Bezpieczeństwo systemów srk a nowe technologie informacyjne

Security of Railway Control Systems and new information technologies

Andrzej Lewiński

Prof. dr hab. inż.

Wydział Transportu i Elektrotechniki
Uniwersytetu Technologiczno-
Humanistycznego w Radomiu

a.lewinski@uthrad.pl

Streszczenie: Nowe technologie informacyjne, czyli techniki komputerowe, bezprzewodowe (otwarte) standardy transmisji oraz systemy satelitarne wykorzystywane do pozycjonowania miały istotny wpływ na inne podejście do kryterium bezpieczeństwa systemów sterowania ruchem kolejowym. Przyjęta dla systemów przekaźnikowych zasada „fail-safe" opierała się na bardzo dużej niezawodności przekaźników (gwarantowana liczba zadziałań) oraz rygorystycznej procedurze utrzymania (legalizacji). Implementacja nadmiarowych, redundantnych systemów komputerowych zmodyfikowała pojęcie bezpieczeństwa w kierunku tolerowalnego poziomu ryzyka (THR), gdzie bezpieczeństwo komputerowych systemów wyrażono w formie intensywności zdarzeń krytycznych uwzględniających testowanie. Technologie bezprzewodowe uwzględniły z kolei zagrożenia i ich wpływ na funkcjonalność, dostępność i niezawodność systemów srk.

Słowa kluczowe: *Systemy Sterowania Ruchem Kolejowym; Fail-Safe; Tolerowalny poziom ryzyka; Prawdopodobieństwo wystąpienia uszkodzenia krytycznego*

Abstract: The new information technologies, such computer techniques, wireless (open) transmission standards and satellite systems applied for positioning have a important influence for different approach to safety criteria of railway control systems. The "fail-safe" rule assumed for relay control systems is based on high reliability of applied relays (guaranteed number of switches) and rigorous maintenance (homologation) procedure. The implementation of redundant, parallel computer systems has modified the concept of safety towards Tolerable Hazard Rate, where safety of computer systems is defined as an intensity of critical (dangerous, catastrophic) failures including self-testing. The wireless technologies respect the threats and their influence for functionality, availability and reliability of railway control systems (defined as probability).

Keywords: *Railway Control Systems; Fail-Safe; Tolerable hazard rate; Probability of critical failure*

Od początku kolejnictwa pojawił się problem zapewnienia bezpieczeństwa ruchu pociągów. Bezpieczeństwo było zależne od człowieka – dyżurnego ruchu i podległych mu służb związanych z zapewnieniem prawidłowego przejazdu pociągu na szlaku oraz w obrębie stacji kolejowych [25]. Czynności te wykonywali odpowiedzialni, przeszkoleni zdyscyplinowani pracownicy, dla których praca była „służbą". Pierwsze urządzenia zależnościowe (kluczowe) i wprowadzenie łączności telefonicznej uzależniało bezpieczeństwo ruchu pociągów od człowieka: dyżurnego ruchu, nastawniczego praz osób odpowiedzialnych za utrzymanie infrastruktury, Pomimo rygorystycznie przestrzeganych procedur dochodziło do poważnych wypadków, w przeważającej części spowodowanej przez błąd człowieka, rzadziej przez niezawodność urządzeń zabezpieczenia ruchu.

Wprowadzenie urządzeń elektrycznych: najpierw przekaźnikowych, potem komputerowych, a następnie przyszłościowych z otwartą transmisją radiową wprowadziło stopniową eliminację wpływu człowieka na bezpieczeństwo systemów zarządzania i sterowania ruchem kolejowym. Proces kontroli najpierw objął dyżurnego ruchu eliminując możliwość błędnego ustawienia przebiegu, ale w następnym kroku uwzględnił również poprawność zachowania maszynisty – jego reakcję na sygnalizację przytorową. We współczesnych systemach zarządzania i sterowania ruchem kolejowym, związanych z Kolejami Dużych Prędkości takich jak system ERTMS/ETCS kontrolowane są również parametry pociągu w kontekście bezpiecznego przemieszczania na tzw., „widzialność elektryczną", gdzie są zapewnione odległości między pociągami i bezpieczna droga hamowania.

Artykuł przedstawia ewolucję kryteriów bezpieczeństwa na przestrzeni wielu lat, odpowiadających zarówno normom UE jak też metodom naukowym wynikających bezpośrednio z tych zaleceń. Autor chciałby w tym miejscu podziękować dr inż. Andrzejowi Toruniowi z Instytutu Kolejnictwa w Warszawie oraz dr hab. inż. Tomaszowi Perzyńskiemu, profesorowi nadzwyczajnymi na Wydziale Transportu i Elektrotechniki Uniwersytetu Techno-

logiczno – Humanistycznego w Radomiu za udostępnienie wyników wielu prac naukowo – badawczych wspólnie prowadzonych w tym zakresie

Bezpieczeństwo systemów przekaźnikowych

Znaczącym krokiem w rozwoju urządzeń zabezpieczenia ruchu pociągów było zastosowanie w latach 40 ubiegłego wieku urządzeń elektrycznych (przekaźnikowych). Ten fragment odnosi się do opracowania [4], ale zasady projektowania, eksploatacji i utrzymania systemów przekaźnikowych można znaleźć [[1] i [6].

Przekaźnikowe systemy srk projektowane były jako systemy bezpieczne oparte na regule *fail-safe* – żadne pojedyncze uszkodzenie nie może prowadzi do błędnego wysterowania urządzeń zewnętrznych (sygnalizatora, zwrotnicy). Oznacza to, iż w przypadku przekaźnikowych urządzeń srk pojedyncze uszkodzenie musi wymuszać zmianę stanu systemu na taki, który zdefiniowany jest jako stan bezpieczny (np. uniemożliwienie wyświetlenia sygnału zezwalającego, wykluczenie możliwości nastawienia przebiegu, przestawienia zwrotnicy, ….). Osiągnięcie stanu bezpiecznego powoduje określone ograniczenia w dostępności systemu do sterowania lecz nie powoduje sytuacji zagrożenia w ruchu kolejowym. Podstawowo bezpieczeństwo obwodów elektrycznych osiągane było przez:

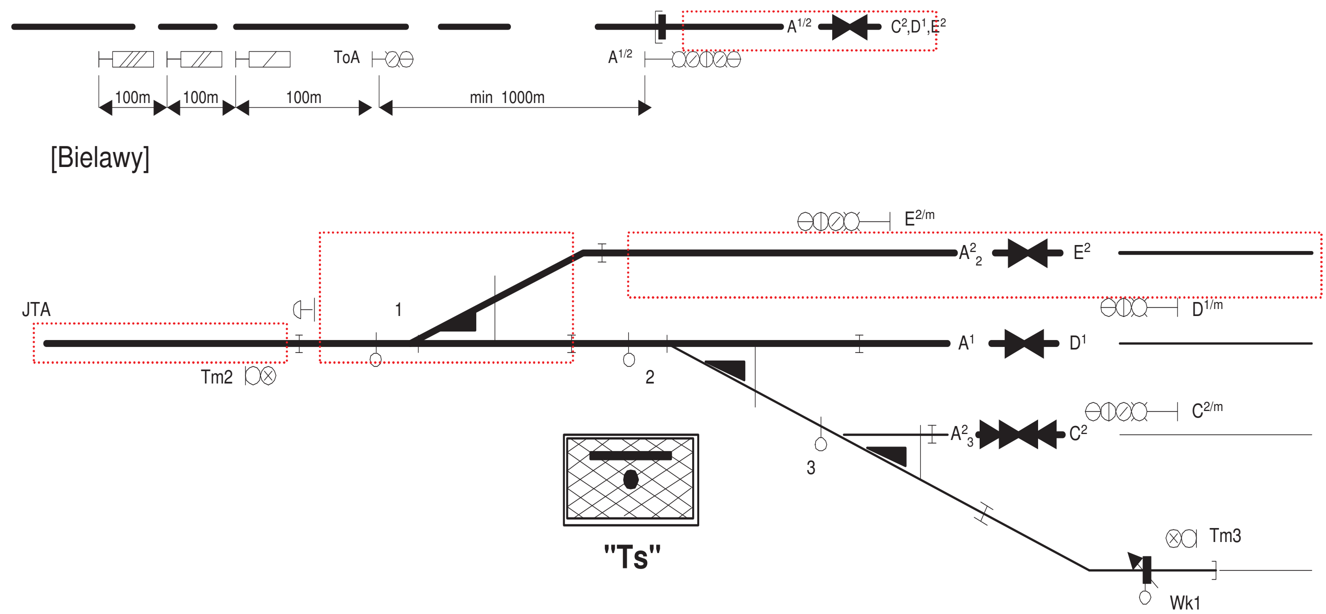
a) zastosowanie odpowiednich elementów konstrukcyjnych obwodów tj. przekaźniki zabezpieczeniowe określonej klasy, transformatory, przekładniki prądowe, dławiki, bezpieczniki,
b) odpowiednie ukształtowanie obwodu elektrycznego, zgodnie z opracowanymi przez uprawnione jednostki kolejowe albumy typowych układów dla poszczególnych systemów zabezpieczenia ruchu kolejowego.

Ze względu na sposób projektowania i montażu urządzenia przekaźnikowe urządzenia sterowania ruchem kolejowym sklasyfikowane zostały na dwie podstawowe grupy:

a) urządzenia projektowane indywidualnie (np. stacyjne typu E), dla których wykorzystywane były zasady projektowania oparte o albumy schematów typowych a zasady bezpiecznego prowadzenia ruchu zdefiniowane były w zależności od układu torowego i charakterystyki ruchowej obiektu (stacji) w postaci tablicy zależności lub kart przebiegów,
b) urządzenia geograficzne - zblokowane (budowane w strukturze modułowej tj. IZH 111, CBP83, SUP-3, SUP-3M) definiowane jako graf powiązania typowych modułów funkcjonalnych.

Zasada: *fail-safe* jako nadrzędne wymaganie bezpieczeństwa sprowadzała się do wykrycia usterki krytycznej i bezpiecznej reakcji systemu na wykrytą usterkę. W praktyce zdefiniowane zostały zarówno zasady bezpiecznego projektowania jak i sklasyfikowane zostały usterki w zależności od ich wpływu na bezpieczeństwo działania systemów:

a) usterki niekrytyczne (bezpieczne), które powodują ograniczenie funkcjonalności systemu, powodując zakłócenia w ruchu pocią-



Lp	Przebieg	Opis przebiegu	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
			Przebiegi pociągowe														
			A^2_3	A^1_1	A^2_2		C	D	E		S^2_3	S^2_1	S^1_2		M^2_1	L^1_1	K^2_1
1	A^2_3	Ze st. Bielawy na tor 3	–	+	+		+	+	+		+						
2	A^1_1	Ze st. Bielawy na tor 1	+	–	+		+	+	+			+					
3	A^2_2	Ze st. Bielawy na tor 2	+	+	–		+	+	+				+				

Lp	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
	Przebiegi manewrowe																		
		Tm 3	C^m	D^m	E^m		Tm2 5	Tm2 3	Tm2 1	Tm2 2		Tm 11	M^m	L^m	K^m	Tm13 5	Tm13 3	Tm13 1	Tm13 2
1		+	+	+	+		+	+	+	+			+				+		
2		+	+	+	+		+	+	+	+				+				+	
3		+	+	+	+		+	+	+	+					+				+

Lp	1	2	3	4	5	6	7	8	9	Odcinki izolowane	
	Zwrotnice i wykolejnice										
		1	2	3/Wk1	10/Wk6	11	12/13	14/15		Torowe	Zwrotnicowe
1		+	–	+						A,3	1,2,3/Wk1
2		+	+	+o	+o					A,1	1,2
3		–								A,2	1

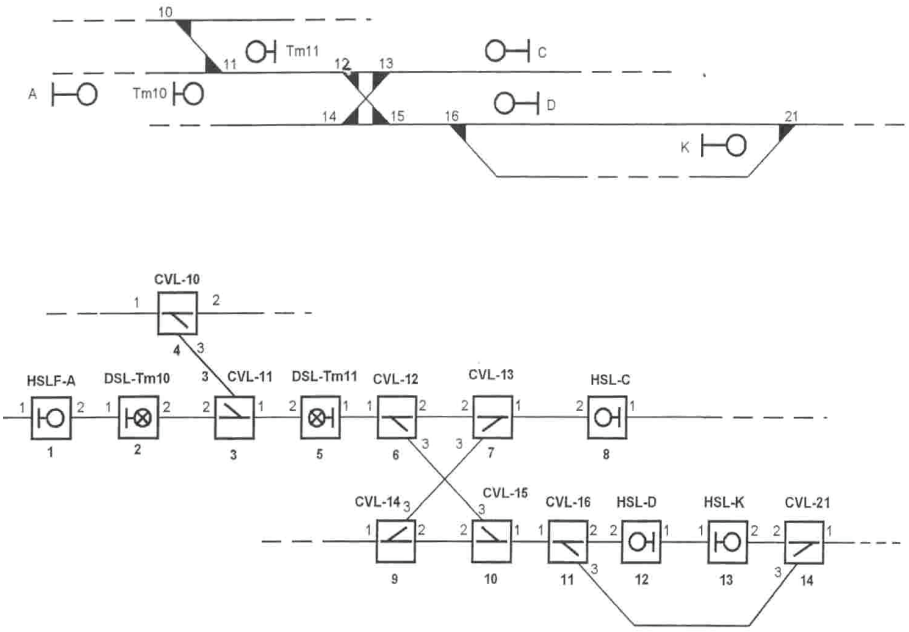
1. Przykładowy układ torowy stacji wraz z tablicą zależności

gów ale bez możliwości spowodowania kolizji pociągów,

b) usterki krytyczne – (niebezpieczne), które wprowadzają bezpośrednie zagrożenie bezpieczeństwa i mogą prowadzić do powstania sytuacji niebezpiecznej – kolizji.

W praktyce realizacja zasady „*fail – safe*" opiera się na stosowaniu odpowiednich elementów – przekaźników klasy I (N), gdzie wykorzystuje się ich właściwości asymetryczności uszkodzeń polegającą na przyjęciu założenia że bardziej prawdopodobne przyjmuje się zdarzenie niewzbudzenia się przekaźnika (przy zamknięciu obwodu wzbudzenia) na skutek np. przerwy w obwodzie cewki przekaźnika, oraz jako nieprawdopodobne ze względów konstrukcyjnych wystąpienie przypadku pozostania przekaźnika w stanie wzbudzonym po zaniku zasilania uzwojenia cewki tego przekaźnika. A w przypadku przekaźników klasy II (C), jako prawdopodobne przyjmuje się wystąpienie obu wyżej opisanych zjawisk (uszkodzeń np. pozostanie w stanie wzbudzonym na skutek sklejenia styków).

Na rys. **1** przedstawiono fragment przykładowego układu torowego stacji wraz z przykładowymi zapisami zależności zamieszczonymi w Tablicy Zależności. System ten (E} [15], charakteryzuje się dość ograniczonym, ale wystarczającym do prowadzenia ruchu na stacji, zestawem realizowanych funkcji i podstawowo zapewnia możliwość indywidualnego sterowania poszczególnymi obiektami tj. zwrotnica, wykolejnica, sygnalizator. Oznacza to w praktyce indywidualne wybieranie i nastawianie dróg przebiegów, przy jednoczesnej kontroli elementów tych dróg przebiegów (niezajętości odcinków izolowanych torów i zwrotnic, położenia zwrotnic i wykolejnic, stany sygnalizatorów, ….). Dla zapewnienia bezpieczeństwa prowadzenia ruchu na posterunku dodatkowo oprócz kontroli stanu elementów dróg przebiegów, system na podstawie indywidualnie projektowanej dla każdego posterunku tablicy zależności wyklucza przebiegi sprzeczne oraz kontroluje warunki bezpiecznego nastawiania i zwalniania dróg przebiegów.



***2**. Przykładowy sposób powiązania modułów systemu JZH 111*

System ten najlepiej sprawdza się w przypadku stacji małej i średniej wielkości, ponieważ dla dużych stacji kłopotliwe jest odpowiednie zaprojektowanie obwodów tak aby możliwe było osiągnięcie optymalnych wskaźników eksploatacyjno – ruchowych dla stacji (głównie w przypadku definiowania wykluczeń przebiegów sprzecznych).
System przekaźnikowych urządzeń zblokowanych JZH 111 przedstawiony na rys. **2** [15], [26], [27], wyróżnia się w swojej budowie zastosowaniem określonych, powtarzalnych bloków przekaźnikowych odpowiadających za obsługę i sterowania jednego określonego typu urządzenia na stacji (zwrotnicy, sygnalizatora, …) wykonanych w formie zamkniętego uniwersalnego , powtarzalnego, wielo-przekaźnikowego zmontowanego modułu.

Poszczególne moduły łączone są między sobą odpowiednimi ścieżkami logicznymi, poniżej wymienione zostały przykładowe ścieżki logiczne: wybierania elementów drogi przebiegu, kontroli dostępu do modułu, poszukiwania ochrony bocznej, nastawiania elementów drogi przebiegu, utwierdzania modułów, kontroli prędkości (obrazu sygnałowego), przekaźników sygnałowych, automatycznego zwalniania przebiegu, doraźnego zwalniania przebiegu. Przykładowy sposób powiązania modułów systemu JZH 111 przedstawia rysunek **2**:

W praktyce na stacjach eksploatowanych przez PKP PLK S.A. spotkać można wiele systemów przekaźnikowych srk zarówno wykonanych w technice przebiegowej (urządzenia typu E, PB) jaki i zblokowanej (IZH 111, SUP-3, OSA-H, …), które coraz częściej dostosowywane są do współpracy z komputerowymi pulpitami nastawczymi oraz podlegają centralizacji sterowania w ramach budowy lokalnych centr sterowania. Świadczy to o tym że urządzenia te spełniają zakładane funkcje ruchowe, ponadto jak wykazały to doświadczenia ponad 50 lat eksploatowania urządzeń przekaźnikowych na sieci PKP, charakteryzują się one dużą trwałości i niezawodnością oraz gwarantują wymagany poziom bezpieczeństwa technicznego (pod warunkiem zachowania zasad ich utrzymania i eksploatacji, co staje się ze względu na upływ czasu coraz trudniejsze zapewnienie właściwych elementów niezbędnych do ich bezpiecznej eksploatacji (tj. przekaźniki których produkcja jest kosztowna ze względu na konieczność utrzymywania drogiej technologii oraz spadające zapotrzebowanie na rynku).

Tab. 1. *Bezpieczeństwo systemów sterowania ruchem kolejowymw UE*

Założenia	Intensywność usterek (na godzinę) [h^{-1}]
Dopuszczalna wypadkowość spowodowana niebezpieczną usterką techniczna = 1 wypadek rocznie w UE	10^{-4} Dla całego systemu kolei w UE (wszystkie instalacje systemów)
1 niebezpieczna usterka na 10 prowadzi do wypadku	10^{-3} Dla całego systemu kolei w UE (wszystkie instalacje systemów)
1 usterka na 10 jest usterką systemu sterowania ruchem kolejowym	10^{-4} Dla całego systemu sterowania ruchem kolejowym w UE (wszystkie instalacje srk)
Margines bezpieczeństwa 10:1 zapewniający odpowiedni poziom tolerancji	10^{-5} Dla całego systemu sygnalizacji kolejowej w UE (wszystkie instalacje sygnalizacji)
1000 kompletnych systemów sygnalizacji w UE	10^{-8} Dla kompletnego systemu sygnalizacji (np. sterowanie w obszarze lub na linii)
10 podsystemów wchodzących w skład jednego kompletnego systemu sygnalizacji	10^{-9} Dla podsystemu sygnalizacji (np. duży scentralizowany system zależnościowy)
100 elementów systemowych w jednym podsystemie	10^{-11} Dla jednego elementu systemowego (sterownik zwrotnicy, sygnalizatora)
Współczynnik 100:1 pomiędzy sąsiednimi Poziomami Bezpieczeństwa	10^{-11} (dla Poziomu Bezpieczeństwa 4) 10^{-9} (dla Poziomu Bezpieczeństwa 3) 10^{-7} (dla Poziomu Bezpieczeństwa 2) 10^{-5} (dla Poziomu Bezpieczeństwa 1)

Bezpieczeństwo systemów komputerowych

Filozofia bezpieczeństwa wprowadzanych w latach 70 ubiegłego wieku systemów komputerowych zakładała jednakowe prawdopodobieństwo przekłamań 1 → 0 i 0 → 1. Spowodowało to inne podejście do pojęcia bezpieczeństwa – usterka krytyczna była wynikiem wystąpienia więcej niż jednego uszkodzenia, powinno wystąpić co najmniej dwie niezależne usterki w odizolowanych od siebie niezależnych kanałach przetwarzania, Dodatkowo każda usterka pojedyncza, niekrytyczna powinna być wykryta w określonym (przez normę) czasie.

Tabela **1** przedstawia filozofię bezpieczeństwa, jak od podstawowego założenia (jedno zdarzenie krytyczne, katastroficzne, czyli wypadek z ofiarami w ludziach, przekłada się na niezawodność systemów , podsystemów, urządzeń i zastosowanych podzespołów. Interpretując Tabelę I można stwierdzić, że wyjściowe założenie – jedno zdarzenie krytyczne rocznie na terenie UE stanowi minimum jakim jest dopuszczalny poziom ryzyka *THR*, przekłada się to na zredukowaną intensywność uszkodzeń komponentów podsystemów srk. Przyjęcie takich intensywności prowadzi do średniej intensywności uszkodzeń scentralizowanego systemu sterowania rzędu 10-5/h, co daje średnią intensywność uszkodzeń rzędu 10^{-3}/h w całym kolejnictwie w UE (średnio jedno niebezpieczne uszkodzeni w ciągu roku).

Podstawą projektowanych systemów były systemy nadmiarowe (ang. *redundant systems*) – wielokanałowe systemy komputerowe z niezależnym zasilaniem, zwielokrotnionym i niezależnymi i kanałami transmisji oraz rygorystycznie przestrzeganymi standardami oprogramowania i konfiguracji sprzętowej. Określały to normy grupy EN 5012x, obowiązujące w Polsce po 2005 roku. Podstawą wprowadzonych nowych kryteriów bezpieczeństwa był Tolerowalny Poziom Ryzyka *THR* (ang. *//Tolerable Hazard Risk*) [3], [10], którego zasady zostaną poniżej przedstawione.

Realizacja bezpieczeństwa systemów komputerowych stosowanych w kolejnictwie oparta jest o zasadę *fail-safe* [5]. W kolejnictwie występuje wiele systemów, które ze względu na potencjalne zagrożenia wynikające z ich uszkodzenia, zostały odpowiednio sklasyfikowane [3]. W tabeli **1**. przedstawiona została nowa koncepcja bezpieczeństwa oparta na teorii niezawodności [2]. Koncepcja bezpiecznych systemów komputerowych stosowanych w kolejnictwie zakłada bardzo małą intensywność usterek, co przy całkowitej niezależności kanałów przetwarzania (2 lub 3) gwarantuje znikome prawdopodobieństwo wystąpienia usterki podwójnej lub wielokrotnej – decydującej o uszkodzeniu katastroficznym (krytycznym). Podstawą analizy jest akceptowalny, dopuszczalny poziom ryzyka.

Zgodnie z normą [9] bezpieczeństwo systemu zależy nie tylko od intensywności uszkodzeń, ale od czasu detekcji uszkodzeń pojedynczych i podwójnych (wielokrotnych). W tym celu wprowadzono współczynnik tolerowalnego poziomu uszkodzeń (*THR - Tolerable Hazard Rate*). Współczynnik ten można obliczyć z zależności:

$$THR = \prod_{i=1}^{n} \frac{\lambda_i}{t_{d_i}^{-1}} \cdot \sum_{i=1}^{n} t_{d_i}^{-1} \qquad (1)$$

gdzie: λ_i – intensywność uszkodzeń dla kanału i, t_d^{-1} – czas reakcji systemu na błąd od czasu powstania dla kanału i.
Zgodnie z zaleceniami UIC i CENELEC dla systemów bezpiecznych przyjmuje się współczynnik 100:1 pomiędzy intensywnościami usterek dla sąsiednich poziomów bezpieczeństwa. Koncepcja bezpiecznych systemów komputerowych stosowanych w kolejnictwie zakłada bardzo małą intensywność usterek, co przy całkowitej niezależności kanałów przetwarzania (2 lub 3). Z bezpieczeństwem systemów srk zakwalifikowanych do poziomu SIL-4 wiąże się również czas diagnostyki usterek pojedynczych:

$$T_{sf} = \frac{k}{1000 \cdot \lambda} \qquad (2)$$

oraz usterek podwójnych:

$$T_{2sf} = \frac{2}{\lambda} \qquad (3)$$

gdzie: k - współczynnik nadmiarowości równy 1 dla systemów „2z2" i 0.5 dla systemów '2z3", λ - suma średnich intensywności uszkodzeń elementów, których jednoczesne uszkodzenie może prowadzić do zagrożenia.

Ze wzoru (1) wynika, ze dla syste-

mów z jednym kanałem przetwarzania wartość *THR* odpowiada intensywności uszkodzeń λ . Z kolei dla systemu złożonego z dwóch kanałów przetwarzania wzór przyjmuje postać $\lambda \cdot 2t_d/t_{TF}$, co oznacza, że intensywność uszkodzeń krytycznych została zredukowana w stopniu $2t_d/t_{TF}$, gdzie t_d jest czasem reakcji na uszkodzenie, zaś t_{TF} jest średnim czasem do wystąpienia uszkodzenia w kanale.

Wspomniane w tabeli poziomy bezpieczeństwa odnoszą się do systemów zarządzania i sterowania ruchem kolejowym, systemy srk są zaliczone do najwyższego, czwartego poziomu bezpieczeństwa (SIL4).

W związku z wejściem Polski do struktur unijnych obowiązujące stały się normy oznaczone odpowiednio: PN-EN 50126 [17], PN-EN 50128 [18] oraz PN-EN 50129 [19].

W normie PN-EN 50126 określono niezawodność, gotowość, dostępność i bezpieczeństwo (RAMS - *Reliability, Availability, Maintainability and Safety*), jako proces oparty o cykl życia systemu (ang. system *life-cycle*). W procesie tym zdefiniowano poszczególne etapy systemu i procedury związane z zatwierdzaniem przed przejściem do następnego etapu. (specyfikacja wymagań, projekt., implementacja, itp.).

Tab. 2. *Klasyfikacja bezpieczeństwa w systemach zarządzania i sterowania ruchem w UE*

POZIOM	Wymagany stan bezpieczeństwa	Konsekwencje wystąpienia błędu	Charakterystyka systemu w kolejnictwie	Nazwa systemu stosowana w kolejnictwie
4	Bardzo wysoki	Utrata życia ludzkiego	Zabezpieczenie przed wykolejeniem i kolizją pociągów	System bezpieczny *Fail-safe* system
3	Wysoki	Obrażenia i utrata zdrowia	Zapewnienie poprawnego prowadzenia pociągu	System o wysokim poziome bezpieczeństwa
2	Średni	Skażenie środowiska	Zapewnienie kiero wania ruchem pociągu	System o znaczącym poziomie bezpieczeństwa
1	Niski	Utrata mienia	Zapewnienie obsługi pasażerów	System o niskim poziome bezpieczeństwa
0	Nie dotyczy	Utrata informacji nie mających wpływu na bezpieczeństwo	Zapewnienie prawidłowego utrzymania kolei	Nie związany z bezpieczeństwem

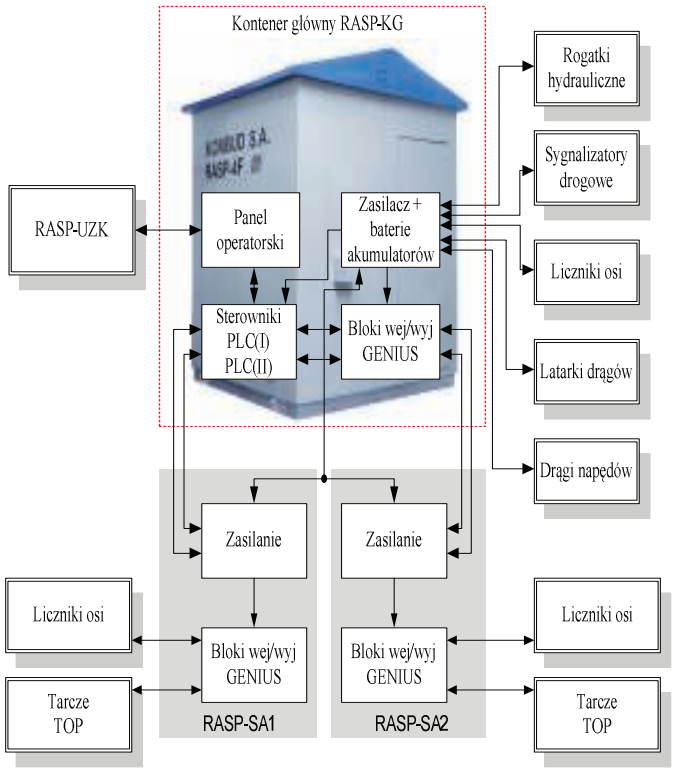
Norma PN-EN 50128 określa procedury i wymagania techniczne dla projektowania oprogramowania bezpiecznego systemu elektronicznego dla sterowania i zabezpieczenia na kolei, [98]. Należy stwierdzić, iż norma ta nie jest w pełni obligatoryjna.

Norma PN-EN 50129 definiuje wymagania dotyczące projektowania, testowania, odbioru i zatwierdzania elektronicznych systemów, podsystemów i urządzeń sygnalizacji związanych z bezpieczeństwem w zastosowaniach kolejowych].

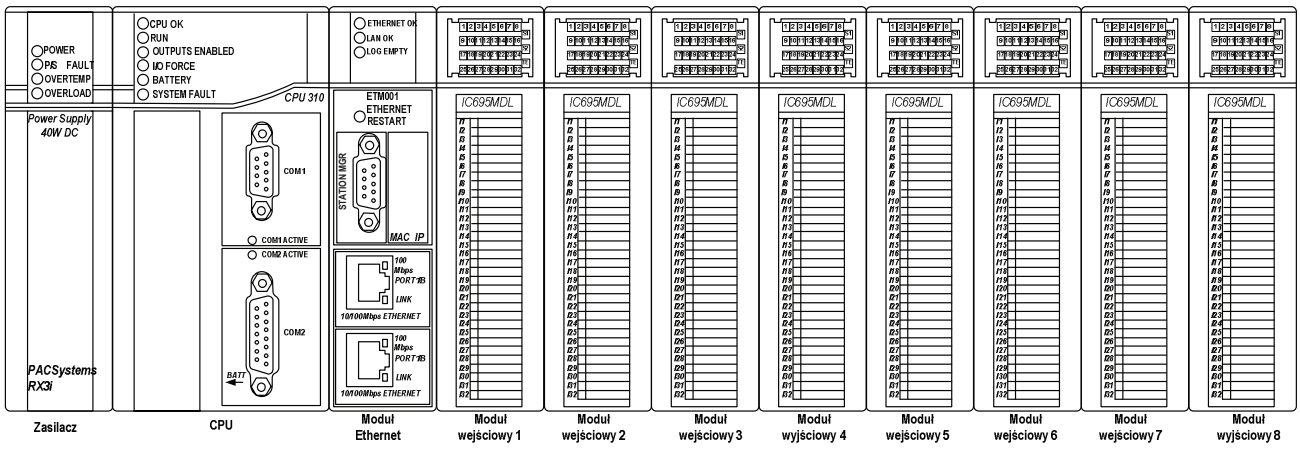
Uwzględniając takie parametry jak: czas reakcji systemu na błąd od czasu wykrycia, czas reakcji systemu na błąd od czasu powstania, czas cyklicznego testowania elementu systemu, średnie czasy T_{MBF} składowych systemu, można wyznaczyć współczynnik *THR*. Dopuszczalne wartości współczynnika *THR* dla poziomów bezpieczeństwa SIL

Tab. 3. *Dopuszczalne wartości THR zgodne zobowiązującymi normami*

THR (na godzinę na funkcję)	SIL (Safety Integrity Level)
$10^{-9} \le THR < 10^{-8}$	4
$10^{-8} \le THR < 10^{-7}$	3
$10^{-7} \le THR < 10^{-6}$	2
$10^{-8} \le THR < 10^{-7}$	1



3*. Dwukanałowa realizacja samoczynnej sygnalizacji przejazdowej RASP-4F*



***4**. Kaseta samoczynnej sygnalizacji przejazdowej RASP-4F*

przedstawia tabela **3** [9].

Co oznacza, że intensywność uszkodzeń krytycznych została zredukowana w stopniu $2t_d/t_{TF}$, gdzie td jest czasem reakcji na uszkodzenie, zaś t_{TF} jest średnim czasem do wystąpienia uszkodzenia w kanale.

W ten sposób można było ocenić bezpieczeństwo typowego systemu sygnalizacji przejazdowej (RASP4 produkcji KOMBUD S.A [29], [30].) zaliczonego do najwyższego poziomu bezpieczeństwa SIL4. Jest to typowy system dwukanałowy (rys. **3**), dwa niezależne sterowniki PLC realizują wszystkie funkcje wyszczególnione w normach i zarządzeniach.

Sterowniki PLC zbudowane są w oparciu o dwa identyczne zestawy zbudowane na kasetach tworząc dwa niezależnie działające sterowniki ze wzajemną wymianą danych i synchronizacją pracy poprzez magistralę Ethernet. W skład pojedynczego sterownika wchodzą:

- kaseta bazowa IC695CHS012,
- zasilacz prądu stałego IC695PSD140,
- jednostka centralna typu IC695CPU310,
- interfejs komunikacyjny IC695ETM001,
- moduł wejść dyskretnych IC694MDL660,
- moduł wyjść dyskretnych IC694MDL754

Dla zastosowanego sprzętu autorzy podali następujące wartości MTBF (średni czas pomiędzy wystąpieniem uszkodzeń) na podstawie danych producenta/dystrybutora sprzętu (firma Astor Kraków):

a) kaseta bazowa IC695CHS012 – 761 000 [h]
b) zasilacz prądu stałego IC695PSD140 – 1 092 000 [h]
c) jednostka centralna IC695CPU310 – 638 000 [h]
d) interfejs komunikacyjny IC695ETM001 – 992 000 [h]
e) moduł wejść dyskretnych IC694MDL660 – 6 393 000 [h]
f) moduł wyjść dyskretnych IC694MDL754 – 553 000 [h].

Konfiguracja sterowników zawiera różne ilości modułów, co przy założeniu najgorszego przypadku (szeregowa struktura niezawodnościowa) prowadzi do wypadkowej wartości MTBF dla poszczególnych zestawów:

1 zestaw z 2 modułami e) i 1 modułem f) – 144 374.4267 [h]
2 zestaw z 3 modułami e) i 1 modułem f) – 141 185.9945 [h]
3 zestaw z 4 modułami e) i 1 modułem f) – 138 135.3490 [h]
4 zestaw z 6 modułami e) i 2 modułami f) – 106 832.6186 [h].

Autorzy zapewnili dostatecznie krótki czas wykrywania pojedynczego uszkodzenia i przejście do stanu bezpiecznego. (Czas ten, t_{sf}, jest znacznie krótszy niż oczekiwany średni czas między uszkodzeniami obu komputerów.) Zgodnie z normą PN-EN 50129 czas wykrywania pojedynczego uszkodzenia spełniający warunek ‚t_{sf} <= k/(1000 · a), gdzie k = 1.0 dla systemów „2 z 2", a – 1/MTBF.

Autorzy przyjęli do obliczeń współczynnika *THR* następujące wartości:

- czas cyklicznego testowania wejść/wyjść (T) 250ms
- czas reakcji na błąd (NT) 1s,

co daje wartość czasu reakcji na błąd (SDT) równą 0.0003125 [h] i w efekcie daje wartość *THR* poniżej co 10e-1, zgodnie z normą PN-EN 50129 dla poziomu SIL4. Obliczony czas wykrycia błędów pojedynczych (*TSF*) spełnia kryterium wynikające z granicznej wartości odniesionej do oszacowanej wartości MTBF dla systemu „2 z 2" podane w normie PN-EN 50129.

Współczynnik *THR* można również określić *n* a podstawie:

- danych eksploatacyjnych (czyli systemów obecnie eksploatowanych) na podstawie danych pochodzących z eksploatacji (wymagany do weryfikacji czas to ponad 10 lat [x]),
- danych z prognozowania obliczonych na podstawie reguł szacowania niezawodności urządzeń elektronicznych w oparciu o standard MIL [xx}.

Obie wymienione metody uzupełniają ocenę bezpieczeństwa zgodnie z wymienionymi normami i regulacjami krajowymi.

Bezpieczeństwa systemów z nowymi technologiami informacyjnymi

Bardzo dobrym przykładem wpływu nowych technologii informatycznych na bezpieczeństwo systemów zarządzania i sterowania ruchem w transporcie jest Europejski System Zarządzania i Sterowania Ruchem pociągów ERTMS (ang. *European Rail Traffic Management System*) obligatoryjnie wdrażany w państwach członkowskich UE. Podsystem odpowiedzialny bezpośrednio za bezpieczeństwo pociągu ETCS (ang. *European Train Control System*) został zdefiniowany dla trzech poziomów sterowania, w kolejnictwie polskim został wdrożony na wybranych odcinkach linii poziom 1, trwają prace nad wdrażaniem poziomu 2 co wiąże się bezpośrednio z bezpieczeństwem pociągów o podwyższonej prędkości (linia CMK) [5], [14]. Wprowadzenie, jako obowiązkowego systemu ERTMS/ETCS wykorzystującego transmisję radiową powinno zapewnić osiągnięcie, jako główny cel wysokiego poziomu funkcjonalności i interoperacyjności w obsłudze pociągów pasażerskich, w tym kontroli i monitorowania sieci linii kolei dużych prędkości (KDP).

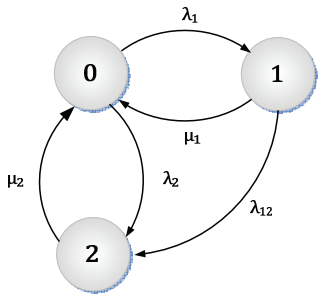
W przypadku implementacji systemu ETCS przyjęte zostało następujące kryterium bezpieczeństwa: nowe rozwiązania technologiczne nie mogą obniżyć istniejącego poziomu bezpieczeństwa. Przypadku systemu ETCS można było odwołać się do systemów tradycyjnych (eksploatowanych obecnie systemów ze stałym odstępem blokowym opartych na odcinkach izolowanych i blokadą liniową) i pokazać jak nowe technologie radykalnie zmniejszają prawdopodobieństwo błędu krytycznego. Podstawowe zagadnienia związane z systemem ERTMS/ETCS odnoszą się do:

- poprawy bezpieczeństwa (monitoring maszynisty),
- zwiększenie przepustowości linii kolejowych, zwłaszcza linii KDP,
- wdrożenie nowego standardu komunikacji wykorzystującego system ERTMS/GSM-R, a w przyszłości bardziej efektywnych standardów transmisji radiowej w tym LTE lub WiFi [9].

Pociągi wyposażone w urządzenia pokładowe systemu ERTMS/ETCS będą informowane o tym, które z poziomów ERTMS są obsługiwane w danym obszarze z chwilą minięcia grupy balis informujących o zbliżaniu się do danego obszaru ERTMS/ETCS. Urządzenia pokładowe (zgodnie z kompatybilnością części pokładowej z przytorową) po odebraniu informacji wjazdu w obszar przełączą się do poziomu systemu ERTMS/ETCS, który zdefiniowany jest w ramach realizacji projektu zabudowy systemu.

Poziom pierwszy stanowi nakładkę na urządzenia stacyjne i liniowe zachowującą rozproszony charakter sterowania ruchem kolejowym. Urządzenia ERTMS/ETCS poziomu 1 zapewniają, że pociąg nie przejedzie poza miejsce ograniczające ustawioną i utwierdzoną drogę przebiegu, oraz że nie przekroczy prędkości dopuszczalnej na żadnym odcinku drogi przebiegu. Tor wyposażony w urządzenia poziomu pierwszego wykorzystuje eurobalisy przełączalne i nieprzełączalne. Dodatkowo może być wyposażony w europętle lub radio wykorzystywane do uaktualniania informacji przekazywanej poprzez eurobalisy lub do dwukierunkowej komunikacji tor-pojazd w celu prowadzenia wstępnej obróbki informacji przez urządzenia przytorowe.

Poziom drugi ERTMS/ETCS to sterowanie ruchem w oparciu o ciągłą, cyfrową, dwukierunkową transmisję radiową. Tor jest wyposażany poza eurobalisami dodatkowo w radiowe centra sterowania (RBC). Jednocześnie z toru można usunąć semafory, gdyż ich funkcje przejmuje ciągła transmisja cyfrowa. Informacje zmienne łatwo można przekazywać poprzez kanał radiowy, dzięki temu eurobalisy nie muszą już być przełączalne. Poziom trzeci stanowi rozwinięcie poziomu drugiego poprzez przeniesienie kontroli zajętości torów z urządzeń przytorowych do urządzeń pojazdowych. Pozwala to na sterowanie następstwem pociągów według zasady ruchomego odstępu blokowego oraz umożliwia rezygnację



***5**. Uniwersalny model sterowania i kontrolo pociągu*

z obwodów torowych i liczników osi.

Jazda pociągu z punktu widzenia urządzeń sterowania ruchem kolejowym mogą być przedstawiane podejściem prezentowanym przez proces stochastyczny. W wielu pracach [[8], [10], [12] do opisu przejść między stanami odpowiadającymi za typowe zachowania pociągu wskazywany jest jednorodny, stacjonarny i ergodyczny proces Markowa.

Taki proces kontroli pociągu zaprezentowany jest na rysunku **5** [14]. Zaprezentowane stany odpowiadają następującym sytuacjom:

0 – stan prawidłowej jazdy według ostatniej otrzymanej informacji, maszynista prowadząc pojazd trakcyjny według ostatnio otrzymanego pozwolenia na jazdę aż do odebrania następnej informacji o nowym zezwoleniu na jazdę,

1 – stan poprawnej realizacji procedury kontroli (zgodnie z zobrazowaniem sygnałowym prezentowanym na sygnalizatorze lub według zaleceń komputera pokładowego),

2 – stan awaryjnego zatrzymania lub zmniejszenia prędkości wynikające z zaistnienia sytuacji, w której utracona została kontrola (awaryjne hamowanie wymuszone przez system ATP – w warunkach Rzeczpospolitej Polskiej – system SHP klasy AWS).

Przejścia pomiędzy stanami związane są z występowaniem podstawowych parametrów w wykonywanych procedurach realizowanych w urządzeniach sterowania ruchem kolejowym. W dalszych rozważaniach, zakładamy przyjęcie maksymalnej długości od-

stępu blokowego wynoszącą 1500 m (minimalna odległość 1300 m nie jest w tych analizach obligatoryjna) dla maksymalnej prędkości 160 km/h, oraz parametry λ i μ określające:

- λ_1 – intensywność wymaganych jazd dla poprawnie otrzymanych zezwoleń na jazdę wynoszącą 106,67h^{-1} (odpowiadająca czasowi przygotowania do wyświetlenia pojazdowi trakcyjnemu sygnału zezwalającego 33,75s),
- μ_1 – intensywność typowej obsługi wynosząca 300 h^{-1} (odwrotność czasu obsługi 12s),
- λ_2 – intensywność dla błędnych interpretacji względem wymagań (wskaźnik awaryjności) wynoszący 0,000227687 h^{-1} (związany z wystąpieniem 2 jazd zakończonych zatrzymaniem awaryjnym w roku),
- λ_{12} – intensywność pojawiających się błędnych interpretacji względem wymagań (wskaźnik awaryjności) 0,005952381 h^{-1} (związana z czasem występującym podczas jazd awaryjnych, 1 w tygodniu)
- μ_2 – intensywność obsługi awaryjnej wynosząca 72 h^{-1} (odwrotność czasu obsługi awaryjnej 50 s).

Wykorzystywane do opisu przejść pomiędzy stanami równania różniczkowe oparte są na:

– parametrach odległości oraz prędkości zaprezentowanych powyżej oraz

- λ_1 – intensywności zdarzeń związanych z wyjazdem pociągu na sygnał zezwalający lub otrzymane zezwolenie na jazdę (MA) oraz otrzymaną informacją o kolejnej procedurze jazdy,
- λ_{12} – intensywności zdarzenia związanego z błędną reakcją maszynisty lub niewłaściwego działania systemu ATP,
- λ_2 – intensywności zdarzenia związanego z wdrożeniem przez sygnał alarmowy hamowania (bez udziału maszynisty) trwającego aż do całkowitego zatrzymania pociągu,
- μ_1^{-1} – czasu niezbędnego do wyświetlania maszyniście informacji o następnym działaniu – procedura jazdy pociągu z uwzględnieniem warunków bezpieczeństwa,
- μ_2^{-1} – czasu niezbędnego maszyniście do rozpoczęcia jazdy po automatycznym zatrzymaniu pociągu.

W istniejących urządzeniach srk, które są wykorzystywane do prowadzenia pociągu opartego na stałym odstępie blokowym (zajętość kolejnych odcinków) następuje na podstawie wyświetlenia sygnału zezwalającego na jazdę z jednoczesnym uzyskaniem informacji o zajętości od przemieszczającego się po linii kolejowej pojazdu trakcyjnego.

Oczywisty jest sens powyższej sekwencji zdarzeń. Dlatego stan P2 może być traktowany jako współczynnik operacyjny (funkcjonalny), który odpowiedzialny jest za skuteczność sterowania. Oznacza to, że sposób sterowania pociągiem odniesiony jest do zdolności przepustowości linii kolejowej wynikającej z możliwości zajmowania kolejnych odcinków torowych.

Zakładając maksymalną długość odstępu blokowego wynoszącą 1500 m i maksymalną prędkości 160 km/h oraz parametry dla modelu Markowa przedstawione na rysunku **5** wynoszące:

- λ_1 – intensywność wymaganych jazd dla poprawnie otrzymanych zezwoleń na jazdę wynoszącą 106,67h^{-1} (odpowiadająca czasowi przygotowania do wyświetlenia pojazdowi trakcyjnemu sygnału zezwalającego 33,75s),
- μ_1 – intensywność typowej obsługi wynosząca 300 h-1 (odwrotność czasu obsługi 12 s),
- λ_2 – intensywność dla błędnych interpretacji względem wymagań (wskaźnik awaryjności) wynoszący 0,000227687 h^{-1} (związany z wystąpieniem 2 jazd zakończonych zatrzymaniem awaryjnym w roku),
- λ_{12} – intensywność pojawiających się błędnych interpretacji względem wymagań (wskaźnik awaryjności) 0,005952381 h^{-1} (związana z czasem występującym podczas jazd awaryjnych, 1 w tygodniu)
- μ_2 – intensywność obsługi awaryjnej wynosząca 72 h^{-1} (odwrotność czasu obsługi awaryjnej 50 s)

po podstawieniu do powyższych równań i dokonaniu obliczeń otrzymujemy wartość dla stałego odstępu blokowego wynoszącą P_{2FBD} =2,401·10^{-5}.

System ERTMS/ETCS jest inteligentną nakładką na istniejące zapewniające wysoki poziom bezpieczeństwa kolejowe systemy kontroli i zarządzania ruchem kolejowym. Wszystkie pociągi niewyposażone w urządzenia pokładowe systemu ERTMS/ETCS będą odbierały zezwolenie na jazdę (MA) poprzez wyświetlone zobrazowanie sygnałowe na sygnalizatorze. Pojazdy trakcyjne wyposażone w pokładowe urządzenia systemu ERTMS/ETCS poziomu 1 otrzymują zezwolenie na jazdę po przejechaniu nad grupą balis umieszczona przed sygnalizatorem, natomiast w przypadku poziomu 2 zezwolenie na jazdę będzie odbierane przez pojazd trakcyjny z radiowego centrum sterowania (RBC) za pośrednictwem bezpiecznej sieci kolejowego globalnego systemu komunikacji ruchomej ERTMS/GSM-R. Urządzenia trakcyjne posiadają możliwość pracy według różnych planów (poziomów i trybów) przy uwzględnieniu zgodności urządzeń pokładowych z urządzeniami przytorowymi. Istniejące zasady współpracy urządzeń pokładowych z odpowiednimi urządzeniami przytorowymi zapewniają współpracę w tzn "dół", tj. Pojazd trakcyjny wyposażony w urządzenia poziomu 2 może jeździć po liniach kolejowych z zainstalowanymi urządzeniami poziomu 2 jak i poziomu 1, natomiast pojazdy trakcyjne wyposażone w urządzenia poziomu 1 mogą poruszać się tylko po liniach kolejowych wyposażonych w ten sam poziom.

Pociągi wyposażone w urządzenia pokładowe systemu ERTMS/ETCS będą informowane o objęciu ich kontrolą w określonym obszarze kolejowym ograniczonym balisami określającymi także odpowiedni poziom systemu.

Poziom 1 jest nakładką na urządzenia sterowania ruchem kolejowym stosowane na stacjach oraz na szlakach i

jest traktowany jako rozproszony system kontroli. Urządzenia poziomu 1 systemu ERTMS/ETCS zapewniają to, że nadzorowany pojazd trakcyjny nie przejedzie po za wyznaczone zezwolenie na jazdę na szlaku po którym się porusza oraz jazda pojazdu trakcyjnego odbywa się z nadzorowaniem nieprzekroczenia dozwolonej prędkości na przemierzanej drodze kolejowej. W torze, na którym zabudowany jest poziom 1, w obszarach kontrolnych, wykorzystywane są eurobalisy, zarówno w wersji przełączalnej jak i nieprzełączalnej. Dodatkowo torowa infrastruktura kolejowa może być wyposażona w europętlę lub radio wykorzystywane jako uaktualnienie informacji przekazywanej pomiędzy torem a pojazdem trakcyjnym lub do dwukierunkowej komunikacji pojazdu trakcyjnego służącej do aktualizacji informacji o pojeździe po stronie urządzeń przytorowych [14].

Zakładając maksymalną długość odstępu blokowego wynoszącą 1500 m oraz w tym przypadku dla maksymalnej prędkości 160 km/h oraz parametrów dla modelu Markowa przedstawionych na rysunku **5** wynoszących:

- λ'_1 – intensywność połączenia przed balisą (semaforem) wynoszącą λ_1=166,67h^{-1} (w odniesieniu do 21,6s),
- μ'_1 – oszacowane (intensywności) usług wynoszące 360000 h^{-1} (związane z max 10 ms) jest związane z założeniem czasu synchronizacji przy przejechaniu 1 m,
- λ'_{12} – intensywność uszkodzonych telegramów z balis prowadzących do zatrzymania pociągu wynosząca 0,33·10^{-9}/h ,
- λ'_2 – intensywność awarii urządzeń pokładowych wynosząca zgodnie z *THR* dla urządzeń pokładowych 1·10^{-9},
- μ'_2 – intensywność przełączeń urządzeń pokładowych do trybu dedykowanego dla pociągów niewyposażonych wynosząca 0,03333 h (związana z 120 s, czasem wdrożenia jazdy w trybie pociągu niewyposażonego)

po podstawieniu do powyższych równań i dokonaniu obliczeń otrzymujemy wartość dla ERTMS/ETCS poziomu 1 P2ETCS L1 = 3,003·10-8.

Przeprowadzone obliczenia analityczne pokazują jak nowy system (ETCS) w istotny sposób minimalizuje wystąpienie zdarzenia katastroficznego (P_2).

Wnioski

W artykule pokazano ewolucję pojęcia bezpieczeństwa systemów zarządzani i sterowania ruchem kolejowym na przestrzeni ostatnich lat. Punktem wejściowym było przyjęcie poziomu bezpieczeństwa przekaźnikowych systemów srk. Przedstawione rozwiązania systemów JZH i E oparte były na koncepcji bezpiecznego przekaźnika, którego najbardziej prawdopodobne uszkodzenie nie miało wpływu na bezpieczne wysterowanie urządzeń zewnętrznych.

Omówione powszechnie stosowane systemy komputerowe oparte były na nadmiarowości i stosunkowo krótkim czasie wykrywania usterek. Wynikowym parametrem był *THR* (Tolerowalny Poziom Ryzyka), którego wartości były zdefiniowane w obowiązujących normach (PN EN 50 159).

Kolejnym krokiem było wprowadzenie otwartych standardów transmisji opartych na publicznych sieciach, głównie bezprzewodowych [9]. Badania potwierdzają, że zastosowanie typowych standardów komunikacji opartych na bezprzewodowym dostępie do Internetu przy zastosowaniu odpowiednich procedur, a zwłaszcza metod kryptograficznych, pozwala zapewnić ten sam poziom bezpieczeństwa co w przypadku dotychczas stosowanych transmisji kablowych w rozproszonych systemach komputerowych. Generalnie począwszy od systemów przekaźnikowych po przyszłe realizacje oparte na transmisji otwartej stosowana jest ta sama zasada *fail-safe*: każde pojedyncze uszkodzenie nie może prowadzić do sytuacji niebezpiecznej. W systemach komputerowych wyznaczany jest dodatkowo czas detekcji usterki. W systemach opartych na sieciach publicznych dodatkowo analizuje się minimalizację czasu opóźnień (spowodowanych np. zanikiem lub przekłamaniem transmisji i związana z tym koniecznością powtórzeń itp.) co pozwoliło zapewnić identyczny poziom funkcjonalności co w systemach realizowanych dotychczas, tych komputerowych jak i przekaźnikowych.

W każdym zaprezentowanym modelu (stały odstęp blokowy, poziom 1) prawdopodobieństwo stanu 2 jest istotne z punktu widzenia niedostępności systemu (stan 2 odpowiada niekontrolowanemu awaryjnemu zatrzymaniu pojazdu trakcyjnego spowodowanego przez wadliwe działanie urządzeń sygnalizacyjnych lub urządzeń automatycznej kontroli pojazdu trakcyjnego). Możemy zauważyć, że każdy następny poziom kontroli pojazdu trakcyjnego zmniejsza prawdopodobieństwo wystąpienia stanu 2, więc dostępność całego systemu ulega polepszeniu. Jest to związane z ideą systemu ERTMS/ETCS: lepszą przepustowością, dostępnością i w konsekwencji lepszymi parametrami ruchu kolejowego, w tym także kolei dużych prędkości [2, 6]. Prace te zawierają również podobną analizę dla poziomu 2 i 3 systemu ETCS, pokazującą istotne zmniejszenie (o trzy rzędy wielkości) prawdopodobieństwa wystąpienia zdarzenia katastroficznego.

Do analizy bezpieczeństwa można stosować też inne metody [20], [21], takie jak np. analiza drzewa usterek FTA (ang. *Fault Tree Analysis*) uzupełniona o zależności czasowe [13] staje się silnym narzędziem zapewnienia bezpieczeństwa.

Podsumowując, nowe technologie informacyjne wprowadzane na przestrzeni ostatnich lat zapewniają poziom bezpieczeństwa, nie gorszy niż w systemach przekaźnikowych tradycyjnie uznane za bezpieczne. Nowe technologie informacyjne kontrolują człowieka (maszynistę, dyżurnego ruchu) minimalizując wystąpienie zdarzenia krytycznego określonego przez zredukowaną intensywność (*THR*) lub prawdopodobieństwo wystąpienia takiego zdarzenia. ◄

Materiały źródłowe

[1] Dąbrowa – Bajon M. „Podstawy sterowania ruchem kolejowym" – ISBN 83-7207-343-0 Oficyna Wydawnicza Politechniki Warszawskiej 2002,

[2] Jaźwiński J., Ważyńska – Fiok K.: „Bezpieczeństwo i niezawodność systemu sterowania ruchem kolejowym", Zeszyt 95, WKiŁ, Warszawa 1982

[3] Lewiński A., Perzyński T.: „Akceptowalny poziom ryzyka jako kryterium bezpieczeństwa w transporcie kolejowym", prace konferencji Wydziału Transportu Politechniki Radomskiej Logi-Trans 2007

[4] Lewiński A., Perzyński T., Toruń A., „Tendencje rozwojowe systemów srk, na przestrzeni ostatnich lat", Problemy Kolejnictwa, Zeszyt 3, 2014,

[5] Lewiński A., Perzyński T., Toruń A, „ETCS jako metoda poprawy funkcjonalności i przepustowości na liniach kolejowych",materiały konferencji LOGITRANS2015

[6] Karaś S. „Urządzenia zabezpieczenia ruchu kolejowego" wyd. 3, WKiŁ W-wa 1986,

[7] Lewiński A., Toruń A. The changeable block distance system analysis, Springer – Verlag Heilderberg 2010 – J. Mikulski (Ed.) TST 2010 CCIS 104, 2010

[8] Lewiński A. „Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego" Politechnika Radomska Monografie nr 49/2001

[9] Lewiński A., Perzyński T., Toruń A.,: "Risk Analysis as a Basic Method of Safety Transmission System Certification". Communications in Computer and Information Scienc 239), Springer-Verlag Berlin Heidelberg 2011

[10] Lewiński A., Perzyński T.: The reliability and safety of railway control systems based on new information technologies. Communications In Computer and Information Scienece 104. Springer 2010'. Transport Systems Telematics

[11] Lewiński A., Toruń A.,: " The Changeable Block Distance System Analysis", Communications in Computer and Information Science (104), Springer-Verlag Berlin Heidelberg 2010

[12] Lewiński A., Torun A., Perzyński T.: "The Analysis of Open Transmission Standards", materiały Międzynarodowej Konferencji Transport Systems Telematics Tst2014, Monografia, Communications In Computer And Information Sience, Telematics – Support Of Transport, Nr 329, Springer-Verlag Berlin Heidelberg 2012 in Railway Control and Management

[13] Magott J., Skrobanek P., Timing analysis of safety properties using fault trees with time dependencies and timed state-charts, Reliability Engineering & Systems Safety, 2012, vol. 97, Nr 1

[14] Lewiński A., Toruń A., Gradowski P: "Modeling of ETCS with respect to functionality and safety including Polish Railways conditions", materiały Międzynarodowej Konferencji Transport Systems Telematics Tst2014, Monografia, Communications In Computer And Information Sience, Telematics – Support Of Transport, Nr471, Springer-Verlag Berlin Heidelberg 2014

[15] Mickiewicz T., Mikulski A., „Elektryczne urządzenia zabezpieczenia ruchu kolejowego – urządzenia stacyjne" WKiŁ Warszawa 1968,

[16] Miksza E., „Zblokowany system sterowania ruchem kolejowym na stacjach typu IZH 111" WKiŁ Warszawa 1979,

[17] Norma PN-EN 50126:2002 (U) Zastosowania kolejowe. Specyfikowanie i wykazywanie Nieuszkadzalności, Gotowości, Obsługiwalności i Bezpieczeństwa (RAMS). Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia.

[18] Norma PN-EN 50128:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Oprogramowanie dla kolejowych systemów sterowania i zabezpieczenia.

[19] Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.

[20] Norma PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów. Procedura analizy rodzajów i skutków uszkodzeń (FMEA),

[21] Norma PN-EN 61025:2007 Analiza drzewa niezdatności (FTA),

[22] Norma PN-EN 61078:2006 Techniki analizy niezawodności – Metoda schematów blokowych niezawodności oraz metody boolowskie,

[23] Norma PN-IEC 60300-3-9:1999 Analiza ryzyka w systemach technicznych,

[24] Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym – DG PKP KA nr KA2b-5400-01/98 z dnia 06.02.1998r.,

[25] Norma PN-EN 50159: 2010. Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania.

[26] Album schematów – zbiór przykładowych rozwiązań – geograficzny system stacyjnych przekaźnikowych urządzeń srk typu CBP83, 1985r.

[27] Geograficzny, zblokowany system urządzeń stacyjnych zrk typu JZH 111 – dokumentacja techniczna, Katowice 1977

[28] Grant MNil pt:„Wpływ nowych technologii informacyjnych na poprawę funkcjonalności i bezpieczeństwa ruchu pociągów" nr 4T12C00529. Politechnika Radomska 2006.

[29] Kombud – materiały Zakładu Automatyki KOMBUD S.A. w Radomiu

[30] Kontron – materiały Kontron East Europe sp. z o.o

[31] Jaźwińskil J., Ważyńska - Fiok K.: „Bezpieczeństwo systemów", PWN Warszawa 1993

[32] Military Hand Book, Reliability Prediction of Electronic Equipment, USA Department of Defense

[33] Quality of Service Test Specification form 11.09.2003 and parameters: GSM-R Interfaces Class 1 Requirements. SUBSET-093 z 11.10.2005r.

[34] Winter P. and other: Compendium on ERTMS. ISBN 978-3-7771-0396-9, UIC, (1st edition 2009)