mgr inż. Adrian Gill
dr inż. Adam Kadziński
Politechnika Poznańska

System obsługiwania pojazdów szynowych jako element w warstwowym modelu ich systemów bezpieczeństwa

W artykule przedstawiono koncepcję organizacji systemu obsługiwania obiektów pojazdów szynowych (ops), jako elementu w warstwowym modelu systemu bezpieczeństwa tych obiektów. Koncepcja metody polega na zastosowaniu warstwy zabezpieczeń w postaci systemu okresowych obsług profilaktycznych. Analizę systemu bezpieczeństwa przeprowadzono metodą Analizy Warstw Zabezpieczeń (AWZ). Przedstawiono algorytm metody AWZ dla ops. Podano sposób optymalizacji czasu między obsługami elementów ops.

1. Wprowadzenie

Rosnąca złożoność i koszt obiektów technicznych, obawa przed wyczerpywaniem się zasobów surowcowych, konieczność ochrony środowiska oraz względy ekonomiczne spowodowały rozwój zagadnień eksploatacji obiektów [17]. Szczególne znaczenie przypisuje się przy tym zagadnieniu obsługiwania obiektów, którego doskonalenie może wpłynąć na utrzymanie wysokiej produktywności i niezawodności obiektów. W wyniku takiego podejścia opracowano wiele strategii i metod obsługiwania obiektów technicznych. Do najbardziej znanych z nich – za autorem pracy [17] – można zaliczyć: obsługiwanie nakierowane na niezawodność (*Reliability Centred Maintenance* – RCM), obsługiwanie według stanu obiektu (*Condition Based Maintenance* – CBM), kompleksowe traktowanie problemu, pełne obsługiwanie produkcyjne (*Total Productive Maintenance* – TPM), wspomagane komputerowo zarządzanie obsługiwaniem (*Computer Aided Maintenance Managment* – CAMM). Autor pracy [19] proponuje podział metod obsługiwania na: metody dynamiczne czyli obsługiwanie według stanu technicznego, metody quasi-dynamiczne i metody statyczne. Wszystkie systemy obsługiwania oparte na wymienionych tu metodach, są systemami planowo-zapobiegawczymi.

W przypadku obiektów technicznych o istotnym wpływie na bezpieczeństwo ludzi, problem obsługiwania nabiera szczególnego znaczenia. Uzasadniona może być zatem potrzeba tworzenia nowych metod obsługiwania uwzględniających m.in. stopień tego wpływu. Jak podaje autor pracy [9], w ostatnich kilku latach nastąpił rozwój metod obsługiwania wykorzystujących miary ryzyka. Są to tzw. metody obsługiwania na podstawie ryzyka (*Risk Based Maintenance* – RBM). Za pomocą miar ryzyka można ocenić stopień wpływu uszkodzeń obiektów technicznych na bezpieczeństwo ludzi, środowisko i funkcjonowanie samych obiektów. Metody RBM znajdują więc zastosowanie szczególnie do obiektów, których uszkodzenie może być przyczyną zagrożenia bezpieczeństwa ludzi lub środowiska. W różnych opracowaniach, np. w [3, 9, 18, 23], podano przykłady zastosowania RBM do różnego typu obiektów technicznych. Prezentowaną w artykule koncepcję organizacji systemu obsługiwania obiektów pojazdów szynowych (*ops*) można zaliczyć także do metod RBM.

2. Koncepcja i główne założenia metody

Aby zmniejszyć ryzyko związane z uszkodzeniami obiektów technicznych stosuje się różnego rodzaju zabezpieczenia. Najczęściej są to zabezpieczenia o charakterze technicznym np. urządzenia alarmowe, osłony fizyczne, układy zabezpieczające. Innym sposobem redukcji ryzyka jest zastosowanie systemów bezpieczeństwa o charakterze organizacyjnym, czyli np. zespołu ludzi działających według ustalonych wcześniej odpowiednich procedur postępowania. Zasadność organizacyjnych rozwiązań redukcji ryzyka wskazuje m.in. autor pracy [6] podkreślając stosunkowo niski (bezinwestycyjny) koszt ich realizacji. Największe korzyści może przynieść odpowiednia organizacja systemu obsługiwania obiektów. System taki można potraktować jako system bezpieczeństwa realizujący – za pomocą odpowiednich urządzeń i działań (np. człowieka) – pewną funkcję bezpieczeństwa (system sprzyjający redukcji ryzyka). W organizacji systemu obsługiwania obiektów szczególną uwagę zwraca się na możliwość redukcji ryzyka poprzez unikanie uszkodzenia, które prowadzi do tzw. zdarzeń niepożądanych. Przez **Zdarzenie Niepożądane** (ZN) rozumie się każde zdarzenie powodujące straty w systemie eksploatacji *ops*.

W celu analizy systemu bezpieczeństwa wielu autorów np. [7, 11, 12, 13] proponuje przedstawiać go w postaci warstwowej. Przyjęcie warstwowego modelu

do opisu systemu bezpieczeństwa ułatwia przeprowadzenie analizy i oceny ryzyka, szczególnie w zakresie tworzenia scenariuszy zdarzeń niepożądanych. Prezentowana koncepcja organizacji systemu obsługiwania *ops* polega na wykorzystaniu procedur analizy i oceny ryzyka związanego z uszkodzeniem obiektu w celu konfiguracji warstwy zabezpieczeń zorganizowanej w postaci systemu okresowych obsług profilaktycznych.

Istotą warstwowego modelu systemu bezpieczeństwa jest podział wszystkich czynników, mających wpływ na wzrost bezpieczeństwa, na niezależne od siebie grupy – tzw. **Niezależne Warstwy Zabezpieczeń** (NWZ). Przyjmując taką koncepcję systemu bezpieczeństwa *ops* założono wstępnie, że składa się on z dwóch głównych warstw:

1. **Warstwy zapobiegania**, której zadaniem jest nie dopuszczanie do powstawania warunków do wystąpienia uszkodzenia obiektu. Można tutaj wymienić odpowiednie procedury użytkowania, obsługiwania obiektów, itp.
2. **Warstwy przeciwdziałania** poważnym skutkom uszkodzeń, której zadaniem jest zabezpieczenie systemu przed poważnymi następstwami uszkodzenia obiektu.

Jeśli zagrożenia są właściwie kontrolowane, to występuje poziom ryzyka określany jako akceptowany. Taki stan jest korzystny z punktu widzenia zapewnienia bezpieczeństwa, ale nie zawsze jest korzystny ekonomicznie. Autor pracy [7] podaje przykład firmy Shell Global Solutions, która w oparciu o normę IEC 61508 przeprowadziła analizę stosowanych zabezpieczeń. W wyniku tej analizy firma uznała, że 65% tych zabezpieczeń jest przeinwestowanych. Jeden z powodów stosowania tak nieracjonalnie rozbudowanych systemów ochrony wymienia autor pracy [21]. Wskazuje on, że wiele firm, aby uniknąć problemów z zapewnieniem bezpieczeństwa, wprowadza zabezpieczenia o najwyższym poziomie pewności działania bez przeprowadzenia analizy ryzyka. W wyniku takiej analizy można przecież otrzymać informacje niezbędne do oceny ryzyka a to z kolei, jak podaje [15], umożliwia podejmowanie wyważonych decyzji o bezpieczeństwie związanym z obiektem. Analiza ryzyka dostarcza ponadto miary pozwalające na uwzględnienie i porównanie ze sobą wielu czynników decyzyjnych [20].

System bezpieczeństwa może zatem realizować nadmierną liczbę funkcji bezpieczeństwa, które generują często istotne koszty zarówno inwestycyjne jak i eksploatacyjne. Uzasadniona jest więc racjonalizacja zależności między występującymi zagrożeniami a stosowanymi lub projektowanymi systemami bezpieczeństwa. W podejmowaniu racjonalnych decyzji możliwe jest wykorzystanie oceny ryzyka wspartej odpowiednimi metodami jego analizy. W przypadku stosowania wielowarstwowych systemów bezpieczeństwa, autor pracy [12] proponuje wykorzystanie tzw. **Analizy Warstw Zabezpieczeń** (AWZ). Główne etapy AWZ oraz przykłady jej zastosowania, zaprezentowano m.in. w pracach [2, 12]. Za pomocą AWZ ustalono wymagania, jakie spełniać musi system obsługiwania *ops*. Algorytm AWZ dla obiektów pojazdów szynowych przedstawiono na rysunku 1.

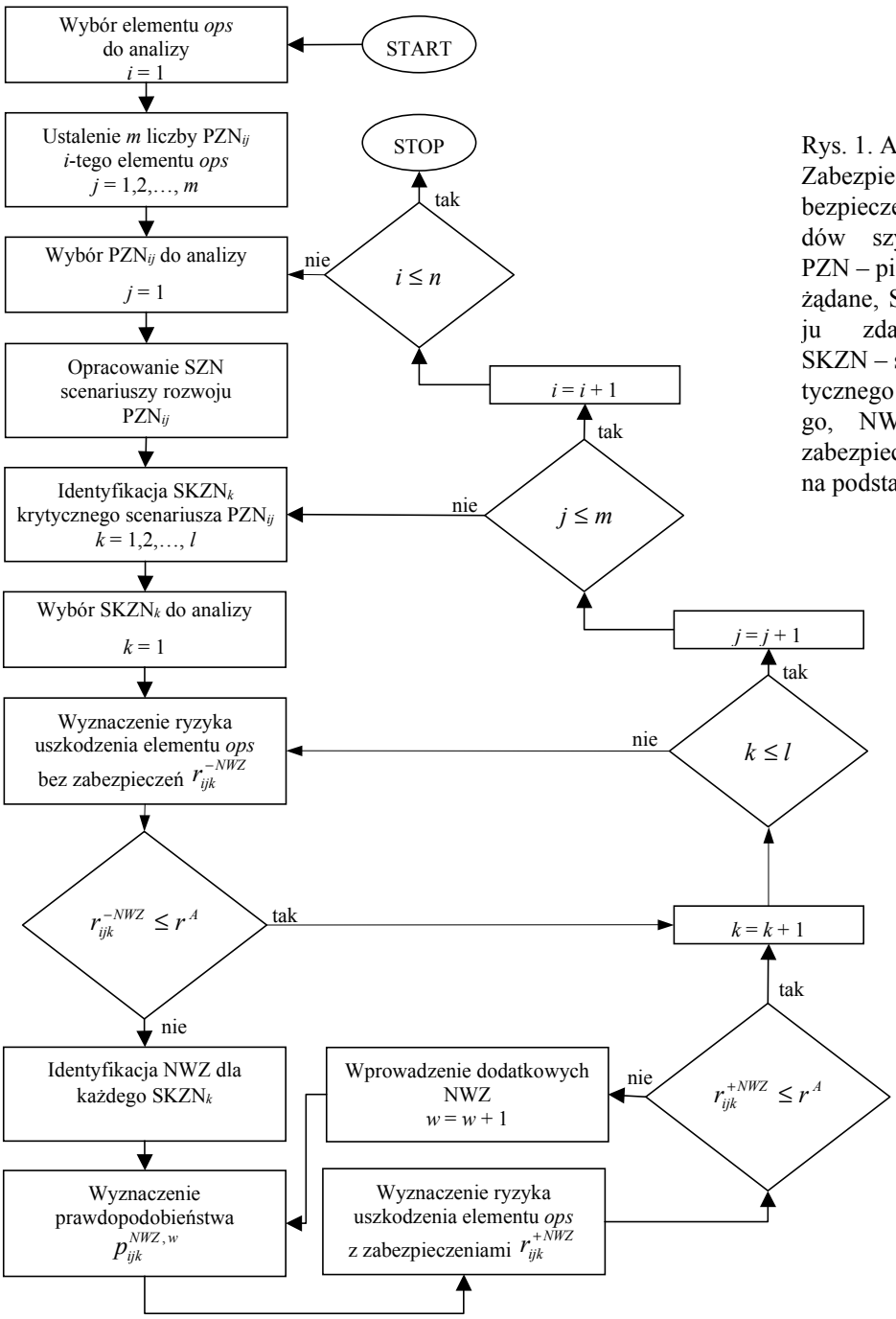
3. Analiza Warstw Zabezpieczeń (AWZ) dla systemu bezpieczeństwa obiektów pojazdów szynowych

Podstawą AWZ jest zastosowanie pojęcia ryzyka rozumianego jako wzajemna relacja między występującymi zagrożeniami procesowymi a zastosowanymi systemami bezpieczeństwa [13]. Jako obiekt analizy przyjęto silnik spalinowy 2112SSF lokomotyw. W celu identyfikacji zagrożeń związanych z eksploatacją tego silnika wykorzystano dane historyczne o uszkodzeniach tego typu obiektów oraz **Wstępną Analizę Zagrożeń (** PHA) [16].

Na podstawie identyfikacji zagrożeń wskazano tzw. **Pierwotne Zdarzenia Niepożądane** (PZN), którymi są uszkodzenia elementów *ops* (rys. 1). PZN mogą inicjować sekwencję wtórnych ZN [24]. Przykładem wtórnego ZN może być wyciek paliwa spowodowany uszkodzeniem przewodów paliwowych niskiego ciśnienia, który stanowi źródło potencjalnego pożaru lub wybuchu, czyli np. zgodnie z normą PN-EN 1050, zagrożenie termiczne związane z zapłonem substancji palnej.

Lista ZN inicjowanych przez PZN może być znacznej długości. W takich przypadkach celowe jest jej skrócenie do tzw. **Krytycznych Zdarzeń Niepożądanych** (KZN). KZN należy rozumieć **–** podobnie jak np. w pracy [13] **–** jako zdarzenia, które mogą wystąpić nie tylko teoretycznie i charakteryzują się najpoważniejszymi potencjalnymi skutkami. Listę taką można utworzyć na podstawie oceny stopnia dotkliwości zdarzenia lub poziomu częstości jego występowania. Istotnym krokiem algorytmu AWZ (rys. 1) jest ustalenie **Scenariuszy** powstawania **Zdarzeń Niepożądanych** (SZN).

W celu opracowania SZN korzysta się najczęściej z **Analizy Drzewa Zdarzeń** (ETA – *Event Tree Analysis*). ETA jest metodą indukcyjną polegającą na tzw. „myśleniu do przodu". W technice drzewa zdarzeń analizowane są możliwości rozwoju PZN (nazywanych w ETA zdarzeniami inicjującymi), względem funkcjonowania systemów bezpieczeństwa znajdujących się w danym systemie (np. technicznym) i/lub oddziaływania niektórych warunków zewnętrznych [13]. Przyjmuje się, że to funkcjonowanie zachodzi zawsze według dwóch stanów logicznych: sukces („tak") i niepowodzenie („nie"). W wyniku rozwoju PZN otrzymuje się zdarzenia wyjściowe (ZWY). ZWY kończą sekwencję zdarzeń w drzewie zdarzeń.

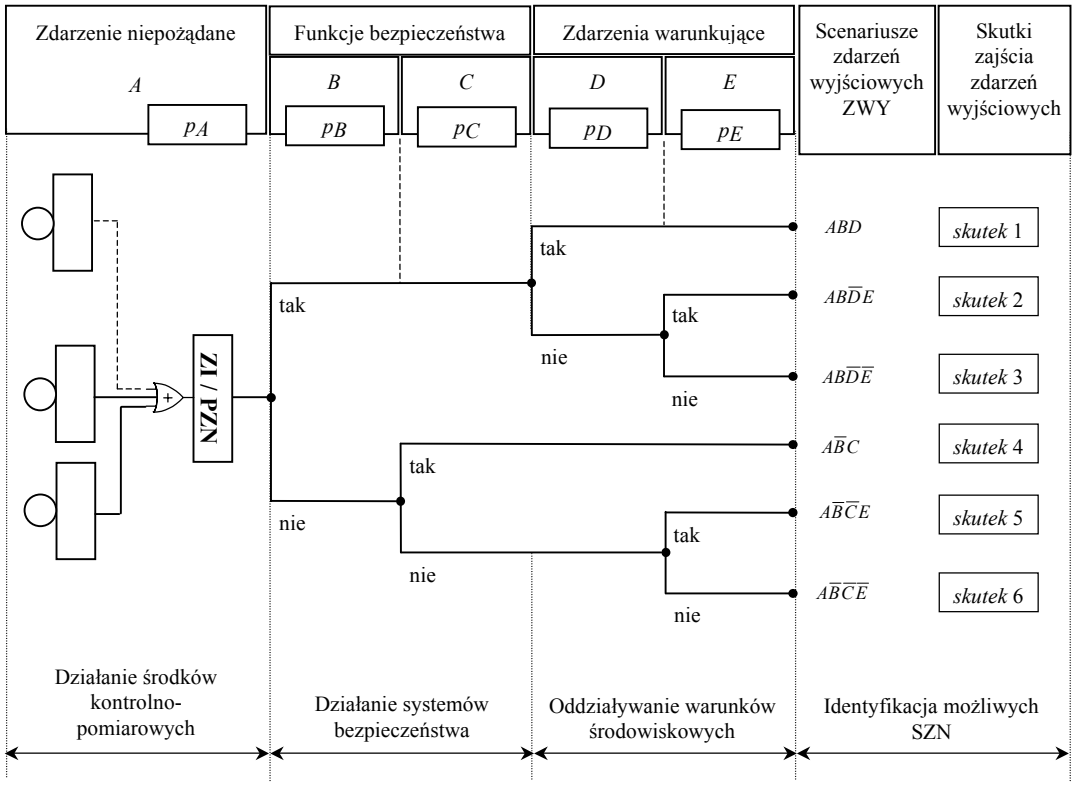


Rys. 1. Algorytm Analizy Warstw Zabezpieczeń (AWZ) dla systemu bezpieczeństwa obiektów pojazdów szynowych (*ops*), gdzie: PZN – pierwotne zdarzenie niepożądane, SZN – scenariusze rozwoju zdarzenia niepożądanego, SKZN – scenariusze rozwoju krytycznego zdarzenia niepożądanego, NWZ – niezależne warstwy zabezpieczeń (opracowanie własne na podstawie [12])

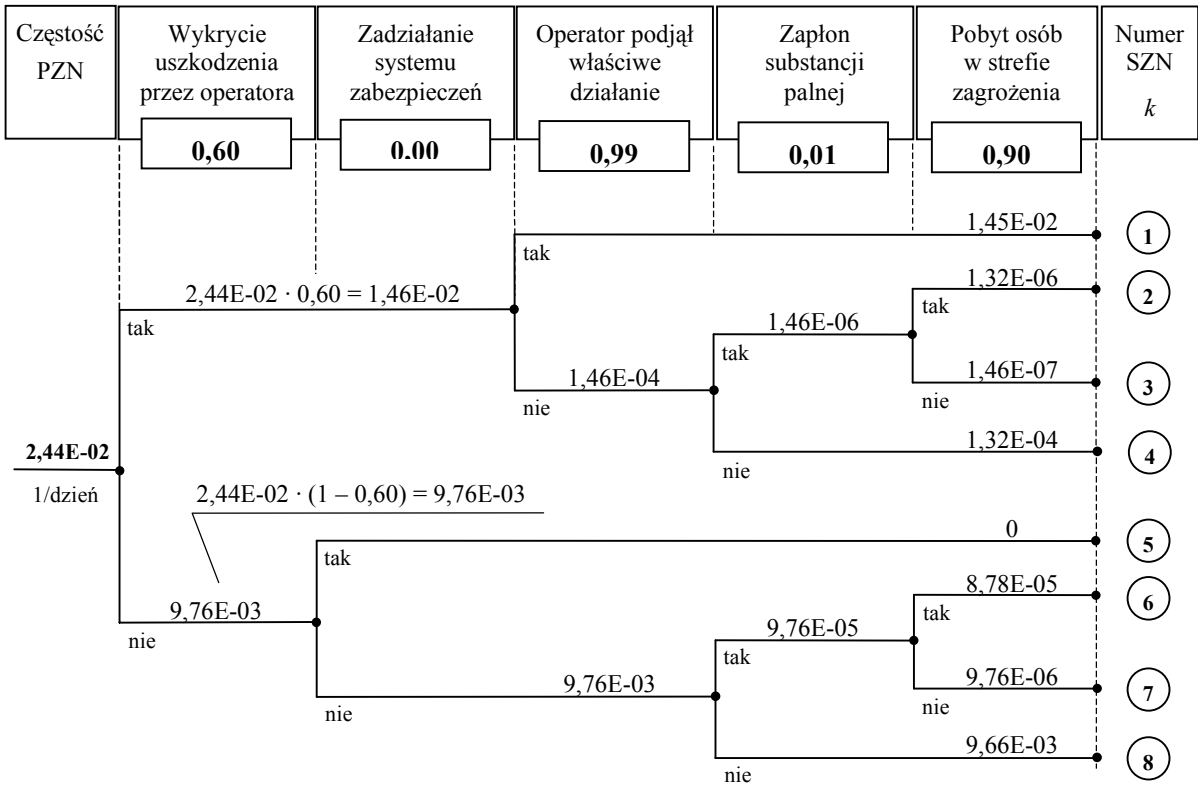
Procedura metody ETA składa się z sześciu następujących etapów [13]:

1. Wskazanie zdarzenia inicjującego lub zdarzenia szczytowego.
2. Identyfikacja oraz opis systemów bezpieczeństwa i oddziaływania warunków zewnętrznych spełniających określone funkcje bezpieczeństwa.
3. Konstrukcja drzewa zdarzeń.
4. Określenie sekwencji zdarzeń powodujących ZN lub określone zagrożenie.
5. Ilościowa analiza drzewa zdarzeń.
6. Dokumentacja analizy drzewa zdarzeń.

Etap 1. Podstawą do rozpoczęcia budowy drzewa zdarzeń jest wskazanie **Zdarzenia Inicjującego** (ZI). W prezentowanej metodzie przyjęto, że ZI są uszkodzenia *ops*. Uszkodzenia obiektów można klasyfikować według różnych kryteriów np. charakteru ujawniania się uszkodzenia. Uszkodzenia *ops* podzielono na: uszkodzenia nagłe (przeciążeniowe) i uszkodzenia starzeniowe (w wyniku stopniowego zużywania). Uszkodzenia te są zdarzeniami niezależnymi i stąd też w procedurze wyznaczania prawdopodobieństwa odpowiednich ZWY powinny być uwzględniane oddzielnie. Schemat ideowy rozwoju scenariuszy PZN przedstawiono na rysunku 2.



Rys. 2. Schemat ideowy scenariuszy rozwoju pierwotnego zdarzenia niepożądanego (PZN) – opracowanie własne na podstawie [13, 24]



Rys. 3. Przykład identyfikacji scenariuszy rozwoju pierwotnego zdarzenia niepożądanego (PZN) jakim jest uszkodzenie przewodów paliwowych niskiego ciśnienia w silniku lokomotyw spalinowych

Etap 2. Systemy bezpieczeństwa i ochrony spełniają określone zadania zwane funkcjami bezpieczeństwa. Zwykle mogą to być: automatyczne zamknięcia instalacji, alarmy informujące operatora o sytuacji wypadkowej (o zagrożeniu), ustalone procedury działań w sytuacji wypadkowej, fizyczne systemy ograniczania skutków czyli tzw. systemy i/lub elementy bezpieczeństwa biernego.

W trakcie tego etapu ETA należy w badanym systemie zdefiniować wszystkie systemy bezpieczeństwa i określić ich funkcje bezpieczeństwa. Dla potrzeb ilościowej analizy zdarzeń należy również określić prawdopodobieństwo ich prawidłowego zadziałania lub prawdopodobieństwo niezadziałania.

Innym ważnym elementem drugiego etapu ETA jest określenie warunków środowiskowych mogących mieć wpływ na rozwój ZI. Są to warunki meteorologiczne, prędkość i kierunek wiatru, stabilność atmosferyczna oraz występowanie natychmiastowych lub opóźnionych źródeł zapłonu. Podobnie jak w przypadku „funkcji bezpieczeństwa" należy określić prawdopodobieństwo ich występowania lub prawdopodobieństwo niewystępowania.

Etap 3. Konstrukcję drzewa zdarzeń w metodzie ETA rozpoczyna się od wskazania zdarzenia inicjującego oraz określenia funkcji bezpieczeństwa realizowanych przez wskazane systemy bezpieczeństwa. Ilustruje to przykładowo rysunek 2. Rozwój PZN rozpatruje się kolejno względem określonych funkcji bezpieczeństwa (oznaczonych literami *B* i *C*) oraz warunków środowiskowych (oznaczonych literami *D* i *E*). Konstrukcja drzewa zdarzeń doprowadza do uzyskania ZWY.

Etap 4. Uzyskane zdarzenia ZWY reprezentują określone sekwencje zdarzeń, odwzorowujące działanie lub niezadziałanie funkcji bezpieczeństwa na zdarzenie inicjujące. Na przykład sekwencja ABD oznacza, że zaszło zdarzenie *A* i z sukcesem zadziałała funkcja bezpieczeństwa *B* oraz funkcja bezpieczeństwa *D*. Sekwencja $A\overline{B}C$ oznacza zaś, że zaszło zdarzenie inicjujące *A*, funkcja bezpieczeństwa *B* systemu bezpieczeństwa nie zadziałała (niepowodzenie) oraz funkcja bezpieczeństwa *C* zadziałała (sukces).

Etap 5. Ilościowa analiza drzewa zdarzeń polega na określeniu prawdopodobieństwa występowania zdarzeń ZWY. Uzyskuje się to poprzez kolejne mnożenie częstości (lub prawdopodobieństwa) wystąpienia zdarzenia inicjującego przez prawdopodobieństwa wystąpienia warunków związanych z daną gałęzią drzewa. Dla gałęzi odpowiadającej sukcesowi („tak") przyjmuje się prawdopodobieństwo sukcesu q_s, natomiast dla gałęzi odpowiadającej niepowodzeniu („nie") przyjmuje się prawdopodobieństwo $q_n = 1 - q_s$. Suma prawdopodobieństw na każdym rozgałęzieniu musi być równa 1, a suma prawdopodobieństw wszystkich zdarzeń wyjściowych ZWY (gałęzi) powinna być równa wartości częstości występowania zdarzenia inicjującego. Na rysunku 3 przedstawiono przykład identyfikacji scenariuszy rozwoju PZN jakim jest uszkodzenie przewodów paliwowych niskiego ciśnienia w przyjętym silniku lokomotyw spalinowych.

Etap 6. Ostatnim etapem metody jest opracowanie dokumentacji analizy drzewa zdarzeń. Należy tu przedstawić listę sekwencji zdarzeń prowadzących do zagrożeń, jak również wynikające z analizy zalecenia co do poprawy stanu bezpieczeństwa, np. dodatkowe funkcje bezpieczeństwa i ich wpływ na obniżenie prawdopodobieństwa występowania zagrożeń.

Przyjęto, że zanim dojdzie do wypadku operator może zauważyć (wykryć) 60% powstałych uszkodzeń. Działając bez stresu podejmuje on w 99% właściwe działania zapobiegawcze [2]. Określenie prawdopodobieństwa wykrycia uszkodzenia przez operatora stanowi jednak osobne zagadnienie, które może być analizowane bardziej szczegółowo, np. przy pomocy analizy drzewa błędów. W analizie tej można uwzględnić prawdopodobieństwo reakcji operatora na urządzenia alarmowe, wykrywalność danego typu uszkodzenia, itp.

4. Konfiguracja warstwy zabezpieczeń obiektów pojazdów szynowych

Aby zmniejszyć ryzyko związane z uszkodzeniami obiektów pojazdów szynowych przeprowadza się obsługi profilaktyczne. Przyjęto zatem, że pierwsza z warstw w systemie bezpieczeństwa *ops* – tj. warstwa zapobiegania – jest zorganizowana w postaci systemu okresowych obsług profilaktycznych.

W *ops* – np. w silniku spalinowym – można wyróżnić różnego typu układy (podzespoły) złożone z określonej liczby elementów. Można ponadto założyć, że każdy z tych elementów charakteryzuje się innym poziomem ryzyka związanego z jego uszkodzeniem. Oznacza to, że w zależności od elementu układu będzie istniało inne wymaganie dla systemu obsługiwania – inny poziom nienaruszalności bezpieczeństwa SIL (*Safety Integrity Level*). Można także wstępnie założyć, że tylko niektóre z elementów posiadają dwuwarstwowy system bezpieczeństwa.

Przyjęto, że system obsługiwania, uwzględniający wymienione tu założenia, powinien zapewniać akceptowany poziom ryzyka uszkodzenia *ops* złożonego z *n*-tej liczby elementów, jeżeli dla *i*-tego elementu tego obiektu spełniona będzie zależność:

$$\bigvee_{i=1,2,\ldots,n} r_i \le r^A \qquad (1)$$

gdzie:

r_i – ryzyko związane z uszkodzeniem *i*-tego elementu obiektu pojazdu szynowego

r^A – akceptowana wartość ryzyka uszkodzenia obiektu pojazdu szynowego.

Straty spowodowane uszkodzeniem elementu *ops* można rozpatrywać uwzględniając rodzaj powstałego uszkodzenia. Korzystając z metody drzewa zdarzeń można określić prawdopodobieństwo $p(s_{ijk})$ występowania tych strat z następującej zależności:

$$p(s_{ijk}) = f_{ij}^{ZI} \cdot \prod_{w} p_{ijk}^{NWZ,w} \cdot \prod_{v} p_{ijk}^{ZW,v}, \quad j = 1,2,...,m,\ k = 1,2,...,l \tag{2}$$

gdzie:

s_{ijk} – strata występująca w *k*-tym scenariuszu zdarzeń związana z *j*-tego rodzaju uszkodzeniem *i*-tego elementu obiektu pojazdu szynowego

$p(s_{ijk})$ – prawdopodobieństwo wystąpienia straty s_{ijk}

f_{ij}^{ZI} – częstość występowania zdarzenia inicjującego, tj. *j*-tego rodzaju uszkodzenia *i*-tego elementu obiektu pojazdu szynowego

$p_{ijk}^{NWZ,w}$ – prawdopodobieństwo niezadziałania *w*-tej niezależnej warstwy zabezpieczeń (NWZ) obiektu pojazdu szynowego w *k*-tym scenariuszu rozwoju *j*-tego rodzaju uszkodzenia *i*-tego elementu tego obiektu

$p_{ijk}^{ZW,v}$ – prawdopodobieństwo wystąpienia *v*-tego rodzaju zdarzeń warunkujących (ZW) w *k*-tym scenariuszu rozwoju *j*-tego rodzaju uszkodzenia *i*-tego elementu obiektu pojazdu szynowego.

W rozwoju pierwotnego zdarzenia niepożądanego może istnieć sekwencja zdarzeń prowadząca do wystąpienia KZN. KZN charakteryzuje się występowaniem poważnych strat i najczęściej generuje nieakceptowany poziom ryzyka. Sekwencję takich zdarzeń można nazwać scenariuszem rozwoju krytycznego zdarzenia niepożądanego (SKZN). Niech r_{ijk}^{-NWZ} będzie ryzykiem uszkodzenia *i*-tego elementu *ops* w wyniku *j*-tego uszkodzenia w *k*-tym scenariuszu zdarzeń w przypadku braku NWZ.

Aby dokonać odpowiedniej konfiguracji systemów bezpieczeństwa, należy w pierwszej kolejności wyznaczyć wartość r_{ijk}^{-NWZ}. Jeżeli wartość ta przekroczy akceptowany poziom ryzyka r^A, to wprowadza się odpowiednie NWZ. Następnie dokonuje się weryfikacji wprowadzonych rozwiązań wyznaczając r_{ijk}^{+NWZ} ryzyko uszkodzenia *i*-tego elementu *ops* w wyniku *j*-tego uszkodzenia w *k*-tym scenariuszu zdarzeń z funkcjonującymi NWZ. Jedną z takich warstw – warstwą zapobiegania – może być np. system obsług profilaktycznych.

Warstwę zapobiegania należy tak skonfigurować, aby spełniona została zależność (1). Konfigurację NWZ można przeprowadzić w oparciu o jeden scenariusz zdarzeń, tj. scenariusz SKZN prowadzący do KZN. Można jednak ogólnie założyć, że ryzyko związane z uszkodzeniem *ops* będzie akceptowane, jeżeli akceptowaną wartość osiągnie każde ryzyko r_{ijk}^{+NWZ}, tzn. aby:

$$\bigvee_{i=1,2,...,n} \bigvee_{j=1,2,...,m} \bigvee_{k=1,2,...} r_{ijk}^{+NWZ} \le r^A \tag{3}$$

Można ponadto założyć, że ryzyko r_{ijk}^{+NWZ} jest wyrażone prawdopodobieństwem $p(s_{ijk})$ wystąpienia straty s_{ijk}, a wtedy uwzględniając zależności (3) zapisać, że:

$$r_{ijk}^{+NWZ} = p(s_{ijk}) \Rightarrow \bigvee_{k=1,2,...,l} p(s_{ijk}) \le p^A(s_{ijk}) \tag{4}$$

gdzie: $p^A(s_{ij})$ jest akceptowanym prawdopodobieństwem wystąpienia straty s_{ijk} np. prawdopodobieństwem utraty życia przez maszynistę pojazdu szynowego.

Prawdopodobieństwo $p(s_{ijk})$ wystąpienia strat jest zależne m.in. od prawdopodobieństwa $p_{ijk}^{NWZ,w}$ niezadziałania niezależnych warstw zabezpieczeń. Aby spełnić zależność (4) należy określić odpowiednie wymagania w stosunku do NWZ. Wymagania te mogą być zapisane z wykorzystaniem poziomów nienaruszalności bezpieczeństwa SIL w następujący sposób:

$$\begin{aligned}
&10^{-2} < p_{ijk}^{NWZ,w} \le 10^{-1} && \text{dla SIL1} \\
&10^{-3} < p_{ijk}^{NWZ,w} \le 10^{-2} && \text{dla SIL2,} \\
&10^{-4} < p_{ijk}^{NWZ,w} \le 10^{-3} && \text{dla SIL3,} \\
&10^{-5} < p_{ijk}^{NWZ,w} \le 10^{-4} && \text{dla SIL4.}
\end{aligned} \tag{5}$$

Organizację systemu obsługiwania *ops* należy zatem rozpocząć od określenia wymaganego poziomu SIL dla poszczególnych elementów tego obiektu. Ocena SIL ma kluczowe znaczenie dla wyboru koncepcji układu zabezpieczającego i jego zaprojektowania. Ma także decydujący wpływ na treść procedur użytkowania i obsługiwania (eksploatacji) *ops* .

5. Określenie wymaganego poziomu SIL

Metod określenia SIL jest wiele [10, 14, 21]. Spośród metod jakościowych wybrano macierz ryzyka pokazaną m.in. w pracach [1, 21, 22]. Jeśli dysponuje się stosunkowo dokładnymi informacjami o uszkodzeniach obiektów, to w celu identyfikacji poziomu SIL można zastosować metody ilościowe. Wykorzystując wprowadzone wcześniej oznaczenia można zapisać, że:

$$p_{ijk}^{NWZ,w} = \frac{p^{A}(s_{ijk})}{p(s_{ijk})} \tag{6}$$

W obliczeniach przyjęto, że akceptowane prawdopodobieństwo najpoważniejszych skutków tj. utraty życia maszynisty *ops* spowodowane uszkodzeniem elementów obiektu, nie może być większe niż 1,00E-04 [4].

Korzystając z zależności (6) wyznacza się poziom nienaruszalności bezpieczeństwa SIL dla warstwy zabezpieczeń elementów układu paliwowego silników lokomotyw spalinowych, tak jak to pokazano w tabeli 1.

Wyniki identyfikacji poziomu nienaruszalności bezpieczeństwa SIL dla warstw zabezpieczeń elementów układu paliwowego silników lokomotyw spalinowych

Tabela 1

Lp.	Nazwa elementu	Częstość uszkodzeń [1/dzień]	Pożądany poziom nienaruszalności bezpieczeństwa
1	Przewody paliwowe niskiego ciśnienia	2,44E-02	SIL1
2	Przewód paliwowy wysokiego ciśnienia	2,70E-02	SIL1
3	Pompa wtryskowa	7,75E-03	SIL1
4	Wtryskiwacze	3,70E-02	SIL1
5	Filtr paliwa	1,64E-02	SIL1

Źródło: opracowanie własne na podstawie [25]

6. Optymalizacja terminów obsługiwania obiektu

Pewną koncepcję optymalizacji przebiegu między obsługami okresowymi elementów obiektu przedstawiono już w pracy [5]. Niech zatem *z* będzie funkcją łącznych jednostkowych kosztów związanych z obsługą *n* elementów obiektu technicznego, opisaną następującą zależnością:

$$z(l_1, l_2, ..., l_N) = \sum_{i=1}^{n} \frac{C_i}{l_i}, \quad i = 1,2,...,n, \tag{7}$$

gdzie:

C_i – koszt obsługi *i*-tego elementu,

l_i – liczba jednostek pracy (*jp*) między obsługami *i*-tego elementu.

Liczba jednostek pracy do obsługi *i*-tego elementu powinna być tak ustalona, aby ryzyko związane z uszkodzeniem tego elementu po przepracowaniu l_i jednostek pracy, nie przekroczyło dopuszczalnej wartości tzn.:

$$r_{ijk}^{+NWZ,1}(l_i) \le r^{A}, \quad i = 1,2,...n. \tag{8}$$

Jeżeli przyjąć ponadto, że prawdopodobieństwo q_i uszkodzenia *i*-tego elementu dane jest pewną funkcją φ jego przebiegu w kilometrach, tj.:

$$q_i = \varphi(l_i) \tag{9}$$

to zgodnie z wymaganiami dotyczącymi warstwy zabezpieczeń zapisanymi w postaci zależności (5) można wyznaczyć graniczną wartość L_i liczby jednostek pracy elementu, po której należy przeprowadzić określony typ jego obsługi:

$$L_i = \varphi^{-1}(q_i) \tag{10}$$

Planowana liczba *jp* do obsługi *i*-tego elementu będzie zawierała się w granicach:

$$0 < l_i \le L_i \tag{11}$$

Zwiększenie efektywności pracy opisywanego tu systemu polega na wyznaczeniu takiej wartości l^* tj. optymalnej liczby *jp* między obsługami poszczególnych elementów *ops*, aby spełniona była zależność (8). Jako funkcję celu można potraktować zależność (7).

Konfiguracja warstwy zabezpieczeń zorganizowanej w postaci systemu obsług powinna uwzględniać różne kryteria klasyfikacji obsługi przypisanych *ops*. Przykłady takich kryteriów można znaleźć np. w pracy [19]. Niektóre z systemów eksploatacji obiektów technicznych np. systemy eksploatacji pojazdów szynowych są oparte na planowo-zapobiegawczej strategii obsługiwania [8, 25]. Istotą tak zorganizowanego systemu obsługiwania jest występowanie krotności między liczbą *jp* do obsługi poszczególnych elementów *ops*.

7. Uwagi końcowe

Przedstawiono koncepcję wykorzystania elementów procedur zarządzania ryzykiem w organizacji

systemów i procesów obsługiwania obiektów systemów transportowych. Koncepcja opiera się na założeniu, że system obsług profilaktycznych obiektów może być jedną z niezależnych warstw jego zabezpieczeń. W takim przypadku aby właściwie skonfigurować systemy i procesy obsługiwania można wykorzystać m.in. analizę warstw zabezpieczeń (AWZ). Przedstawiona koncepcja powinna zapewnić możliwość dostosowania parametrów procedur obsługiwania obiektów do występujących zagrożeń w trakcie ich eksploatacji, a w efekcie ograniczyć ryzyka związane z tymi zagrożeniami.

Potraktowanie systemu obsługiwania obiektów jako warstwy zabezpieczeń jest oryginalnym założeniem przedstawionej metody. Aktualnie brak jest rozwiązań aplikacyjnych opartych na zaprezentowanej tu koncepcji organizacji systemów i procesów obsługiwania obiektów. Jej autorzy są przekonani, że są one możliwe. To przekonanie i już osiągnięte wyniki, są podstawą dalszych prac w tej dziedzinie.

Literatura

[1] *Beckman L.: Determining the required safety integrity level for your process. ISA Transaction 37, 1998.*

[2] *Dowell A.M.: Layer of protection analysis for determining safety integrity level. ISA Transactions 37, 1998.*

[3] *Fujiyamaa K., Nagaia S., Akikunib Y., Fujiwarab T., Furuyab K., Matsumotob S., Takagib K., Kawabatac T.: Risk-based inspection and maintenance systems for steam turbines. International Journal of Pressure Vessels and Piping, 2004, nr 81.*

[4] *Fórmaniak A.: Zagadnienia integracji gotowości i bezpieczeństwa systemów infrastruktury kolejowej na etapie projektowania. Pojazdy Szynowe, nr 2 2004.*

[5] *Gill A.: Metoda wyznaczania struktury cyklu napraw elementów pojazdów szynowych. Pojazdy Szynowe, nr 3-4/ 2004.*

[6] *Głodek W.: Ryzyko awarii przemysłowych. Jak rozpoznawać i oceniać ryzyko? BMP Chemia Przemysłowa, 2002, nr 4. Strona internetowa: www.sipi61508.com.*

[7] *Głodek W.: Automatyka zabezpieczeniowa w przemyśle procesowym – przegląd unormowań. Warsztaty SIPI61508, Gdynia, maj 28÷29, 2003. Strona internetowa: www.sipi61508.com, 2005.*

[8] *Kadziński A.: O modelach i badaniach symulacyjnych systemów kolejowych pojazdów szynowych w aspekcie ich niezawodności. W: Materiały XXX Zimowej Szkoły Niezawodności nt. Niezawodność systemów, Szczyrk, 2002.*

[9] *Khan F.I., Haddara M. R., Risk-based maintenance of ethylene oxide production facilities. Journal of Hazardous Materials A108, 2004.*

[10] *Knegtering B., Brombacher A.C.: Application of micro Markov models for quantitative safety assessment to determine safety integrity levels as defined by the IEC 61508 standard for functional safety. Reliability Engineering and System Safety, nr 66, 1999.*

[11] *Kosmowski K.T.: Aktualne problemy analizy ryzyka i zarządzania bezpieczeństwem w systemach technicznych. W: Materiały konferencji „Analiza ryzyka i zarządzanie bezpieczeństwem w systemach technicznych", Gdańsk-Gdynia, 25-27 czerwca, 2001.*

[12] *Markowski A.S., Borysiewicz M.: Zastosowanie analizy warstwy zabezpieczeń do oceny ryzyka dla rurociągów. Strona internetowa: http://manhaz.cyf.gov.pl / manhaz, 2005.*

[13] *Markowski A. S.: Zapobieganie stratom w przemyśle. Cz. 3, Zarządzanie bezpieczeństwem i higieną pracy, Wyd. Politechniki Łódzkiej, Łódź 2000.*

[14] *Marszal E.M.: Tolerable risk guidelines. ISA Transaction, nr 40, 2001.*

[15] *Norma PN-EN 1050:1999. Maszyny. Bezpieczeństwo. Zasady oceny ryzyka..*

[16] *Młyńczak M.: Analiza ryzyka w transporcie i przemyśle. Seria NAVIGATOR, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 1997.*

[17] *Moczarski M.: Nowe tendencje w obsługiwaniu obiektów technicznych. Zeszyty Naukowe Politechniki Poznańskiej, seria MRiP, nr 41, 1994.*

[18] *Nilsson F., Risk based approach to plant life management. Nuclear Engineering and Design, nr 221, 2003.*

[19] *Niziński S.: Eksploatacja obiektów technicznych. Wydawnictwo i Zakład Poligrafii Instytutu Technologii Eksploatacji, Radom, 2002.*

[20] *Pietrzyk A., Uhl T.: Wykorzystanie analizy ryzyka w procesie planowania zadań serwisowych. Problemy Eksploatacji, 2005, nr 3.*

[21] *Summers A.E.: Techniques for assigning a target safety integrity level. ISA Transactions 37, 1998.*

[22] *Stavrianidis P.: Bhimavarapu K., Safety instrumented functions and safety integrity levels (SIL). ISA Transaction, nr 37, 1998.*

[23] *Straub D., Faber M.H., Risk based inspection planning for structural systems. Structural Safety, nr 27, 2005.*

[24] *Szopa T.: Niezawodność i bezpieczeństwo. W: Podstawy Konstrukcji Maszyn, t. 1, WNT, Warszawa 1999.*

[25] *Tomaszewski F.: Zagadnienia wyznaczania stanu technicznego złożonego obiektu mechanicznego za pomocą sygnału wibroakustycznego na przykładzie silnika spalinowego pojazdu szynowego. Wydawnictwa Politechniki Poznańskiej, Seria Rozprawy, Poznań, 1998.*