PRACE NAUKOWE POLITECHNIKI WARSZAWSKIEJ
z. 96 Transport 2013

Andrzej Lewiński, Tomasz Perzyński, Lucyna Bester

Uniwersytet Technologiczno – Humanistyczny im. Kazimierza Pułaskiego w Radomiu

KOMPUTEROWE WSPOMAGANIE ANALIZY BEZPIECZEŃSTWA W SYSTEMACH STEROWANIA RUCHEM KOLEJOWYM

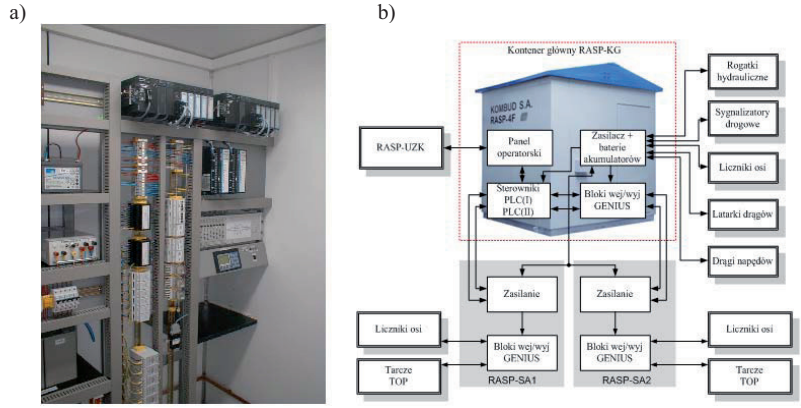
Rękopis dostarczono, marzec 2013

Streszczenie: W pracy przedstawiono komputerowe wspomaganie analizy bezpieczeństwa na każdym etapie życia systemu sterowania ruchem kolejowym: projektowania, testowania i eksploatacji. Dotyczy to szacowania niezawodności systemów nowoprojektowanych, aktualnie produkowanych oraz tych eksploatowanych od co najmniej kilku lat. Pokazano możliwość stosowania komputerowego wspomagania analizy wystąpienia sytuacji krytycznych metodą FTA, szacowanie prawdopodobieństwa takich zdarzeń, czy weryfikację oszacowanych wartości metodą symulacji komputerowej. Artykuł jest podsumowaniem prac naukowo badawczych prowadzonych w Zakładzie Elektroniki i Diagnostyki na Wydziale Transportu i Elektrotechniki UTH w Radomiu
Słowa kluczowe: bezpieczne systemy srk, komputerowe wspomaganie analizy bezpieczeństwa

1. WPROWADZENIE

Przystąpienie Polski do UE w 2005 roku spowodowało obligatoryjne stosowanie norm związanych z projektowaniem, testowaniem, wdrażaniem i utrzymywaniem bezpiecznych systemów automatyki kolejowej. Obowiązujące stały się normy oznaczone odpowiednio: PN-EN 50126 [10], PN-EN 50128 [11], PN-EN 50129 [12] oraz PN-EN 50159 [15]. We wspomnianych normach określono m.in. niezawodność, gotowość, dostępność, bezpieczeństwo [10], procedury i wymagania techniczne dla projektowania oprogramowania bezpiecznego systemu elektronicznego dla sterowania i zabezpieczenia na kolei [11]. Dodatkowo normy definiują wymagania dotyczące projektowania, testowania, odbioru i zatwierdzania elektronicznych systemów, podsystemów i urządzeń sygnalizacji [12] oraz bezpieczną łączność w układach otwartych i zamkniętych [15]. Obecnie podstawowym liczbowym kryterium oceny systemu jest wskaźnik THR (ang. *Tolerable Hazard Rate*) [16]. Określenie liczbowej wartości wskaźnika THR nie jest jedynym sposobem oceny ryzyka systemów srk. Przydatne okazują się inne wskazane w normach metody takie jak analiza za pomocą procesów Markowa, czy analiza drzewa niezdatności (FTA) [7]. Przy analizie bezpieczeństwa bardzo istotna jest symulacja komputerowa (zazwyczaj stosowana jako

metoda weryfikacji parametrów przyjętych w analizie matematycznej). Przedstawiona praca ma pokazać, jak metody obligatoryjne i zalecane standardy UE mogą być wspomagane przez profesjonalne oprogramowanie oraz użyteczne programy opracowane dla konkretnych aplikacji (np. wyznaczenia wypadkowej intensywności uszkodzeń dla złożonych konfiguracji systemów o strukturze szeregowo-równoległej). W pracy oparto się na systemie sygnalizacji przejazdowej typu RASP-4, której producent udostępnił wszystkie wymagane dane do oceny bezpieczeństwa. Jest to typowy system realizowany w strukturze dwukanałowej („2 z 2"), [8], [16], [22].



Rys. 1. Samoczynna sygnalizacja przejazdowa RASP-4 a) zdjęcie układu w kontenerze, b) struktura systemu.

2. SZACOWANIE I WERYFIKACJA WSPÓŁCZYNNIKA THR JAKO METODA ANALIZY BEZPIECZEŃSTWA WYNIKAJĄCA Z OBOWIĄZUJĄCYCH NORM

Koncepcja bezpiecznych systemów komputerowych stosowanych w kolejnictwie zakłada bardzo małą intensywność usterek, co przy całkowitej niezależności kanałów przetwarzania gwarantuje znikome prawdopodobieństwo wystąpienia usterki podwójnej lub wielokrotnej – decydującej o uszkodzeniu katastroficznym (krytycznym). Podstawą analizy jest akceptowalny, dopuszczalny poziom ryzyka określony z zależności (bezpieczeństwo systemu zależy nie tylko od intensywności uszkodzeń, ale od czasu detekcji uszkodzeń pojedynczych i podwójnych), [16]:

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

gdzie: λ_i – intensywność uszkodzeń dla kanału i, $t_{d_i}^{-1}$ – czas reakcji systemu na błąd dla kanału *i.*

Dopuszczalne wartości *THR* dla poziomu bezpieczeństwa SIL-4 zawierają się w przedziale $10^{-9} \leq THR \leq 10^{-8}$. Z bezpieczeństwem systemów srk zakwalifikowanych do poziomu SIL-4 wiąże się również czas diagnostyki usterek pojedynczych:

$$T_{sf} = \frac{k}{1000 \cdot \lambda} \tag{2}$$

oraz usterek podwójnych:

$$T_{2sf} = \frac{2}{\lambda} \tag{3}$$

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.

Jednym z programów służących do prognozowania i szacowania parametrów niezawodnościowych jest program SOBIN [21]. Program ten składa się podstawowych bloków: blok wprowadzania danych oraz blok obliczania parametrów niezawodnościowych. W przypadku stosowania rozwiązań analitycznych dla układu złożonego z elementów pracujących w strukturze szeregowej i przy założeniu wykładniczego charakteru funkcji uszkodzeń, sumuje się wskaźniki intensywności uszkodzeń poszczególnych modułów:

$$\lambda_0 = \lambda_1 + \lambda_2 + ... + \lambda_i = \sum_{i=1}^{n} \lambda_i \tag{4}$$

W przypadku elementów pracujących równolegle, istnieje pewien problem z oszacowaniem w prosty sposób intensywności uszkodzeń dla takiego układu, dlatego też podobną analizę można przeprowadzić w oparciu o wyznaczenie średniego czasu do wystąpienia usterki. Dla n=2 oraz n=3 (typowe nadmiarowości w systemach srk) przedstawia to wzór (5), [16]:

$$T_{MTF_{n=2}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2} = \frac{3}{2\lambda}\bigg|_{\lambda_1=\lambda_2=\lambda}$$

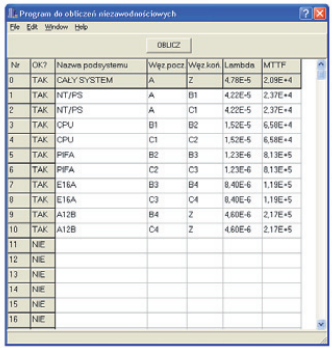
$$T_{MTF_{n=3}} = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \frac{1}{\lambda_3} - \left(\frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_2 + \lambda_3} + \frac{1}{\lambda_1 + \lambda_3} \right) + \frac{1}{\lambda_1 + \lambda_2 + \lambda_3} = \frac{11}{6\lambda}\bigg|_{\lambda_1=\lambda_2=\lambda_3=\lambda} \tag{5}$$

przy czym średni czas do wystąpienia usterki w module *i* jest równy:

$$T_{MTF_i} = \int_0^\infty R_i(t)dt = \int_0^\infty e^{-\lambda_i t}dt = \frac{1}{\lambda_i} \tag{6}$$

Na rys. 2.a przedstawiono okno programu, w którym zdefiniowano strukturę połączeń kanału systemu RASP-4 (w programie SOBIN) oraz tabelę z wykazem elementów składowych.

a)



Nr	OK?	Nazwa podsystemu	Węz.pocz	Węz.koń	Lambda	MTTF
0	TAK	CAŁY SYSTEM	A	Z	4,78E-5	2,09E+4
1	TAK	NT/PS	A	B1	4,22E-5	2,37E+4
2	TAK	NT/PS	A	C1	4,22E-5	2,37E+4
3	TAK	CPU	B1	B2	1,52E-5	6,58E+4
4	TAK	CPU	C1	C2	1,52E-5	6,58E+4
5	TAK	PIFA	B2	B3	1,23E-6	8,13E+5
6	TAK	PIFA	C2	C3	1,23E-6	8,13E+5
7	TAK	E16A	B3	B4	8,40E-6	1,19E+5
8	TAK	E16A	C3	C4	8,40E-6	1,19E+5
9	TAK	A12B	B4	Z	4,60E-6	2,17E+5
10	TAK	A12B	C4	Z	4,60E-6	2,17E+5
11	NIE					
12	NIE					
13	NIE					
14	NIE					
15	NIE					
16	NIE					

b)

ELEMENT	ILOŚĆ	ŚREDNIA WARTOŚĆ
Układy scalone VSI	11	1,20E-06
Układy scalone MSI	27	2,94E-06
Układy scalone LSI	12	1,31E-06
Kwarc	5	2,50E-06
Kondensator elektrolityczny	17	1,70E-06
Inne kondensatory	209	2,11E-05
Cewki	75	4,31E-06
Rezystory	378	4,35E-06
Tranzystory	9	1,75E-06
Diody	4	1,42E-07
LEDy	3	3,63E-07
	SUMA	4,16E-05

Rys. 2. Okno programu wspomagającego wyznaczanie wypadkowej intensywności uszkodzeń a) okno programu, b) tabela z wykazem elementów.

2.1. SZACOWANIE THR NA PODSTAWIE DANYCH PRODUCENTA

Dla zastosowanego sprzętu systemu RASP-4 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:

- zestaw z 2 modułami e) i 1 modułem f) – 144 374.4267 [h],
- zestaw z 3 modułami e) i 1 modułem f) – 141 185.9945 [h],
- zestaw z 4 modułami e) i 1 modułem f) – 138 135.3490 [h],
- 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 cyklicznego testowania wejść/wyjść T równy

250ms oraz czas reakcji na błąd (NT) 1s) co daje wartość czasu reakcji na błąd (SDT) równą 0.0003125 [h] i w efekcie wartość THR równą 2.19e-13, zgodną z normą PN-EN 50129 dla poziomu SIL-4.

2.2. PROGNOZOWANIE JAKO METODA SZACOWANIA NIEZAWODNOŚCI NOWYCH SYSTEMÓW

W przypadku analizy systemu o nieznanych charakterystykach niezawodnościowych elementów, możliwe jest wstępne oszacowanie wskaźników poprzez obliczenie wypadkowych intensywności uszkodzeń systemu na podstawie ilości i struktury niezawodnościowej zastosowanych elementów dyskretnych oraz scalonych o różnej skali integracji. Ogólna postać dla szacowania niezawodności eksploatacyjnej dyskretnych elementów półprzewodnikowych wynosi [8], [9], [16]:

$$\lambda_p = \lambda_b \left(\pi_T \cdot \pi_A \cdot \pi_R \cdot \pi_S \cdot \pi_C \cdot \pi_Q \cdot \pi_E \right) \tag{7}$$

gdzie:

- $\lambda_b = \lambda_0 \cdot \pi_{ST}$ - bazowa intensywność uszkodzeń, zależna od parametru λ_0 oraz obciążenia temperaturowego i elektrycznego π_{ST},
- λ_p - intensywność uszkodzeń podczas eksploatacji,
- π_E - współczynnik uwzględniający oddziaływanie czynników środowiskowych innych niż temperatura,
- π_A - współczynnik uwzględniający rodzaj aplikacji,
- π_S - współczynnik uwzględniający obciążenia napięciowe,
- π_T - współczynnik temperaturowy,
- π_R - współczynnik uwzględniający maksymalne dopuszczalne parametry elementu,
- π_Q - współczynnik jakościowy,
- π_C - współczynnik uwzględniający wpływ obecności kilku złącz w jednej obudowie lub konstrukcje elementu.

Na podstawie otrzymanej dokumentacji technicznej dokonano wstępnego studium analizy bezpieczeństwa w celu wyznaczenia wskaźnika intensywności uszkodzeń λ oraz wyznaczenia współczynnika THR. Wyniki z szacowania są następujące:

- sterownik czujników i tarcz – λ =8,8E-05,
- sterownik radiowy 1– λ = 4,09558E-05,
- sterownik radiowy 2 – λ = 1,50242E-05,
- układ decyzyjny – λ = 2,54E-04.

Wypadkowy wynik: λ=3,98E-04, co przy t_d rzędu 1,25s zapewnia THR równy $1.1*10^{-10}$.

2.3. SZACOWANIE THR NA PODSTAWIE DANYCH EKSPLOATACYJNYCH

Na podstawie danych eksploatacyjnych możliwe było oszacowanie wartości intensywności uszkodzeń. Jednym ze sposobów weryfikacji założonej hipotezy intensywności uszkodzeń są testy zgodności. W artykule posłużono się testem $\chi 2$ Pearsona [16], który jest testem weryfikacji nieparametrycznej dotyczącej postaci funkcyjnej dystrybuanty cechy populacji. Test ten stosowany jest w przypadku, gdy n - krotnie powtarzane doświadczenie może dać k różne wyniki. Statystyka ta wyraża się wzorem:

$$\chi^2_{emp} = \sum_{i=1}^{k} \frac{(n_i - n_i^t)^2}{n_i^t} \tag{8}$$

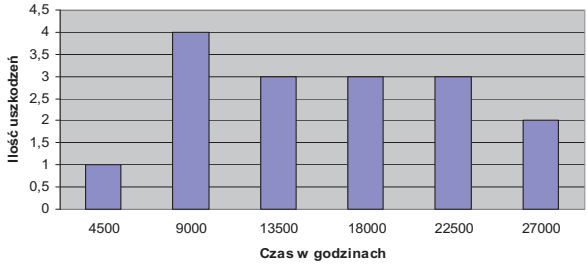
gdzie $n_i^t = N \cdot p_i^t$, $N = \sum_{i=1}^{k} n_i$, $p_i^t = P_F$ {X przyjęta wartość klasy i}.

Jeżeli $\chi^2_{emp} > \chi^2(\alpha; k-r-1)$, to założoną hipotezę H0 odrzucamy, (r – liczba nieznanych parametrów hipotetycznego rozkładu F). W tabeli 1 pokazano opis statystyki, a na rys. 3 wykaz uszkodzeń dla badanych systemów typu RASP-4 w założonym przedziale czasu 27000 godzin (każdy przedział po 4500h). Razem zarejestrowano 16 usterek, [16].

Tablica 1

Opis statystyki

KLASA	LICZEBNOŚĆ
$(-\infty, x_1)$	n_1
$\langle x_1, x_2)$	n_2
⋮	⋮
$\langle x_{k-2}, x_{k-1})$	n_{k-1}
$\langle x_{k-1}, \infty)$	n_k

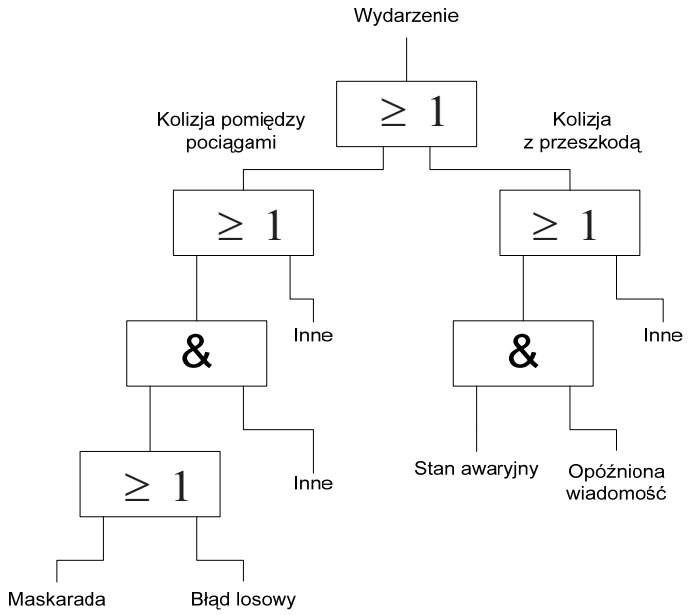


Rys. 3. Szacowanie intensywności uszkodzeń na podstawie badań eksploatacyjnych, wykaz uszkodzeń w przedziałach czasu

Do oszacowania wartości współczynnika uszkodzeń λ zastosowano program Statistica [19]. Ponieważ nie odrzucono hipotezy o odrzuceniu przyjętych założeń dla rozkładu wykładniczego, oszacowana wartość λ wyniosła $7.40741*10^{-5}h^{-1}$. Do obliczenia współczynnika THR użyto wcześniejszych danych (czas cyklicznego testowania wejść/wyjść T = 500ms, czas reakcji na błąd wejścia NTwe = 1s, czas reakcji na błąd wyjścia NTwy = 1s) co dla jednakowych kanałów dało wskaźnik THR równy: $5,56\ 10^{-12}$.

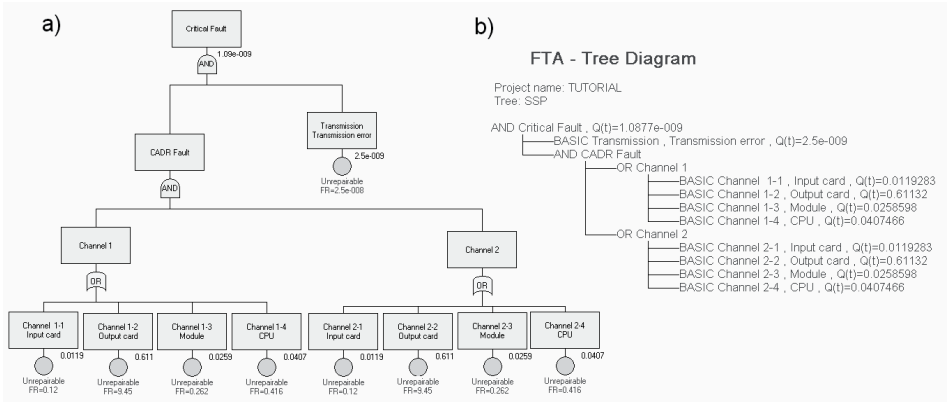
3. ANALIZA FTA

W modelowaniu ryzyka systemów srk wykorzystuje się graficzny opis za pomocą drzewa niezdatności i drzewa zdarzeń. Analiza drzewa niezawodności pozwala w sposób usystematyzowany rozpatrywać różnorodne czynniki mające wpływ na niezdatność systemu. W przypadku analizy drzewa zdarzeń analizowana jest możliwość rozwoju zdarzenia inicjującego (określa się bariery bezpieczeństwa i rozpatruje się sekwencje zdarzeń) [11]. Na rys. 4 pokazano przykład drzewa zdarzeń dla systemu srk [11].



Rys. 4. Przykładowe drzewo zdarzeń systemu srk

Do analizy bezpieczeństwa metodą FTA [14] zastosowano oprogramowanie firmy RAM Commander - ALD Company [17] (wersja demonstracyjna), która pokazuje propagację zdarzenia (Critical Fault) w przedstawionym systemie transmisji otwartej (rys. 5).



Rys. 5. Drzewo FTA dla systemu ssp typu RASP-4 a) okno analizy, b) raport analizy

Do analizy założono następujące wartości intensywności uszkodzeń oszacowane w wyniku prognozowania:

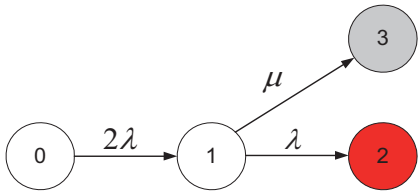
- karta wej. 1.21e-05,
- karta wyj. 9,45e-06,
- CPU 4.16e-05,
- moduł interfejsu 2.62e-05,
- błąd transmisji oszacowano na podstawie [8]:

$$\lambda_{NT} = \lambda_N \cdot p_{UE} = \lambda_N \cdot 2^{-32} \tag{9}$$

Przykładowy raport pokazano na rys. 5b. Dla takiego drzewa i założonych parametrów, Q (t) wynosi 1.09e-10 (dla czasu analizy 100 000h).

4. PROCESY MARKOWA ORAZ PARAMETRY PROBABILISTYCZNE I CZASOWE WYKORZYSTYWANE W ANALIZIE BEZPIECZEŃSTWA

System ssp jest systemem bezpiecznym, co oznacza, że każde pojedyncze uszkodzenie powinno być wykryte w odpowiednio krótkim czasie, system powinien zainicjować reakcje bezpieczeństwa a wykryte pojedyncze uszkodzenie nie może prowadzić do sytuacji niebezpiecznej. Dlatego też, procesy stochastyczne w postaci procesów Markowa są dogodną metodą do analizy systemów sterowania ruchem na przejazdach kolejowych, gdzie wymienione procesy stochastyczne charakteryzują systemy bez odnowy.



Rys. 6. Model systemu sygnalizacji przejazdowej, systemu bez odnowy

Model systemu ssp przedstawia system pracy dwóch komputerów pracujących równolegle, poszczególne stany modelu opisują następujące sytuacje:

- Stan 0 - stan poprawnej pracy, dwa komputery pracują,
- Stan 1 - system wykrył uszkodzenie jednego z komputerów,
- Stan 2 - stan uszkodzenia niebezpiecznego, uszkodzone dwa komputery, brak reakcji bezpieczeństwa,
- Stan 3 (stan uszkodzenia kontrolowanego) - system wykrył uszkodzenie i rozpoczął reakcję bezpieczeństwa.

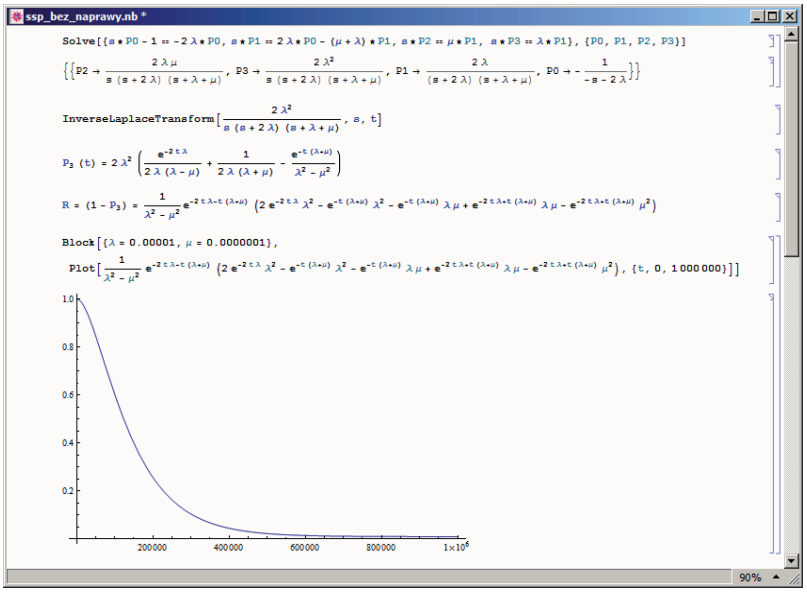
Celem analizy modelu matematycznego badanego systemu jest określenie prawdopodobieństwa wystąpienia sytuacji niebezpiecznej oraz czasu do wystąpienia takiego stanu. W tym celu skorzystano z programu matematycznego Mathematica firmy Wolfram Research Inc., ponieważ jest wszechstronnym programem do realizacji obliczeń symbolicznych i numerycznych z dowolną dokładnością, umożliwia również wizualizację otrzymanych wyników. Okno programu MATHEMATICA dla modelu z rys. 6 pokazano na rys.7 [16], [17]. Rozwiązując odpowiedni układ równań oraz korzystając z odwrotnej transformaty Laplace'a, otrzymano:

$$P2(t) = \frac{\lambda\left(\left(1 + e^{-2t\lambda} - 2e^{-t(\lambda+\mu)}\right)\lambda + \left(-1 + e^{-2t\lambda}\right)\mu\right)}{\lambda^2 - \mu^2} \tag{10}$$

Przyjmując typowe współczynniki λ=0,00001h^{-1} oraz μ=1h^{-1} [16], przebieg funkcji przedstawiającej bezpieczeństwo systemu ssp B =1– P2(t) przedstawiono na rys. 7.

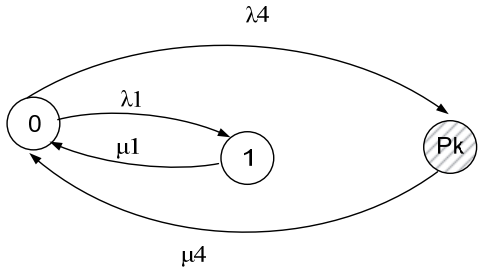
Za pomocą programu Mathematica, stosując transformaty Laplace'a, można wyznaczyć graniczne prawdopodobieństwa przebywania w poszczególnych stanach systemu przy założonym czasie działania systemu t→∞, w tym w najbardziej interesującym stanie P2.

$$P2(t) = \frac{\lambda}{\lambda + \mu} \tag{11}$$



Rys. 7. Okno programu Mathematica dla modelu z rys. 6

Kolejnym bardzo interesującym zagadnieniem jest wyznaczenie prawdopodobieństwa wystąpienia kolizji na przejeździe kat. C (przejazd z sygnalizacją ostrzegającą kierowców bez zapór). Model tego przejazdu jest przedstawiony na rysunku 8 [1], [5].



Rys. 8. Model bezpieczeństwa przejazdu kolejowego kat. C wyposażonego w sygnalizację świetlną

W przedstawionym modelu poszczególne stany opisują sytuacje:
Stan 0 – stan, w którym nie ma zagrożenia

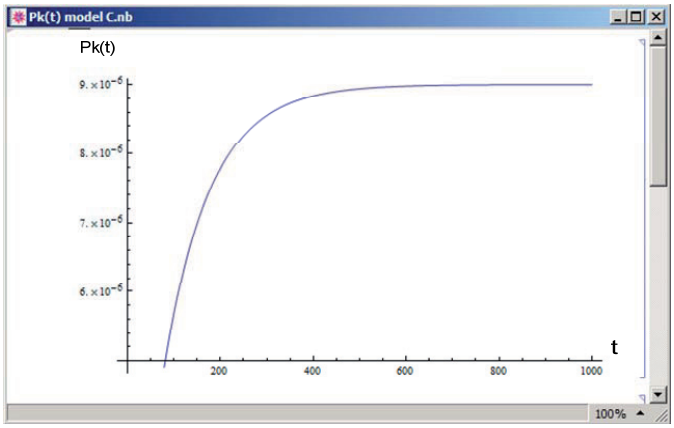
- pojawił się pociąg i nie pojawił się samochód,
- pojawił się samochód i nie pojawił się pociąg,

Stan 1 – kierowca zatrzymał się przed przejazdem, system ssp został załączony,
Stan P_k – Stan katastroficzny, kierowca wjechał pod nadjeżdżający pociąg, awaria systemu ssp.

Przejścia pomiędzy poszczególnymi stanami określają:

- λ_1, λ_4 – intensywności przejścia do stanu 1 i P_k
- μ_1, μ_4 – intensywność powrotu do stanu bez zagrożenia „0".

Graniczne prawdopodobieństwo przebywania w stanie P_k przy $t \to \infty$ pokazano na rys. 9.



Rys. 9. Przebieg zmian prawdopodobieństwa stanu niebezpiecznego P_k

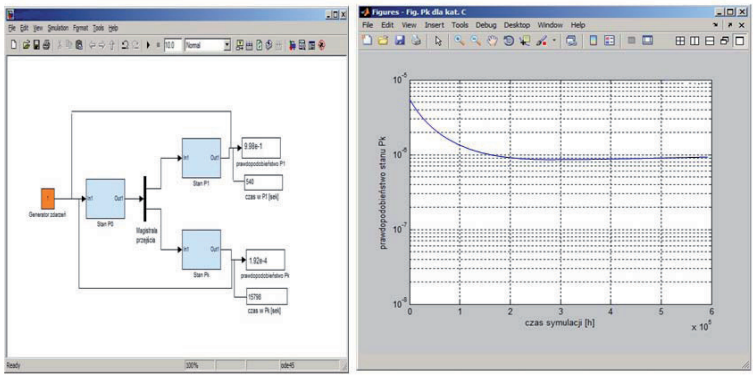
Zakładając wartości parametrów λ_1=0,000000079 [h^{-1}], λ_4=0,0000015 [h^{-1}] i μ_1=0,0016 [h^1], μ_4=0,3 [h^{-1}], prawdopodobieństwo wystąpienia stanu katastroficznego $P_k = 4.98*10^{-6}$. Jest to wartość graniczna, która jest miarą jakości systemu:

$$P_k(t)\,|_{t\to\infty} = \frac{(\lambda_1 + \mu_1)\mu_4}{\lambda_4\mu_1 + (\lambda_1 + \mu_1)\mu_4} \tag{12}$$

5. SYMULACYJNA ANALIZA BEZPIECZEŃSTWA

Z punktu widzenia bezpieczeństwa istotna jest weryfikacja modeli systemów automatyki kolejowej, a zwłaszcza parametrów przyjętych w tych modelach. W rozdziale 2.3 pokazano weryfikację parametrów niezawodnościowych (λ) na podstawie wyników badań eksploatacyjnych w oparciu o typowe metody statystyki. Dla systemów nowoprojektowanych oraz dla systemów gdy brak jest takich badań, jedyną metodą weryfikacji przyjętego modelu jest symulacja komputerowa Na rys. 10 przedstawiono okno programu z modelem symulacyjnym (z rys. 8) przejazdu kolejowego kat. C. Do symulacji zastosowano pakiet MATLAB/SIMULINK (z modułem SimEvents), [1], [5], [18].

a) b)



Rys. 10. Symulacja przejazdu kat. C
a) struktura modelu symulacyjnego w SimEvents, b) przebieg funkcji prawdopodobieństwa stanu P_k w funkcji czasu symulacji.

W wyniku symulacji otrzymano następującą graniczną wartość prawdopodobieństwa wystąpienia stanu katastroficznego P_k, które wynosi $P_k = 1{,}42*10^{-6}$, co okazało się zgodne z wynikiem uzyskanym drogą analizy matematycznej tego modelu [5].

6. PODSUMOWANIE

W pracy pokazano nowoczesne, komputerowo wspomagane metody analizy bezpieczeństwa systemów sterowania ruchem kolejowym. Metody te mogą być obligatoryjne, jak ma to miejsce w przypadku THR i FTA, lub szczególnie zalecane tak jak procesy Markowa czy symulacje komputerowe. Przedstawione oprogramowanie oprócz konkretnych wyników umożliwia też wygenerowanie odpowiedniej dokumentacji potwierdzającej przyjęte założenia funkcjonalne, przede wszystkim parametry niezawodnościowe. W pracy pokazano analizę jednego z wielu systemów ssp [2], [3]. Uzyskane dane potwierdziły zarówno wysoką niezawodność sprzętu jak też odpowiedni poziom bezpieczeństwa (SIL-4) przewidziany dla tego typu urządzeń.

Bibliografia

1. Bester L. „Analiza zintegrowanego systemu bezpieczeństwa w transporcie lądowym na przykładzie przejazdów kolejowych” Rozprawa doktorska, Wydział Transportu i Elektrotechniki Politechniki Radomskiej, Radom 2012
2. Dyduch J., Kornaszewski M.: „Problemy bezpieczeństwa samoczynnych sygnalizacji przejazdowych stosowanych na PKP”, Transport Zeszyt 11 WPR Radom 2000

3. Dyduch J., Kornaszewski M.: „Systemy sterowania ruchem kolejowym", Wydawnictwo Politechniki Radomskiej, Radom 2003.
4. Lewiński A., Bester L.: "The dependability and safety of new wireless systems in railway control and management" ADVANCES IN TRANSPORT SYSTEMS TELEMATICS – 2007 (monograph), Katowice – Ustroń 2007.
5. Lewiński A., Bester L: "Additional warning system for cross level". Communications in Computer and information Sience (104), Springer-Verlag Berlin Heidelberg 2010.
6. Lewiński A., Perzyński T. „Modelowanie bezpiecznych systemów w sterowaniu ruchem kolejowym", Materiały Konferencji Naukowej TRANSCOMP 2005, Zakopane 2005
7. 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.
8. 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.
9. Military Hand Book, Reliability Prediction of Electronic Equipment, USA Department of Defense (1991).
10. 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.
11. Norma PN-EN 50128:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Oprogramowanie dla kolejowych systemów sterowania i zabezpieczenia.
12. Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.
13. Norma PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów. Porcedura analizy rodzajów i skutków uszkodzeń (FMEA),
14. Norma PN-EN 61025:2007 Analiza drzewa niezdatności (FTA),
15. Norma PN-EN 50159: 2010. Zastosowania kolejowe. Systemy łączności, sterowania ruchem i przetwarzania danych -- Łączność bezpieczna w systemach transmisyjnych.
16. Perzyński T.: „Problemy bezpieczeństwa sieci komputerowych stosowanych w sterowaniu ruchem kolejowym". Rozprawa doktorska, Wydział Transportu i Elektrotechniki Politechniki Radomskiej, Radom 2009.
17. Wolfram S.: „Mathematica", version 4, Wolfram Media – Cambridge University Press 1999.
18. Oprogramowanie MATLAB/SIMULINK.
19. Oprogramowanie STATISTICA.
20. Oprogramowanie RAM Commander - ALD Company.
21. Program do szacowania THR (SNOS-SOBIN).
22. Materiały firmy KOMBUD S.A. w Radomiu.

COMPUTER AIDED SAFETY ANALYSIS OF RAILWAY CONTROL SYSTEMS

Summary: The paper deals with computer support of safety analysis of railway control system corresponding to each stage of its life cycle, especially design, testing and maintenance. It is related to the reliability estimation of actually designed, manufactured or exploited from several years railway control systems. But is possible to analyze with computer support the occurrence of critical situations using FTA method, estimation of probability connected with such situations and verification of obtained results using simulation methods. The paper is final report of research works realized in Electronics&Diagnostics Department in Faculty of Transport and Electrical Engineering UTH in Radom.
K**eywords:** safety of railway systems, computer analysis of safety