Adrian GILL, Adam KADZIŃSKI

REJESTR ZAGROŻEŃ

Artykuł dotyczy ważnego kroku algorytmu metod zarządzania ryzykiem zagrożeń – realizacja procesu identyfikacji zagrożeń i przygotowanie rejestru zagrożeń. Rejestr zagrożeń jest ostatecznym rezultatem procesu identyfikacji zagrożeń. Zaprezentowano sposób pozyskiwania informacji do tworzenia rejestrów zagrożeń i propozycję ich formatu. Na tle formatu rejestru podano wytyczne / rekomendacje do wypełniania pól kart charakterystyki pojedynczego zagrożenia składających się na rejestr zagrożeń.

WSTĘP

Rejestr zagrożeń (RZ) jest rezultatem złożonego procesu przeprowadzanego w ramach metod zarządzania ryzykiem to jest tzw. procesu identyfikacji zagrożeń. W związku tym, że proces identyfikacji zagrożeń obejmuje najważniejsze procedury metod zarządzania ryzykiem, jego rezultaty wpływają bezpośrednio na poprawność wyników stosowania tych metod. Zgodnie z wytycznymi Rozporządzenia 402/2013 [13] rejestr zagrożeń oznacza dokument, w którym zestawia się i opatruje stosownymi odniesieniami zidentyfikowane zagrożenia, związane z nimi środki bezpieczeństwa (*safety measures*) i źródła zagrożeń oraz wskazuje podmiot organizacyjny, który ma nimi zarządzać. Do zbudowania RZ konieczne jest zatem właściwe rozumienie podstawowych pojęć, kategorii i relacji, które to pojawiają się w procesie identyfikacji zagrożeń i są składowymi RZ. Ponadto, ważnym jest aby w kontekście tworzenia RZ, realizować proces identyfikacji zagrożeń w sposób uporządkowany, łatwy do modyfikowania oraz pozwalający dokumentować częściowe i ostateczne jego rezultaty.

Rejestr zagrożeń jest jednym z niezbędnych efektów aplikowania metod zarządzania ryzykiem zagrożeń w domenach analiz w transporcie. W szczególności mogą to być domeny analiz będące na przykład:

- przejazdami kolejowo-drogowymi,
- systemami utrzymywania (obsługiwania) pojazdów i statków powietrznych,
- zadaniami w samochodowych przewozach ładunków nienormatywnych,
- procesami produkcji składowych nawierzchni kolejowej i podtorza,
- stanowiskami pracy związanymi z transportem szynowym, drogowym czy lotniczym,
- zadaniami w kolejowych i samochodowych przewozach towarów niebezpiecznych,
- odcinkami sieci tramwajowych.

Celem artykułu jest prezentacja koncepcji i formatu rejestru zagrożeń jako niezbędnego efektu aplikowania metod zarządzania ryzykiem zagrożeń.

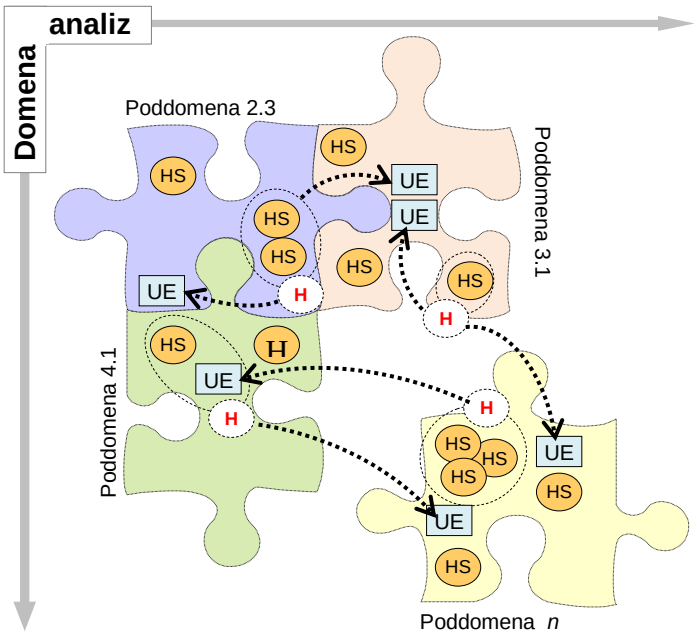
Definicje i rozumienie użytych w artykule pojęć przedstawiono w rozdziale 1..

Do zestawienia wyników procesu identyfikacji zagrożeń przygotowano odpowiedni format zapisu charakterystyki pojedynczego zagrożenia w postaci tzw. karty charakterystyki zagrożenia. Jej opis i strukturę przedstawiono w rozdziale 2.

1. PODSTAWOWE POJĘCIA I DEFINICJE

1.1. Podstawowe składowe domeny 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 [8]. W domenie analiz przeprowadza się procesy identyfikacji zagrożeń. W każdym procesie identyfikacji zagrożeń uczestniczą następujące składowe: źródła zagrożeń (HS – *hazard sources*), zagrożenia (H – *hazard*), zdarzenia niepożądane (UE – *undesirable events*). Wymienione tu składowe wchodzę w charakterystyczne relacje, które pokazano na rysunku 1.



Rys. 1. *Schemat ideowy domeny analiz oraz składowych procesu identyfikacji zagrożeń i relacji między nimi (objaśnienia oznaczeń znajdują się w tekście artykułu)*

Źródła zagrożenia (HS), zwane także w literaturze czynnikami zagrożenia, czynnikami ryzyka, ich część nazywana jest czynnikami niebezpiecznymi, szkodliwymi lub uciążliwymi, są to twory (np. fizyczne, chemiczne, biologiczne, psychofizyczne, organizacyjne, osobowe), których obecność we wskazanym obszarze analiz, stan, właściwości itp. są powodem (źródłem) sformułowania zagrożenia [6, 15].

Zagrożenie (H) (def. 1) – warunkowa możliwość ujawnienia się strat/szkód [11].

Zagrożenie (H) (def. 2) – stan domeny analiz mogący spowodować straty/szkody (modyfikacja def. z [12]).

Zdarzenie niepożądane (UE) – zdarzenie, które może spowodować stratę/szkodę w wyniku aktywizacji (materializacji) zagrożenia [15].

1.2. Procesy

Proces identyfikacji zagrożeń jest to proces systematycznego postępowania przy identyfikacji H, które w wyniku aktywizacji mogą być powodem strat/szkód we wskazanej domenie analiz. Rezultatem identyfikacji H jest m.in. lista HS i lista sformułowanych H. Przykłady realizacji tego procesu przedstawiają m.in. prace [2, 3, 4, 5, 7, 8].

Proces identyfikacji zagrożeń odbywa się na zasadach rozumowania ampliatywnego (twórczego), głównie indukcyjnego a nawet abdukcyjnego, gdyż jak wskazuje Urbański [14], pojawia się tutaj element twórczości, „kreatywnego skoku umysłu", „zdolności do trafnego zgadywania".

W procesie identyfikacji zagrożeń można wskazać pewien kierunek jego realizacji wynikający z kolejności identyfikowania składowych procesu. Kierunki te określono pojęciami *forward reasoning* i *backward reasoning* a w odniesieniu do procesu identyfikacji zagrożeń pojęciami: *forward identification*, *backward identification* [4].

Forward reasoning dotyczy sytuacji, w której do znanych przesłanek próbuje się dobrać wniosek na ich podstawie uzasadniony. *Forward identification* umożliwia zatem formułowanie zagrożeń (H), rozpoczynając od pojedynczych przyczyn tj. od źródeł zagrożeń/czynników. Stosowane jest zwykle wtedy, gdy pożądanym jest wskazanie konsekwencji znanych lub przewidywanych zdarzeń będących wynikiem stanów analizowanych domen.

Backward reasoning 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) strat/szkód. Nieformalnie *backward reasoning* określa się zatem także jako "rozumowanie Sherlocka Holmesa". W odniesieniu do systemów technicznych można powiedzieć, że *backward reasoning* jest stosowane przy ustalaniu sposobu w jaki doszło do wystąpienia pewnego stanu domeny analizy, zwykle wynikającego ze zdarzenia polegającego na uszkodzeniu jego elementów. Realizacja procesu identyfikacji zagrożeń – prowadzona zgodnie z *backward reasoning* – polega na poszukiwaniu i rozpoznaniu SH dla znanych zdarzeń niepożądanych (UE) lub takich, które są znane z innych, podobnych domen analiz [4].

Dalej przyjmuje się za [8], że proces identyfikacji zagrożeń składa się z dwóch części: procesu identyfikacji HS i procesu charakteryzowania H.

Proces identyfikacji źródeł zagrożeń

Identyfikacja HS zgodnie z *forward reasoning* 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:

- rejestry zdarzeń (wypadków),
- listy pytań kontrolnych,
- metody „burzy mózgów",
- opinie ekspertów.

W procesie identyfikacji zagrożeń zgodnie z *backward reasoning*, identyfikacja HS odbywa się w ramach procedur: formułowania zagrożeń i rozpoznawania źródeł zagrożeń. Istotną różnicą w stosunku do *forward reasoning* jest to, że HS identyfikuje się na podstawie sformułowanych H. Nie ma potrzeby ich grupowania, co jest jedną z kluczowych procedur w procesie identyfikacji zagrożeń typu *forward identification*. W tym sposobie identyfikacji do H „przynależy" określona grupa HS.

Jako narzędzie szczególnie przydatne w identyfikacji zagrożeń z wykorzystaniem *backward reasoning* są rejestry zdarzeń/wypadków. Stworzone dla podobnych domen analiz, pozwalają zakładać, że analogiczne zdarzenia/wypadki będą miały miejsce w aktualnie analizowanej domenie.

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

Teoretycznie, każdy z elementów domeny analiz może być generatorem narażeń tj. może być uznany za HS. Zwykle jednak za takie uznaje się twory, z których aktywnością i/lub występowaniem są związane domniemane straty/szkody. Występuje zatem związek HS z poczuciem strachu, obawy przed konsekwencjami UE.

Należy zwrócić uwagę aby odpowiednio ograniczyć zakres poszukiwania HS i zakres wskazywanych UE. Proponuje się aby w przypadku realizowania procesu identyfikacji typu *backward identification*, nie wskazywać HS spoza analizowanej poddomeny. Kluczowe jest tutaj prawidłowo przeprowadzenie charakteryzowania domeny analiz podlegającej procesowi identyfikacji zagrożeń.

Proces charakteryzowania zagrożeń

W procesie charakteryzowania H występują przynajmniej trzy etapy: grupowanie HS, formułowanie H, określenie strat związanych z aktywizacją H. Zgodnie z tymi etapami należy zrealizować odpowiednie procedury, tj. procedurę grupowania HS, procedurę formułowania H. W ramach procesu występują ponadto następujące obiekty jako dane i rezultaty procesu identyfikacji zagrożeń, tj. listy pogrupowanych HS, lista H i potencjalnych strat.

Grupowanie HS polega na utworzeniu grup (list) źródeł, których występowanie i wspólna aktywność w domenie analiz postrzegane jest jako stan tej domeny prowadzący do UE.

Utworzenie grupy HS następuje poprzez ich wskazanie (np. wyodrębnienie z listy HS) i myślowe powiązanie według pewnej zasady wspólnej aktywności. Na podstawie grup HS dokonuje się formułowania H.

Formułowanie zagrożeń można rozumieć potocznie jako sposób wyrażenia i zapisania strachu powodowanego obecnością/aktywnością HS rozpoznanych w domenie analiz.

Do sformułowania H w większości przypadków wystarczają informacje dotyczące tylko jednego HS (*forward identification*) lub UE (*backword identification)*, które identyfikuje się w domenie analiz. Na ogół jest jednak tak, że sformułowanie H staje się możliwe dopiero na podstawie wiedzy o kilku HS (tzn. grupy HS), o kilku odbiornikach narażeń oraz braku lub nieprawidłowym funkcjonowaniu elementów systemów bezpieczeństwa (RRM – *Risk Reduction Measures*).

2. KARTA CHARAKTERYSTYKI ZAGROŻENIA

2.1. Postać karty

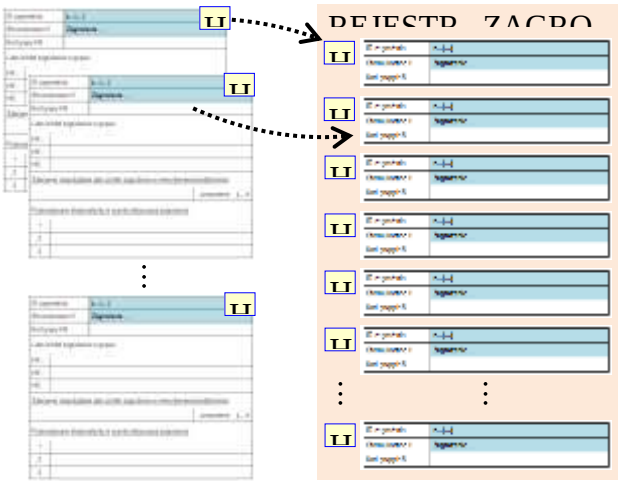
Karta charakterystyki zagrożenia służy do przechowywania najważniejszych informacji uzyskanych w prawidłowo prowadzonym procesie identyfikacji zagrożeń. Rejestr zagrożeń tworzony jest z kart charakterystyk zagrożeń w liczbie odpowiadającej liczbie zidentyfikowanych H. Do przeglądu rejestru wykorzystywać można jego skróconą formę zawierającą tylko nagłówki kart charakterystyk

zagrożeń. Przykładową postać/formę karty charakterystyki zagrożenia przedstawia tabela 1.

***Tab. 1.** Postać/format karty charakterystyki zagrożenia jako składowej rejestru zagrożeń*

ID zagrożenia	**H...(...)**
Sformułowane H	**Zagrożenie ...**
Kod grupy HS	
Lista źródeł i/lub makroźródeł zagrożenia w grupie:	
HS...	
HS...	
HS...	
Zdarzenie niepożądane jako źródło zagrożenia w innej domenie/poddomenie:	
oznaczenie: (... >	
Przewidywane straty/szkody w wyniku aktywizacji zagrożenia:	
1	
2	
3	

Skróconą formę RZ i sposób jej przygotowania przedstawiono schematycznie na rysunku 2.



***Rys. 2.** Schemat ideowy tworzenia rejestru zagrożeń*

2.2. Wytyczne zapisu HS

Należy dążyć do wskazywania HS na jednakowym poziomie szczegółowości (przynajmniej w ramach jednej poddomeny). Często dla HS zidentyfikowanego w poddomenie można wskazać także jego odwzorowania. Przykładowo, dla odwzorowania błędu człowieka operatora (HS1) można użyć rodzaje tego błędu takie jak: pominięcie (HS1.1), naruszenie (HS1.2), nieuwaga (HS1.3). Takie odwzorowania HS należy traktować jako źródła zagrożeń na wyższym poziomie szczegółowości.

W przypadku kilku takich HS, z których każde może być obecne/aktywne w domenie analiz, ale obecność/aktywność jednego z nich wyklucza obecność/aktywność pozostałych HS, proponuje się powołanie tzw. makroźródła zagrożenia. Makroźródło zagrożenia łączy w sobie przynajmniej dwa wykluczające swoją obecność/aktywność HS. Między źródłami makroźródła zagrożenia występują zatem relacje alternatywy wykluczającej. Odpowiada ona wyrażeniu: "albo ... albo ..." i dotyczy wyboru między kilkoma (najmniej dwoma) wykluczającymi się odwzorowaniami. Do oznaczenia alternatywy wykluczającej można użyć symbolu "±". Jeżeli przykładem makroźródła HS1 zagrożenia jest błąd człowieka operatora, a jego odwzorowaniami (źródłami zagrożenia) są wymienione wcześniej rodzaje tego błędu (HS1.1, HS1.2, HS1.3), to korzystając z przyjętych oznaczeń można utworzyć zapis makroźródła zagrożenia HS1 w sposób następujący:

$$(HS1.1 \pm HS1.2 \pm HS1.3) .$$

Wytyczne zapisu grup źródeł zagrożeń

Grupa źródeł zagrożenia składa się ze źródeł i/lub makroźródeł zagrożenia, których konieczność obecności/aktywności w domenie analiz – wg odpowiedniej zasady – doprowadza do aktywizacji zagrożenia. Zasadę konieczności bycia obecnym/aktywnym przez poszczególne źródła i/lub makroźródła zagrożenia tworzące grupę źródeł zagrożeń, można zapisać za pomocą zdań logicznych z wykorzystaniem operatorów (łączników/symboli) logicznych (symbol alternatywy – „+", symbol koniunkcji – „&").

Do zapisu grupy HS przygotowano odpowiednią notację. Zapis grupy HS składa się z kodów identyfikujących źródła i/lub makroźródła zagrożenia (tzw. ID źródła lub makroźródła zagrożenia) np. HS1, HS5, HS17 oraz operatorów (łączników/symboli) logicznych łączących te kody w zdania logiczne. (liczby występujące w ID źródeł lub makroźródeł zagrożenia nie mają charakteru porządkowego).

W tabeli 2 podano przykłady i interpretacje zapisó2.3. grup HS stosowane w karcie charakterystyki zagrożenia rejestru zagrożeń.

***Tab. 2.** Przykłady i interpretacje zapisów grup źródeł zagrożeń stosowanych w karcie charakterystyki zagrożenia rejestru zagrożeń*

Zapis grupy HS	Interpretacja zapisu grupy HS
HS1	grupę źródeł zagrożenia tworzy jedno źródło lub makroźródło zagrożenia; do aktywizacji zagrożenia wystarczy obecność/aktywność jednego źródła lub makroźródła
HS1+HS2	grupę źródeł zagrożenia tworzą łącznie dwa źródła i/lub makroźródła zagrożenia; do aktywizacji zagrożenia wystarczy obecność/aktywność tylko jednego z nich
HS1+HS2+...+HS*n*	grupę źródeł zagrożenia tworzy łącznie *n* źródeł i/lub makroźródeł zagrożenia; do aktywizacji zagrożenia wystarczy obecność/aktywność tylko jednego z nich
HS1&HS2	grupę źródeł zagrożenia tworzą łącznie dwa źródła i/lub makroźródła zagrożenia; do aktywizacji zagrożenia konieczna jest jednoczesna obecność/aktywność obydwu z nich
HS1&HS2&...&HS*n*	grupę źródeł zagrożenia tworzy łącznie *n* źródeł i/lub makroźródeł zagrożenia; do aktywizacji zagrożenia konieczna jest jednoczesna obecność/aktywność wszystkich z nich
(HS1+HS2)&HS3	grupę źródeł zagrożenia tworzą łącznie trzy źródła i/lub makroźródła zagrożenia; do aktywizacji zagrożenia wystarczy obecność/aktywność jednego ze źródeł i/lub makroźródeł HS1 i HS2 oraz obecność/aktywność źródła lub makroźródła zagrożenia HS3

Wytyczne formułowania i zapisu zagrożenia

Prawidłowo sformułowane H pełni rolę informacyjną oraz w pewnym sensie ostrzegawczą. W procesie identyfikacji H powinno natomiast dostarczać informacji o [1]:

- źródle lub źródłach zagrożenia, których wspólna aktywność może doprowadzić do zdarzeń,
- odbiorcy/odbiorniku narażeń (ON),
- sposobie w jaki grupa źródeł zagrożeń realizuje oddziaływanie na odbiornik narażeń,
- konsekwencjach aktywizacji zagrożenia,
- czynnikach eskalujących w procesie aktywizacji zagrożenia.

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 stosowanych w zarządzaniu ryzykiem zagrożeń, np.

w metodzie Bow-Tie, rozpatruje się także aspekt reputacji podmiotów związanych z domeną analiz [9, 10].

W ID zagrożenia – oprócz kolejnego numeru H sformułowanego w ramach poddomeny analiz – podaje się także oznaczenie tej poddomeny. Wtedy ID pojedynczego H może mieć następującą postać np.: H1(2.3), H2-2.3 lub H3/2.3. Takie oznaczenie sformułowanego H ma ułatwić tworzenie rejestru zagrożeń i zarządzanie danymi znajdującymi się w rejestrze.

Wytyczne dotyczące znaczników przeniesienia UE/HS

Charakterystyczny znacznik przeniesienia dotyczy zapisu numerów przypisanych poddomenom, do których kierowane/adresowane jest UE jako SH (rys. 1). Proponuje się przyjąć dwa następujące schematy tworzenia znaczników przeniesienia:

(1) Kierowanie zdarzenia jako źródła zagrożenia z bieżącej poddomeny analiz np. poddomeny 3.1 do poddomeny docelowej np. poddomeny 2.3 – zapisać jako: (2.3>

(2) Przyjmowanie w poddomenie analiz, np. w poddomenie 3.1 źródła zagrożenia jako zdarzenia wskazanego w poddomenie 2.3 – zapisać jako: (2.3> {nazwa_źródła_zagrożenia}.

PODSUMOWANIE

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 wskazanie oznaczenia (kodu) domeny lub poddomeny analiz, w których wskazane zdarzenie powinno być rozważane jako źródło zagrożenia, listę strat/szkód będących opisem konsekwencji aktywizacji zagrożenia. Informacje potrzebne do przygotowania segmentów rejestru zagrożeń są łatwe do uzyskania z dokumentacji prawidłowo przeprowadzanego procesu identyfikacji zagrożeń.

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*, Autobusy – Technika, Eksploatacja, Systemy transportowe, nr 12, 2011, s. 104-114.
3. Gill A., Kadziński A., *The identyfication 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, 2016 Oct 5-7, Juodkrantė, Lithuania.
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. Kadziński A., Gill A., *Integracja pojęć*, podrozdział 7.3.2 w: praca zbiorowa red. R. Krystek, Zintegrowany system bezpieczeństwa transportu, II tom, Uwarunkowania rozwoju integracji systemów bezpieczeństwa transportu, Politechnika Gdańska, WKŁ, Warszawa 2009, s. 285-288.
7. Kadziński A., Gill A., Pruciak K., Rozpoznawanie źródeł zagrożeń jako ważny element metod zarządzania ryzykiem w komunikacji tramwajowej, Technika Transportu Szynowego, nr 9, 2011, s. 49-52.
8. Kadziński A., *Studium wybranych aspektów niezawodności systemów oraz obiektów pojazdów szynowych*, Wyd. Politechniki Poznańskiej, seria Rozprawy, nr 511, Poznań 2013.
9. 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.
10. Kobaszyńska-Twardowska A., Gill A., *Realizacja procedur oceny ryzyka zagrożeń z użyciem procedur Bow-Tie*, Pojazdy Szynowe, nr 2, 2014, s. 1-10.
11. PN-N-18002:2000, Systemy zarządzania bezpieczeństwem i higieną pracy. Ogólne wytyczne do oceny ryzyka zawodowego, Polski Komitet Normalizacyjny, Warszawa 2000.
12. PN-N-18002:2011, Systemy zarządzania bezpieczeństwem i higieną pracy. Ogólne wytyczne do oceny ryzyka zawodowego, Polski Komitet Normalizacyjny, Warszawa 2011.
13. 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.
14. Urbański M., *Rozumowania abdukcyjne. Modele i procedury*, Wyd. Naukowe UAM, Poznań 2009, wersja elektroniczna: http://hdl.handle.net/10593/1025.
15. Zintegrowany system bezpieczeństwa transportu, III tom, Koncepcja zintegrowanego systemu bezpieczeństwa transportu w Polsce, praca zbiorowa pod red. R. Krystek, Politechnika Gdańska, podrozdział 4.3, Jamroz K., Chruzik K., Gucma L., Kadziński A., Skorupski J., Szymanek A., Koncepcja metody zarządzania ryzykiem w transporcie, s. 133-151, WKŁ, Warszawa 2010.

Hazard record

This paper deals with an important step of the risk management methods – implementation of the hazard identification process (HIP) and preparation of the hazard record (HR). The HR is a final result of the HIP. We present the way of gathering information for preparing the HR and some forms of the record. Referring to the HR format, we provide the guidelines / recommendations for filling in the fields of a hazard data sheet concerning a single hazard.

Autorzy:

dr inż. **Adrian Gill** – Politechnika Poznańska, Instytut Silników Spalinowych i Transportu, Zakład Pojazdów Szynowych, e-mail: adrian.gill@put.poznan.pl, tel. 61 6652017

dr hab. inż. **Adam Kadziński** – Politechnika Poznańska, Instytut Silników Spalinowych i Transportu, Zakład Pojazdów Szynowych, e-mail: adam.kadzinski@put.poznan.pl, tel. 61 6652267