w której dla znanego wniosku próbuje się znaleźć uzasadniające go przesłanki. Pojmowane w ten sposób rozumowanie, polega na poszukiwaniu (nieznanych) przyczyn dla (znanych) skutków, czyli na poszukiwaniu (nieznanych) eksplanansów dla (znanych) eksplanandów [4, 13]. Nieformalnie rozumowanie wstecz określa się zatem także jako "rozumowanie Sherlocka Holmesa". W odniesieniu do systemów technicznych można powiedzieć, że jest ono stosowane przy ustalaniu sposobu w jaki doszło do wystąpienia pewnego stanu systemu, zwykle wynikającego ze zdarzeń polegających na uszkodzeniu jego elementów.

Realizacja HIP prowadzona zgodnie z rozumowaniem wstecz polega na poszukiwaniu i rozpoznawaniu HS dla znanych zdarzeń niepożądanych (*undesirable events* –UE) lub takich, które są znane z innych podobnych domen analiz. Zdarzenia niepożądane (UE) są wynikiem tzw. aktywizacji zagrożeń, a z ich występowaniem mogą być związane straty/szkody. Na podstawie przewidywanych i/lub znanych UE są zatem formułowane H. Dalsza część procesu jest odwróceniem HIP prowadzonego z wykorzystaniem rozumowania wprzód. Na rysunku 2 przedstawiono Schemat ideowy procesu identyfikacji zagrożeń wstecz (*backward hazard identification process* – B-HIP) to jest HIP realizowanego z wykorzystaniem rozumowania wstecz.



Rys. 2. Schemat ideowy procesu identyfikacji zagrożeń wstecz (B-HIP)

3. PROCEDURY PROCESU IDENTYFIKACJI ZAGROŻEŃ

3.1. DOMENA ANALIZ

Domena analiz jest to wyróżniona przestrzeń zainteresowań składająca się z trzech elementów: środowiska, człowieka/ludzi, techniki, w związku z którymi osobno lub w różnych kombinacjach mogą pojawić się źródła zagrożeń. W domenie analiz przeprowadza się procesy identyfikacji zagrożeń. Zwykle składa się ona z kilku poddomen, których wyróżnienie ułatwia realizację HIP (*hazard identification process*) i może wpłynąć na kompletność jego rezultatów. Takimi poddomenami mogą być np. etapy produkcji, stanowiska pracy, części procesów technologicznych i transportowych. Dla każdej z poddomen tworzony jest jej model. Z tego powodu domena analiz zwykle jest domeną zagregowaną, a jej model (model zagregowanej domeny analiz) jest agregowany z modeli wyróżnionych poddomen. Identyfikowanie H następuje oddzielnie w każdej z poddomen. Kluczowym jest więc odpowiednie powiązanie składowych procesów identyfikacji zagrożeń w poszczególnych poddomenach tak, aby uzyskać rezultaty procesu identyfikacji zagrożeń dla całej domeny analiz.

3.2. IDENTYFIKACJA ŹRÓDEŁ ZAGROŻEŃ

Identyfikacja HS w F-HIP odbywa się w ramach procedur: przygotowania narzędzi do przeszukiwania domeny analiz i rozpoznawania HS. Do przeszukiwania domeny analiz można w tym przypadku wykorzystać następujące narzędzia [4, 9]: rejestry niepożądanych (katastrof, poważnych wypadków, wypadków i incydentów), listy pytań kontrolnych, metody „burzy mózgów", opinie ekspertów.

W B-HIP, identyfikacja HS odbywa się w ramach procedur: formułowania zagrożeń i rozpoznawania grup źródeł zagrożeń. W związku z tym, że HS są rozpoznawane na podstawie już sformułowanych H, nie ma potrzeby ich grupowania (co jest jedną z kluczowych procedur w F-HIP). Do zagrożenia jest bowiem przynależna określona grupa HS.

Jako narzędzie szczególnie przydatne w B-HIP warto wskazać rejestry zdarzeń (m.in. wypadków). Wykonane dla podobnych domen analiz, pozwalają zakładać, że analogiczne zdarzenia będą miały miejsce w analizowanej domenie.

Identyfikacja UE polega na wskazaniu (nazwaniu) przewidywanych UE i takich, które są znane z innych podobnych domen analiz, a mogą wystąpić w domenie poddanej analizie. Wynikiem tej identyfikacji jest lista zdarzeń. Na podstawie zidentyfikowanych UE i informacji o elementach domen analiz, spełniających rolę odbiorników narażeń pochodzących od HS, określa się straty/szkody. Stanowi to podstawę formułowania zagrożeń.

Niezależnie od sposobu realizacji HIP, rozpoznawanie HS jest działaniem prowadzącym do określenia (nazwania, oznaczenia) HS oraz wskazania, na element domeny analiz, który jest generatorem narażeń.

Rozpoznane HS są więc m.in. wynikiem [6]: przeglądu dokumentacji technicznej obiektów użytkowanych w domenie analiz, przeglądu czynności, procesów zachodzących w analizowanym domenie, studiowania norm i standardów bezpieczeństwa, odbywania wizji terenowych i przeprowadzania wywiadów, dostępnych opisów statystyk zdarzeń niepożądanych oraz wyników specjalistycznych badań tych zdarzeń.

Teoretycznie, każdy z elementów domeny analiz może uczestniczyć w generowaniu narażeń, tj. może być uznany za HS. Zwykle jednak za takie uznaje się twory/czynniki zagrożeń (rozumiane jak np. w [9]), z których występowaniem i/lub aktywnością są związane domniemane straty/szkody. Występuje zatem związek HS z "poczuciem strachu", obawy przed skutkami aktywizacji H.

3.3. GRUPOWANIE ŹRÓDEŁ ZAGROŻEŃ

Grupowanie HS polega na utworzeniu grup (list) źródeł, których występowanie i/lub wspólna aktywność w domenie analiz postrzegane są jako stan tej domeny prowadzący do UE. Procedura grupowania HS nie występuje w B-HIP.

Utworzenie grupy HS następuje poprzez ich wskazanie (np. wyodrębnienie z listy HS) i myślowe powiązanie według wskazanego kryterium wspólnego występowania i/lub aktywności. Na podstawie grup HS formułuje się zagrożenia.

W odniesieniu do procesu grupowania HS można sformułować następujące kluczowe wytyczne:

- należy dążyć do minimalnej liczby HS w grupie,
- w szczególnym przypadku "grupę źródeł zagrożeń" może tworzyć jedno HS,
- jedno HS może występować w wielu grupach HS,
- w grupie HS nie wskazuje się ("nie umieszcza się") braku elementów systemów bezpieczeństwa (braku środków redukcji ryzyka),
- w grupie HS należy uwzględniać uszkodzenia elementów systemów bezpieczeństwa, brak realizacji zaplanowanych funkcji bezpieczeństwa, itp.

3.4. FORMUŁOWANIE ZAGROŻEŃ

Do sformułowania H w większości przypadków wystarczają informacje dotyczące tylko jednego HS lub UE, które identyfikuje się w domenie analiz. Na ogół jest jednak tak, że sformułowanie H jest wynikiem wiedzy o kilku HS i wiedzy dotyczącej elementów domen analiz spełniających rolę narażeń (ON). Prawidłowo sformułowane H pełni rolę informacyjną oraz w pewnym sensie ostrzegawczą. Proces identyfikacji zagrożeń powinien natomiast dostarczać informacji o [1]:

- źródle lub źródłach zagrożenia, których wspólna aktywność może doprowadzać do UE,
- odbiorcy/odbiorniku narażeń,
- sposobie w jaki grupa HS realizuje oddziaływanie na ON,
- konsekwencjach aktywizacji H,
- czynnikach eskalujących w procesie aktywizacji H.

Proponuje się aby w przypadku realizowania B-HIP, nie wskazywać HS spoza badanej domeny analiz (tzn. ograniczać obszar poszukiwania HS i obszar wskazywania UE tylko do niej). Kluczowym jest tutaj prawidłowe dokonanie jej charakterystyki.

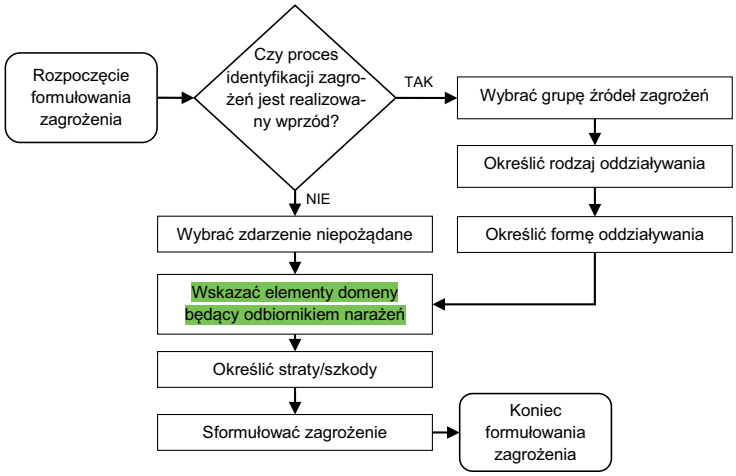
W przypadku realizowania F-HIP, proponuje się aby straty/szkody związane z aktywizacją H były z zakresu wynikającego np. z rodzaju ryzyka, potrzeb podmiotów realizujących zarządzanie ryzykiem. Różny zakres strat (i tym samym różne H) będzie rozpatrywany np. z punktu widzenia operatora środków transportu a inny przez zarząd przedsiębiorstwa, nawet dla tych samych grup HS. Wskazane tutaj założenia mają wykluczyć sytuacje, w których poszukiwanie HS i wskazywanie strat byłoby prowadzone w nieracjonalnie rozbudowany sposób. Szczególnie sprzyja temu realizacja F-HIP.

Do realizacji procedury formułowania H, stosownie do sposobu realizacji HIP, przygotowano odpowiedni algorytm. Algorytm ten przedstawiono w formie graficznej na rysunku 3. Zagrożenie formułuje się na podstawie grupy HS (w F-HIP) lub zdarzenia/zdarzeń niepożądanych (w B-HIP). Zdarzenia niepożądane w stosunku do H, występują w relacjach "jeden do wielu" oraz "wiele do jednego". Oznacza to, że możliwe jest sformułowanie kilku H na podstawie jednego UE, a także kilka UE prowadzi do sformułowania jednego H. Pierwszy rodzaj relacji występuje wtedy, gdy UE dotyczą wielu ON i tym samym występują różne straty/szkody jako wyrażenie konsekwencji UE. Drugi rodzaj relacji rozpatruje się w przypadku, gdy wiele UE prowadzi do powstania tych

samych strat/szkód. W B-HIP niezmiernie istotne jest wskazanie ON.

Rodzaj oddziaływania grupy HS na ON wynika z ich natury i właściwości, które charakteryzuje się podczas procesu identyfikacji HS. Rodzaj oddziaływania jest zwykle związany z postacią HS (postać: fizyczna, chemiczna, biologiczna, psychofizyczna itd.). Jako przykłady rodzajów oddziaływania można wymienić oddziaływanie: mechaniczne, termiczne, elektryczne, wibroakustyczne, itd.

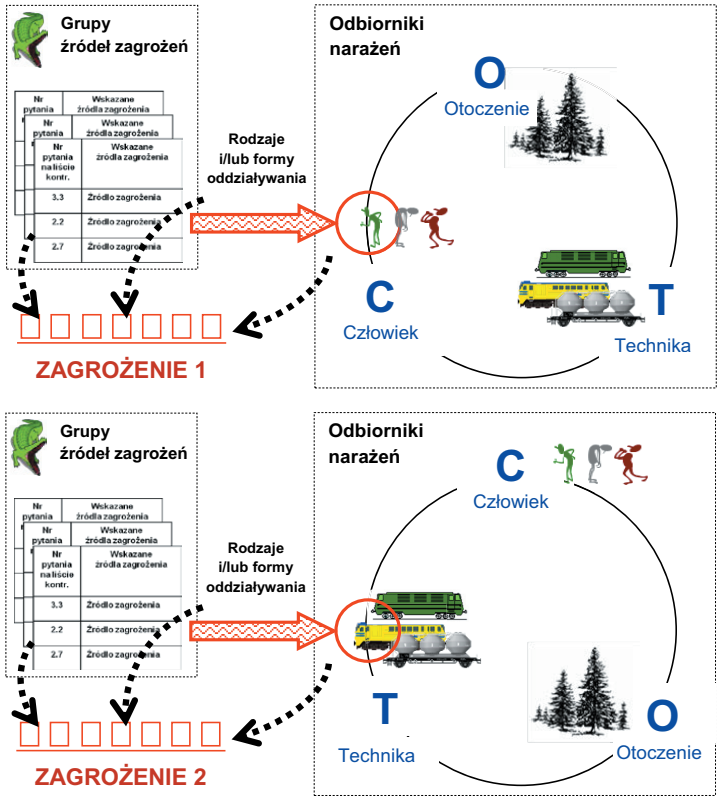
Wpływ grupy HS na elementy domeny analiz (odbiorniki narażeń) może odbywać się w różnej formie lub inaczej – na różnej drodze oddziaływania, zwykle zależnej od rodzaju oddziaływania. Jej określenie polega na wskazaniu sposobu (nośnika) umożliwiającego grupie HS oddziaływanie na odbiornik/odbiorniki narażeń. Typowymi formami oddziaływania są: kontakt fizyczny, forma lotna, bakteryjna, promieniowanie, różne rodzaje dyspersji i dyfuzji.



Rys. 3. Algorytm procedury formułowania zagrożenia w domenie analiz

Wskazanie ON polega na wyborze elementów domeny analiz, na które wpływ mają narażenia pochodzące od HS. Realizacja tego kroku algorytmu może odbywać się na zasadzie systematycznego przeglądu domeny analiz, tj. jego dekompozycji na elementy, a następnie rozpatrywania wpływu każdej z grup źródeł zagrożeń na każdy ze wskazanych elementów. Prawidłowo określony rodzaj i forma oddziaływania w pewnym stopniu sugerują elementy domeny analiz, które uznaje się za odbiorniki narażeń.

Aby właściwie sformułować H należy dla każdego UE określić straty/szkody, związane z ON a pochodzące od grupy HS. Straty/szkody zwykle obejmują trzy rodzaje elementów domeny analiz: człowieka (C), środowisko/otoczenie (O), technikę (T). W niektórych metodach analiz, np. w metodzie Bow-Tie, rozpatruje się także aspekt reputacji firmy [10, 11]. Metodycznie korzystnym jest zatem realizowanie procedury formułowania zagrożeń według określonego schematu, którego ideę przedstawiono na rysunku 4.



Rys. 4. Idea formułowania zagrożenia w wyniku systematycznego przeglądu oddziaływania grup źródeł zagrożeń na elementy domeny analiz (odbiorniki narażeń)

4. PODSUMOWANIE

Proces identyfikacji zagrożeń należy do zbioru najważniejszych procedur metod zarządzania ryzykiem zagrożeń. Jego rezultaty wpływają bezpośrednio na sukces procesu zarządzania ryzykiem. Ważnym jest więc realizować proces identyfikacji zagrożeń w sposób: uporządkowany, łatwy do modyfikowania jego składowych oraz pozwalający dokumentować częściowe i ostateczne jego rezultaty.

Ostatecznym rezultatem procesu identyfikacji zagrożeń jest rejestr zagrożeń. Proponuje się, żeby rejestr zagrożeń składał się z segmentów o jednakowej strukturze. Każdy segment rejestru zagrożeń powinien zawierać: identyfikator zagrożenia (tzw. ID zagrożenia), sformułowanie zagrożenia, kod grupy źródeł zagrożeń, których aktywność jest powodem

sformułowania zagrożenia, listę źródeł zagrożeń tworzących tę grupę, wskazanie zdarzenia niepożądanego będącego konsekwencją aktywizacji zagrożenia oraz ewentualne podanie oznaczenia/numeru (kodu) dotyczącego domeny analiz, w której wskazane zdarzenie powinno być rozważane jako źródło zagrożenia, listę strat/szkód będących opisem konsekwencji aktywizacji zagrożenia.

W niniejszym artykule zaprezentowano sposoby realizacji procesu identyfikacji zagrożeń. Na tle schematów ideowych tego procesu, omówiono procedury: identyfikowania źródeł zagrożeń i zdarzeń niepożądanych, grupowania źródeł zagrożeń i formułowania zagrożeń. Końcowym efektem procesu identyfikacji zagrożeń są charakterystyki zagrożeń, na które składają się: grupa źródeł zagrożenia, sformułowanie/nazwa zagrożenia, potencjalne straty/szkody w wyniku aktywizacji zagrożenia.

Bibliografia

1. Gill A., Koncepcja systemu bezpieczeństwa dla wybranych zagrożeń w komunikacji tramwajowej. Technika Transportu Szynowego, nr 10, 2013, s. 2065÷2074, wersja elektroniczna.
2. Gill A., Kadziński A., Kalinowski D., Identyfikacja zagrożeń związanych z użytkowaniem drzwi podczas eksploatacji tramwajów typu 105Na. Czasopismo AUTOBUSY – Technika, Eksploatacja, Systemy Transportowe, nr 12, 2011, s. 104÷114
3. Gill A., Kadziński A., The identification of hazards generated in municipal transport on the example of the doors fitted in the 105Na tram . Problems of maintenance of sustainable technological systems, vol. IV Automotive Engineering and Vehicle Safety Engineering, Monographs of the Maintenance Systems Unit, Polish Academy of Sciences, Kielce University of Technology, Kielce 2012, s. 38÷51.
4. Gill A., Kadziński A., Hazard identification model, Proceedings of 20th International Scientific Conference Transport Means 2016 Oct 5-7 Juodkrantė, Lithuania, Part 3, Kaunas University of Technology, 2016, s. 885÷890.
5. Gill A., Kobaszyńska-Twardowska A., Identyfikacja zagrożeń w wybranych strefach tramwaju z wykorzystaniem metody Bow-Tie. Logistyka nr 6, 2014, wersja elektroniczna (CD).
6. Jamroz K., Kadziński A., Chruzik K., Szymanek A., Gucma L., Skorupski J., 2010. Trans-Risk – an integrated method for risk management in transport, Journal of KONBiN 13, 209-220.
7. Kadziński A., Gill A., Ogólny model ocen ryzyka zagrożeń identyfikowanych w wybranych obszarach systemów technicznych. Referat wygłoszony na XXXVIII Zimowej Szkoły Niezawodności nt. Ryzyko w eksploatacji systemów technicznych, Szczyrk 2010, wersja elektroniczna.
8. Kadziński A., Gill A., Pruciak K., Rozpoznawanie źródeł zagrożeń jako ważny element metod zarządzania ryzykiem w komunikacji tramwajowej. Czasopismo TTS Technika Transportu Szynowego, 2011, R. 17, nr 9, s. 49÷52.
9. Kadziński A., Studium wybranych aspektów niezawodności systemów oraz obiektów pojazdów szynowych. Wyd. Politechniki Poznańskiej, seria Rozprawy, nr 511, Poznań 2013.
10. Kobaszyńska-Twardowska A., Gill A., Zastosowanie analizy Bow-Tie do identyfikacji warstw ochronnych w systemach bezpieczeństwa. Technika Transportu Szynowego, nr 10, 2013 s. 2287÷2294, wersja elektroniczna.
11. Kobaszyńska-Twardowska A., Gill A., Realizacja procedur oceny ryzyka zagrożeń z użyciem procedur Bow-Tie. Pojazdy Szynowe 2014, nr 2, s. 1÷10.
12. Rozporządzenie wykonawcze Komisji (UE) nr 402/2013 z dnia 30 kwietnia 2013r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009. Bruksela 2013.
13. Urbański M., Rozumowania abdukcyjne. Modele i procedury, Wyd. Naukowe UAM, Poznań 2009, wersja elektroniczna: http://hdl.handle.net/10593/1025.

HAZARD IDENTIFICATION FOR THE ANALYSIS DOMAINS IN RAILWAY SYSTEM

Summary: According to the regulations (CSM documents) the rail company, infrastructure administrator and each railway entity that makes changes in railway system, is responsible to keep the acceptable risk value of all hazards identified in the system. To achieve this, CSM provides for implementation of the risk management process. General indications as to conduct this process can be found in the annex to the CSM document (regulation 402/2013). They do not differ from the classic approaches to risk management. The key is the correct implementation of the procedures that must be implemented as part of this process, but which does not present (or even listed) in the regulations in detail. In this article we present therefore the basics for realizing the hazard identification dedicated domains in the rail system, including: identification of hazard sources, grouping hazard sources, formulating the hazard and the preliminary indication of the size of the loss/damage that may arise as a result of the activation of the hazard. The result of these procedures is list of hazard sources and a list of identified hazard, among others. The hazard identification process is a reflection of certain types of reasoning (inductive and abductive) and therefore we defined and shown the correct ways of its realization.
Keywords: hazard, hazard identification process, risk management