safety of railway control systems,
safety analysis,
safety transmission

Andrzej LEWIŃSKI[1]
Tomasz PERZYŃSKI [2]
Andrzej TORUŃ[3]

ANALIZA RYZYKA JAKO PODSTAWOWA METODA PROJEKTOWANIA BEZPIECZNEJ TRANSMISJI W SIECIACH OTWARTYCH STOSOWANYCH W SYSTEMACH STEROWANIA RUCHEM KOLEJOWYM

Obowiązująca w UE norma PN-EN 50 159-2 dopuszcza możliwość stosowania otwartych systemów transmisji w sterowaniu ruchem kolejowym. Dotyczy to zarówno przewodowych jak też bezprzewodowych standardów transmisji. Podstawowym kryterium jest zapewnienie dopuszczalnego poziomu ryzyka (THR) zgodnie z obowiązującymi normami PN-EN 50 126 i PN-EN 50 129. Oznacza to, że wskaźnik THR dla systemów srk zaliczonych do danego poziomu bezpieczeństwa SIL nie powinien przekroczyć przewidzianej dla tego poziomu maksymalnej wartości. W pracy omówiono analizę ryzyka uwzględniającą realizację kanału transmisji otwartej na przykładzie dwóch systemach srk projektowanych na potrzeby kolejnictwa polskiego.

THE RISK ANALYSIS AS A BASIC DESIGNED METHODS OF SAFETY OPEN NETWORK TRANSMISSION APPLIED IN RAILWAY CONTROL SYSTEMS

Existing in UE standard PN-EN 50 159-2 allows a possibility of applying the open transmission systems in railway control systems. It is related both cable and wireless transmission standards. The basic requirement is connected with ensuring the Tolerable Hazard Rate according to PN-EN 50126 and PN-EN 50129 railway standards. It's mean that appropriate coefficient THR for safety level does not exceed the permitted value. The paper includes the analysis of two systems with open transmission standards designed for the Polish Railways.

[1] Politechnika Radomska Wydział Transportu i Elektrotechniki; 26-600 Radom, ul. Malczewskiego 29
Tel. +48 48 361-77-57, Fax: +48 48 361-77-42, E-mail: a.lewinski@pr.radom.pl
[2] Politechnika Radomska Wydział Transportu i Elektrotechniki; 26-600 Radom, ul. Malczewskiego 29
Tel. +48 48 361-77-57, Fax: +48 48 361-77-42, E-mail: t.perzynski@pr.radom.pl
[3] Instytut Kolejnictwa; Zakład Sterowania Ruchem i Teleinformatyki; 04-275 Warszawa; ul. Chłopickiego 50
Tel. +48 22 47-31-490, Fax: +48 22 47-31-036, *E-mail: atorun@ikolej.pl*

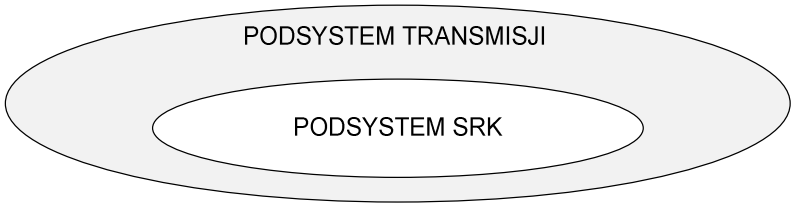
1. WSTĘP

Właściwie przeprowadzona analiza dotycząca oceny wpływu zastosowanego systemu transmisji na parametry niezawodności i bezpieczeństwa systemu srk wymaga indywidualnej analizy odnoszącej się do konkretnego typu aplikacji. Oznacza to, iż każdorazowe zastosowanie systemu transmisji w urządzeniach srk wymaga, zgodnie z normami serii 50 xxx, zastosowania odpowiedniej procedury postępowania, której etapy są zdefiniowane następująco:

- aplikacja,
- analiza zagrożeń,
- redukcja ryzyka,
- przypisanie systemu do poziomów bezpieczeństwa SIL,
- specyfikacja wymagań bezpieczeństwa.

Każdy z wyżej wymienionych punktów wymaga odrębnego uzasadnienia i stosownego udokumentowania. W odniesieniu do systemów srk szczególną uwagę należy położyć na oszacowanie poziomu ryzyka (norma PN-EN 50126). Intensywność uszkodzeń dla ustalonego poziomu SIL określają normy: PN-EN 50126, PN-EN 50128, PN-EN 50129. Na przykład dla systemów sterowania ruchem kolejowym odpowiedzialnych za bezpieczeństwo przyjmuje się wartość z przedziału $10^{-9} \leq \mathrm{THR} < 10^{-8}$ dla poziomu SIL 4.

Przeważnie proponowane systemy transmisji są systemami jednokanałowymi, w związku z tym tolerowany poziom ryzyka THR (*Tolerable Hazard Rate*) jest równy intensywności uszkodzeń. Dla poziomu SIL4 powinien zawierać się w granicach $10^{-9} \div 10^{-8}$ [h^{-1}]. W przypadku, gdy dotyczy systemów dwu lub trzy- kanałowych istotny staje się czas wykrycia usterki, co pozwala na większe intensywności usterek w kanałach transmisyjnych. Schematycznie zależność podsystemu transmisji i srk w systemie z transmisją otwartą pokazano na rys. 1.

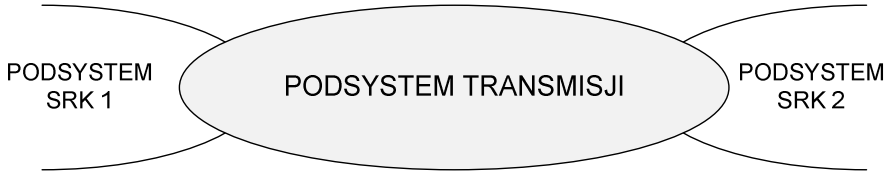


Rys. 1. Struktura systemu z transmisją otwartą wpisaną w system nadmiarowy

Zakładając najbardziej niekorzystny przypadek, gdy transmisja stanowi element w strukturze szeregowej (rys. 2) można oszacować, że intensywność uszkodzeń niebezpiecznych λ_{NT} (związanych z niewykryciem przekłamania w powszechnie stosowanym kodzie integralności CRC32) wyniesie:

$$\lambda_{NT} = \lambda_N \cdot p_{UE} = \lambda_N \cdot 2^{-32} \tag{1}$$

gdzie λ_N jest intensywnością wszystkich uszkodzeń w kanale transmisyjnym, $p_{UE} = 2^{-C}$ jest prawdopodobieństwem niewykrycia błędu (C – numer nadmiarowości bitowej) .



Rys. 2. Szeregowa struktura systemu jednokanałowej transmisji otwartej

2. AKCEPTOWALNY POZIOM RYZYKA JAKO PODSTAWOWE KRYTERIUM BEZPIECZNEJ TRANSMISJI W SYSTEMACH SRK

Norma PN-EN 50159-2 zakłada, że wypadkowa wartość akceptowalnego poziomu ryzyka dla systemu z kanałem transmisji przewodowej lub bezprzewodowej w otwartym kanale transmisji powinna być zgodna z wymaganiami dotyczącymi zapewnienia właściwego poziomu bezpieczeństwa SIL. Dlatego intensywność usterek transmisji należy powiązać z intensywnością uszkodzeń sprzętu oraz oprogramowania. W przypadku sprzętu akceptowalny poziom ryzyka można oszacować na podstawie zależności [4]:

$$THR = \prod_{i=1}^{n} \frac{\lambda_i}{t_{d_i}^{-1}} \cdot \sum_{i=1}^{n} t_{d_i}^{-1} \tag{2}$$

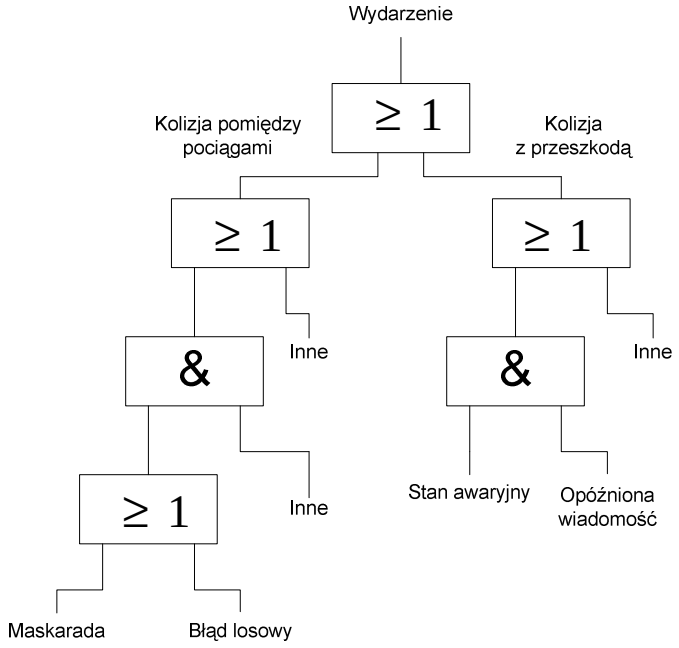
gdzie: λ_i – intensywność uszkodzeń dla kanału i, $t_{d_i}^{-1}$ – czas reakcji systemu na błąd od czasu powstania dla kanału *i.*
Dla systemu, w którym testowanie sprawności odbywa się cyklicznie:

$$t_d = \frac{T}{2} + NT \tag{3}$$

gdzie: T czas cyklicznego testowania wejść/wyjść, NT czas reakcji na błąd wejścia/wyjścia

Analizując zależność (2) widać, że dla systemu, w którym nie zastosowano nadmiarowości wskaźnik THR jest równy intensywności uszkodzeń systemu. Dlatego też w przypadku zastosowania jako medium transmisji bezprzewodowej, należy dodatkowo uwzględnić charakterystyczne wskaźniki dotyczące transmisji, zabezpieczenie czy kodowanie. Ważnym w tym przypadku staje się długość kodu zabezpieczającego, co uwzględniono wcześniej w zależności (1).

W modelowaniu ryzyka systemów srk wykorzystuje się graficzny opis za pomocą drzewa niezdatności i drzewa zdarzeń. Analiza drzewa niezawodności[4] pozwala w sposób usystematyzowany rozpatrywać różnorodne czynniki mające wpływ na niezdatność systemu [5]. W przypadku analizy drzewa zdarzeń[5] analizowana jest możliwość rozwoju zdarzenia inicjującego (określa się bariery bezpieczeństwa i rozpatruje się sekwencje zdarzeń) [6]. Na rys. 3 pokazano przykład drzewa zdarzeń dla systemu srk.



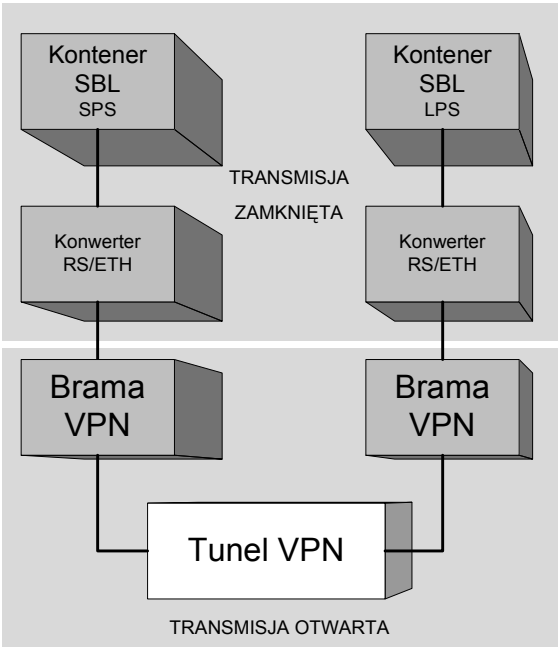
Rys. 3. Przykładowe drzewo zdarzeń systemu srk

3. ANALIZA AKCEPTOWALNEGO POZIOMU RYZYKA NA WYBRANYCH SYSTEMACH TRANSMISJI OTWARTEJ STOSOWANYCH W SYSTEMACH SRK

Przykładowa analiza przeprowadzona została dla systemu transmisji otwartej przeznaczonego do zastosowania w systemie srk o rozproszonej logice. Poniższe analizy prowadzone były dla typowej elektronicznej samoczynnej blokady liniowej eksploatowanej na PKP PLK S.A, w której zastosowano sieć otwartą do wymiany informacji (telegramów) pomiędzy poszczególnymi kontenerami sbl. Oznacza to, iż transmisja przewodowa została

[4] FTA – Fault Tree Analysis
[5] ETA - Event Tree Analysis

zastąpiona transmisją za pośrednictwem standardowych bram VPN[6], co schematycznie przedstawiono na rys. 4.



Rys. 4. Uproszczona struktura transmisji otwartej

Dla zaproponowanej transmisji otwartej przyjęto na podstawie danych producenta typowe wartości MTBF[7] [h]:

- SPS 1(ESP-11) - $2.05*10^4$,
- KONWERTER RS/ETH 1 – $1*10^6$,
- BRAMA VPN (Lynx+L210) - $5.87*10^5$,
- LPS (ESP-11) - $2.05*10^4$,

co daje wartość λ_N równą $1.03*10^{-4}$ (MTBF=9712 [h]).

W przypadku realizacji systemu z transmisją zamkniętą ogólną wartość λ_N jest równą $1.01*10^{-4}$ (MTBF'=9894 [h]). Zakładając, że systemy z transmisją zamkniętą (dopuszczone do eksploatacji w UE i w Polsce) spełniają wymagania norm PN-EN 50129, PN-EN 50128, PN-EN 50159-1 należy uważać że przyjęte rozwiązania systemów z transmisją otwartą opartą o zalecenia normy [2] i normy [3] powinny zapewnić analogiczny poziom bezpieczeństwa. Przyjmując, że poziom niezawodności zarówno dla transmisji zamkniętej

[6] Virtual Private Network

[7] Mean Time Between Failures

jak i otwartej charakteryzowany intensywnością uszkodzeń λ_N jest rzędu 10^{-4}, pozwala to na oszacowanie intensywność uszkodzeń niebezpiecznych:

$$\lambda_{NT} = \lambda_N \cdot 2^{-32} = 10^{-4} \cdot (4 \cdot 10^9)^{-1} = 2{,}5 \cdot 10^{-14} \tag{5}$$

W obu przypadkach dla założonych szeregowych struktur niezawodnościowych układów transmisyjnych, uwzględniając wynik (5) wykazano, iż zarówno dla transmisji przewodowej jak i transmisji z wykorzystaniem sieci otwartych, uzyskane wyniki (dla najbardziej niekorzystnych warunków pracy) dają podstawę do zaliczenia podsystemu transmisji do poziomu SIL 4. Podkreślić należy, iż jest to minimalna intensywność uszkodzeń, a uwzględnienie w praktyce zakłóceń, przerw oraz usterek sprzętu i zaprogramowanych protokołów, może znacznie podwyższyć tę wartość.

Dlatego też, uwzględniając wartość THR dla blokady liniowej na poziomie 10^{-11} [h^{-1}] oraz przyjmując intensywność niebezpiecznych przekłamań na poziomie 1.61 *10^{-16}, przy analogicznej wartości dla systemu transmisji zamkniętej na poziomie 1.29*10^{-16} można założyć, że zaproponowane rozwiązania bezpieczeństwa transmisji otwartej powinny zapewnić ten sam poziom bezpieczeństwa.

Analizując średnie prawdopodobieństwo przebywania w stanie niebezpiecznych uszkodzeń transmisji (zanik, błędne odczytanie) można wykazać, że jest ono zbliżone do wartości otrzymanych dla systemów srk eksploatowanych w kolejnictwie polskim [4]. Przyjmując typowe założenia dla procesów stochastycznych można oszacować to prawdopodobieństwo jako:

$$p_{nb} = \frac{\lambda}{\mu} \cdot p_F \tag{6}$$

gdzie λ jest intensywnością uszkodzeń, μ odwrotnością średniego czasu powrotu po wykryciu uszkodzenia a p_F jest prawdopodobieństwem wystąpienia uszkodzenia krytycznego w stosunku do wszystkich uszkodzeń (przyjmuje się p_F rzędu 10^{-3}, co oznacza, że na 1000 uszkodzeń jedno jest traktowane jako niebezpieczne).

Przyjmując standardowe parametry transmisji (odpowiednie czasy) dla podsystemów transmisji dla różnych systemów srk:

- ssp pomiędzy SSP a UZK:
  maks. czas niedostępności łącza – 16s,
- miedzy punktami sterowania w systemach blokady liniowej:
  maks. czas niedostępności łącza – 2s,
- pomiędzy licznikami osi:
  maks. czas niedostępności łącza – 1s,
- w systemem zależnościowym a sterownikami:
  maks. czas niedostępności łącza – 1s,

dla $\lambda = 10^{-4}$ daje wartości odpowiednio równe: 43.2 $10^{-8}p_F$, 5.4 $10^{-8}p_F$, 2.7 $10^{-8}p_F$, 2.7 $10^{-8}p_F$ (przy sugerowanej wartości p_F rzędu 10^{-3} wszystkie powyższe wartości są zawarte w przedziale $43.2 \cdot 10^{-11} \div 2.7 \cdot 10^{-11}$).

4. WNIOSKI

Dokonane przykładowe analizy i obliczenia potwierdzają wysoki poziom bezpieczeństwa systemów z wymianą danych wykorzystująca standardy otwartych sieci transmisji. Potwierdzają, one właściwy kierunek rozwoju systemów sterowania ruchem kolejowym opartych o zastosowanie technologii bezprzewodowych wymiany danych procesowych, które w przypadku problemów z instalacją sieci przewodowej będą mogły ją zastępować. Implementacja systemów bezprzewodowych, szczególnie w systemach zaliczanych do poziomu bezpieczeństwa SIL4, nie zwalnia producentów od przeprowadzenia odpowiednich udokumentowanych badań. Niezbędna, jak w dotychczasowych systemach, staje się odpowiednia analiza bezpieczeństwa. Szczególną uwagę należy zwrócić na odpowiednie metody kryptograficzne ale również opóźnienia czy przekłamania transmisji.

5. BIBLIOGRAFIA

[1]. Jaźwiński J., Ważyńska – Fiok K.: „Bezpieczeństwo i niezawodność systemu sterowania ruchem kolejowym", Zeszyt 95, WKiŁ Warszawa 1982
[2]. Norma PN-EN 50159 - 2:2002 (U) *Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 2 Łączność systemów bezpiecznych w układach otwartych*.
[3]. Norma PN-EN 50159 - 1:2002 (U) *Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 1 Łączność systemów bezpiecznych w układach zamkniętych*.
[4]. Perzyński T.: „Problemy bezpieczeństwa sieci komputerowych stosowanych w sterowaniu ruchem kolejowym". Rozprawa doktorska, Wydział Transportu i elektrotechniki Politechniki radomskiej, Radom 2009 r.
[5]. PN-IEC 1025:1994 - Analiza drzewa niezdatności (FTA).
[6]. Szopa T.: „Niezawodność i bezpieczeństwo". Oficyna Wydawnicza Politechniki Warszawskiej. Warszawa 2009