dr inż. Andrzej Förmaniak
Ove Arup – Wielka Brytania

Zagadnienia integracji gotowości i bezpieczeństwa systemów infrastruktury kolejowej na etapie projektowania

Publikacja niniejsza ma przybliżyć czytelnikom zagadnienia uwzględniania w procesie projektowania systemu transportowego parametrów bezpieczeństwa przewozów pasażerów przy równoczesnym spełnianiu wymagań w zakresie gotowości systemu. Oparta jest na doświadczeniach autora, nabytych w pracy nad realizacją projektu linii kolejowej na duże prędkości w Wielkiej Brytanii.

1. Wstęp

W praktyce projektowania dużych i skomplikowanych systemów technicznych takich jaką jest nowa linia kolejowa aspekt osiągnięcia gotowości przewozowej jest tak samo ważny jak zapewnienie odpowiedniego poziomu bezpieczeństwa. Często jednak zdarza się tak, że specjaliści od oceny bezpieczeństwa przewozów pracują w większej lub mniejszej izolacji od zespołów projektujących poszczególne systemy zapewniające operacyjne działanie systemu. Różne są tego przyczyny. Najczęściej wynikają one ze słabości organizacyjnej projektu, braku dobrze zdefiniowanych kryteriów, ale również mają podłoże komercjalne. To ostatnie wynika w dużej mierze z dużej separacji podmiotów realizujących zadania projektowe i tych samych zespołów konkurujących ze sobą w innych projektach.

Konsekwencją tego są takie sytuacje, kiedy niespełnianie wymagań bezpieczeństwa zmusza przyszłego operatora systemu do występowania do władz wydających certifikat bezpieczeństwa o tymczasowe zezwolenie na operowanie systemu do czasu usunięcia istotnych niedociągnięć. Częstym powodem powstania takiej sytuacji jest nie w pełni udokumentowane osiągnięcie wymaganego poziom bezpieczeństwa, jak również może być spowodowane brakiem spójności pomiędzy dokumentacją satysfakcjonującą wymagania techniczne, a tą związaną z zapewnieniem bezpieczeństwa.

Ważnym więc wydaje się zadbanie o to na bardzo wstępnym etapie projektu, aby taka sytuacja nie wystąpiła, oraz aby kooperacja pomiędzy zespołami projektującymi była niejako wymuszona systemowo od pierwszego etapu realizacji projektu. Artykuł niniejszy omawia zagadnienie integracji wymagań odnośnie do zapewnienia gotowości systemu z wymaganym poziomem bezpieczeństwa.

2. Kryteria operacyjne i bezpieczeństwa i ich konwersje na wymagania techniczne

Nie jest niczym nadzwyczajnym, że na liście wymagań odnośnie do gotowości projektowanej infrastruktury pojawiają się takie żądania jak wymienione poniżej, dla nowo-projektowanej szybkiej linii kolejowej [1]:

- nie więcej niż dwa pociągi dziennie mogą mieć spóźnienie przekraczające 10 minut,
- nie więcej niż dwa pociągi na miesiąc mogą mieć spóźnienie w granicach między 10 i 30 minut,
- nie więcej niż dwa pociągi na kwartał mogą mieć spóźnienie w granicach między 30 i 60 minut,
- nie więcej niż dwa pociągi na rok mogą mieć spóźnienie powyżej 60 minut, bądź być odwołane.

Coraz częściej strona inwestująca w projekt techniczny stawia wymagania dla projektowanego systemu w taki sposób, że przetworzenie ich na wymagania techniczne wymaga od projektanta pewnego dodatkowego wysiłku. Oczywistym na pierwszy rzut oka jest ich pochodzenie i bezpośrednie połączenie z ogólnym planem ekonomicznym projektu jako elementu większego systemu, w tym przypadku transportu kolejowego. Problem jaki pojawia się dla projektantów polega na konwersji tych komercjalnych wymagań na techniczne w odniesieniu do każdego ze systemów składowych. Rozdział wymagań gotowościowych na poszczególne systemy jest dodatkową trudnością.

Trochę inaczej wygląda ustanawianie wymagań w przypadku bezpieczeństwa przewozów, ponieważ są one wyłącznie w gestii kotrolera całego systemu kolejowego. Plan osiągnięcia pewnego poziomu bezpieczeństwa projektowanego systemu jest bowiem osadzony w bardziej ogólnym, np. Rocznym Planie Bezpieczeństwa Przewozów dla całego systemy transportu kolejowego. Ten ostatni jest ustalany przez władze kontrolujące działanie kolei, a nie na poziomie inwestora nowej linii kolejowej.

Z tego planu wynikają minimalne wymagania, których osiągniecie jest podstawą uzyskania **Certyfikatu Bezpieczeństwa** niezbędnego dla uzyskania pozwolenia na operowanie systemu. Zazwyczaj oczekuje się, że w odniesieniu do parametrów bezpieczeństwa nowe instalacje osiągną lepsze rezulataty niż te, które są już w trakcie ekasploatacji.

Parametry bezpieczeństwa, które podlegaja kontroli to zazwyczaj:

- indywidualne ryzyko utraty życia lub zdrowia przez pasażera,
- indywidualne ryzyko utraty życia lub zdrowia przez pracownika kolei,
- częstotliwość katastrof kolejowych prowadzących do większej ilości ofiar, np. >10, >100, itd., te ostatnie ilustrowane są na rys. 1.

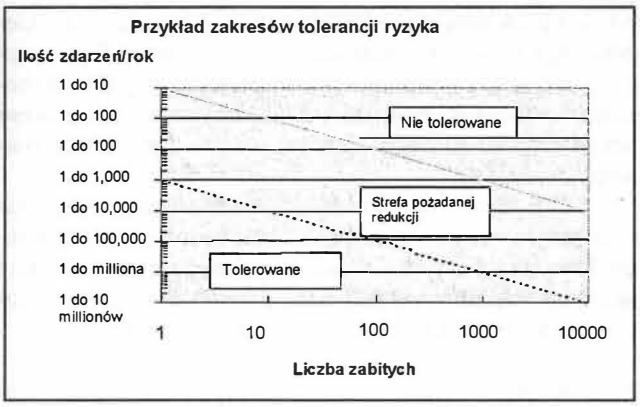
W tabelach 1 i 2 przedstawiono kryteria dopuszczalnego ryzyka indywidualnego oraz społecznego, które przyjęto dla projektu szybkiej kolei w Zjednoczonym Królestwie [2].

Kryteria dopuszczalnego ryzyka indywidualnego **Tabela 1**

Ryzyko utraty życia w skali rocznej	Grupa użytkowników
1 do 100,000	Pasażerowie
1 do 10,000	Pracownicy kolei
1 do 1,000,000	Ludność zamieszkująca w pobliżu linii kolejowej

Kryteria dopuszczalnego ryzyka społecznego **Tabela 2**

Częstotliwośc zdarzeń w skali rocznej	Konsekwencje: Ryzyko utraty życia
1 do 10,000	10 przypadków
1 do 100,000	100 przypadków



Rys. 1 Przykład zakresów tolerancji ryzyka liczby zabitych w katastrofach kolejowych

Oczywiście niezbędne jest wiarygodne zapewnienie spełnienia wymagań zarówno gotowościowych jak i bezpieczeństwa na etapie projektowania.

3. Unia Europejska a spolegliwość kolei

W niektórych państwach zagadnienia bezpieczeństwa przewozów kolejowych są bardziej regulowane niż w innych. Legislacja istniejąca w tej dziedzinie w poszczególnych państwach wydaje się być miarą odpowiedzialności jaką gotowe są one przyjąć na siebie dla zapewnienia bezpiecznego i niezawodnego transportu kolejowego.

Zagadnienia te coraz bardziej stają się aktualne w całej Unii Europejskiej (UE) i pojawiające zarówno dyrektywy jak i ich propozycje są dowodem usiłowań zharmonizowania wymagań bezpieczeństwa przewozów we wszystkich krajach należących do UE [3, 4, 5].

Jak najszybsza implementacja wspomnianych wyżej pakietów dyrektyw Europejskiej Komisji - EC (European Commission) w krajach członkowskich oraz propozycji utworzenia adekwatnych urzędów stanowi aktualnie główną oś strategii działań mających na celu zapewnienie sprawnie działającej i bezpiecznej europejskiej sieci kolejowej – TEN (Trans-European Network).

Spory wysiłek w związku z tym wymagany jest od wielu krajów, a w szczególności od tych które ostatnio przyłączyły sie do UE, i których legislacja w zakresie bezpieczeństwa przewozów powinna być zharmonizowana. EC (European Commission) już uruchomiła fundusze związane z tym procesem.

4. Techniczne aspekty spolegliwości

Wprawdzie **spolegliwość** jest czasami utożsamiana z niezawodnością ale wydaje się, że jest to termin szerszy i w artykule używany będzie dla określenia tego samego co Anglicy nazywają "dependability". W języku angielskim dependability obejmuje RAMS (Reliability, Availability, Maintainability & Safety), a więc niezawodność, gotowość, utrzymanie i bezpieczeństwo. Zagadnienia te dobrze opisane są w normie europejskiej na temat definiowania i zapewnienia parametrów RAMS w projektach kolejowych [6].

Wskaźnik poziomu zintegrowanego bezpieczeństwa, tzw. SIL (Safety Integrity Level) jest aktualnie lansowanym w projektach kolejowych parametrem, który został wprowadzony do praktyki projektowania dla ułatwienia dialogu pomiędzy wieloma stronami związanymi z realizacją bezpiecznych systemów technicznych. EU wprowadziła cztery poziomy SIL. Im wyższy SIL tym wyższe są wymagania dotyczące niezawodności działania stawiane systemom. Zapewnienie osiągnięcia właściwego poziomu SIL może być przeprowadzone na drodze jakościowej lub ilościowej. Wybór sposobu zależy od systemu i możliwości jego oceny na określonym etapie projektu. Szczegóły na ten temat można znaleźć w normie IEC 61508 związanej z bezpieczeństwem funkcjonalnym elektrycznych, elektronicznych i programowalnych elektronicznych systemów zapewniających bezpieczeństwo [7, 8].

Wyższe poziomy SIL, tzn. 3 i 4 mają zastosowanie do systemów, które mają krytyczne znaczenie dla zapewnienia bezpieczeństwa, jak np. sygnalizacja kolejowa. Poziomy 1 i 2 odnoszą się do systemów wpływających na bezpieczeństwo, ale nie są one krytyczne, np. komunikacja telefoniczna lub radiowa pomiędzy pociągiem a centrum kontroli ruchu.

Jak z powyższego wynika, spory wysiłek został podjęty, aby zapewnić spolegliwość systemów , które mają wpływ na bezpieczeństwo przewozów. Jest jednak wiele systemów, których znaczenie funkcjonalne nie jest związane z bezpieczeństwem, albo związki te nie są bezpośrednie. Przykładem może być system zasilania energią dla celów trakcyjnych, albo infrastruktura stacji kolejowej. Tam metodyka SIL nie ma bezpośredniego zastosowania. Tym niemniej w jednym i w drugim przypadku następuje obniżenie gotowości całego systemu, kiedy ich urządzenia zaczynają się uszkadzać.

5. Modele

Ocena jakości działania systemów na etapie projektowania nieodłącznie związana jest z modelowaniem. Idealnie byłoby zbudować taki model, który pozwalałby ocenić/analizować parametry RAMS dla wszystkich systemów, a nie tylko tych związanych z bezpieczeństwem. Wymagane przy tym byłoby, aby model taki ze względów praktycznych zrealizowany był na poziomie wymiennych zespołów, z angielskiego LRU (Line Replaceable Unit).

Oczywistym jest, że taki całościowy model dając możliwość natchmiastowej oceny całego systemu wymaga więcej wysiłku podczas budowy oraz bardziej efektywnych metod analizy ze względu na swoją wielkość. Im więcej parametrów do oceny tym dłuższe czasy obliczeniowe Okazuje się, że trudno znaleźć w dostępnej publicznie literaturze przypadki realizacji takich dużych modeli. Czy jednak takie duże modele są rzeczywiście potrzebne? Wydaje się, że jedynie wtedy są one uzasadnione, kiedy istnieje potrzeba odpowiedzi na bardzo globalnie zdefinowane kryteria.

W transporcie kolejowym, ze względów praktycznych, te duże modele ograniczają się więc jedynie do oceny gotowości systemu. W zrealizowanym już w 2003 roku pierwszym etapie projektu CTRL [1] zastosowano do tego celu oprogramowanie Witness. W rezultacie przeprowadzonych symulacji ruchu przy zdefiniowanych parametrach

niezawodności poszczególnych LRU oraz strategii ich utrzymania można było udzielić odpowiedzi na pytanie: czy kryteria gotowości systemu kolejowego zostały spełnione.

W odniesieniu do projektu CTRL zbudowano oddzielny model bezpieczeństwa – TARM (Train Accident Risk Model). Model Ryzyka Wypadków Kolejowych, który dotyczy jedynie wypadków kolejowych związanych z udziałem pociągu. TARM umożliwia ocenę ryzyka utraty życia przez różne grupy użytkowników CTRL wynikającego z wykolejeń, zderzeń i pożarów pociągów. Dla tych trzech typów wypadków kolejowych zbudowano odpowiednie modele lokalne, dzięki którym powstała możliwość oceny ryzyka w różnych miejsca zaistnienia wypadku, jak np. tunel, wiadukt, nasyp, równoległa inna linia kolejowa, itd.

Modele zbudowane są w oparciu o dwie techniki, tj. drzewo uszkodzeń i drzewo zdarzeń. Drzewo uszkodzeń umożliwia ocenę częstotliwości wypadków, a drzewo zdarzeń ocenę możliwych konsekwecji. To ostatnie to nic innego jak definiowanie różnych scenariuszy, w których konsekwecje są bądź mniejsze bądź poważniejsze w zależności od tego, czy następuje eskalacja niekorzystnych okoliczności, bądź są skutkiem nie działających z odpowiednią niezawodnością urządzeń. Jeśli np. w przypadku wykolejenia konstrukcja ograniczająca ruch wagonów w obrębie toru nie wytrzyma sił wywieranych na nią przez wykolejony pociąg, to liczyć się należy ze znacznie poważniejszymi konsekwencjami niż w przypadku, gdy pociąg zostanie utrzymany w tzw. skrajni budowlanej. W drzewie uszkodzeń wszystkie elementy infrastruktury, których niewłaściwe działanie może się przyczynić do zaistnienia wykolejenia, brane są pod uwagę, np. pęknięcia szyn, uszkodzenia zwrotnic, rozjazdów, itp.

W sumie w TARM około 3500 scenariuszy opisuje możliwe różne konsekwencje, dla których ryzyko jest określane w kategoriach indywidualnego pasażera korzystającego regularnie bądź sporadycznie z CTRL. Podobną ocenę dokonuje się również w stosunku do obsługi pociągu. Wszystkie te wskaźniki są porównywalne z kryteriami bezpieczeństwa, które zostały przyjęte dla tej linii kolejowej. Istnienie tego modelu na wczesnym etapie projektu dało możliwość identyfikacji przekroczeń i podjęcia właściwych działań korekcyjnych. Te działania były podejmowane zarówno po stronie modyfikacji systemów jak i przez zastosowanie odpowiednich procedur operacyjnych, i prowadzone były tak długo, jak było to niezbędne dla uzyskania satysfakcjonujących wskaźników.

Ważnym jest to, aby zarówno model gotowościowy i bezpieczeństwa używały tych samych danych, co w sytuacji rozdziału modeli wprowadza pewien problem.

Trzeba pamiętać o tym, że oprócz ofiar katastrof kolejowych istnieje mniej spektakularna wypadkowość związana ze statyczną infrastrukturą kolejową. Do tej grupy zalicza się wszelkie wypadki w obrębie dworca kolejowego, na peronach, schodach (w tym ruchomych), windach, itp. Dla pełni obrazu wymienić należy wszystkie usiłowania samobójstwa oraz\wszelkie wypadki w pociągu, chociaż nie związane z jego przemieszczaniem się. Przewidywania w tym zakresie dla CTRL realizowane były osobno.

6. Wnioski

Niezawodność działania systemów krytycznych dla zapewnienia płynności ruchu oraz gotowość systemów bezpieczeństwa dla podjęcia działań zapobiegawczych wystąpienia wypadku oraz ograniczających jego skutki w sytuacji wypadku stoją u podstaw działania systemów transportu kolejowego.

Specyfikacja wymagań dla dostawców poszczególnych systemów, które związane są z bezpieczeństwem w sytuacji kiedy istnieją wskaźniki SIL jest łatwiejsza niż kiedykolwiek przed ich ustanowieniem. Metodyka SIL definiuje wymagania i zmusza zarówno projektanta jaki i wykonawcę systemu do podjęcia trudu, który na końcu procesu pozwala liczyć na osiągnięcie projektowanego poziom bezpieczeństwa.

Budowa odpowiednich modeli gotowościowych oraz bezpieczeństwa połączona z ich koordynacją w zakresie korzystania z tych samych baz danych zapewnić może projektantom infrastruktury narzędzia dla wiarygodnej kontroli tego, czy projekt może spełnić wymagane kryteria.

Literatura

[1] *Fórmaniak A., Jak zapewnić bezpieczeństwo przewozów w procesie projektowania linii kolejowej na duże szybkości? Przegląd Techniczny Nr. 4, 2004.*

[2] *Fórmaniak A., Managing Risk in the Design of the Channel Tunnel Rail Link, UK London, Prepared for PSAM5 Conference in Japan, December 2000 (co-authors: Ken Harvey, Charles Milloy and Paul Scott)*

[3] *The European Commission: Railway infrastructure package, 1998; dostępny przez http://europa.eu.int/comm/transport/ rail/index_en.html*

[4] *The European Commission: 2nd Railway infrastructure package, 2001; dostępny przez http:// europa.eu.int/comm/tranport/rail/index_en.html*

[5] *The European Commission: 3rd Railway infrastructure package, 2004; dostępny przez http:// europa.eu.int/comm/ transport/rail/index_en.html*

[6] *EN 50126: Railways Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS); CENELEC standard 1999.*

[7] *IEC 61508: Functional safety of electrical /electronic/ programmable electronic safety-related systems. IEC Standard (International Electrotechnical Commission).*

[8] *Functional Safety and IEC 61508 – Basic Guide, May 2004, dostępny przez http://www.iec.ch/zone/ fsafety/pdf_safe/ hld.pdf*