Metody zapewnienia bezpieczeństwa systemów automatyki kolejowej na przykładzie licznika osi UniAC1

Wojciech Ulatowski[1]

Streszczenie
W artykule przedstawiono metody zapewniające spełnienie najwyższego poziomu nienaruszalności bezpieczeństwa (SIL4) w urządzeniach sterowania ruchem kolejowym. Opisano rozwiązania sprzętowe i programowe zaimplementowane w systemie liczenia osi UniAC1 firmy mającej certyfikat SIL4, w tym dotyczące komunikacji bezpiecznej. Opisano również analizę bezpieczeństwa przeprowadzoną metodą grafów Markowa i zaprezentowano wyniki dla systemu UniAC1.

Słowa kluczowe: bezpieczeństwo, bezpieczeństwo na kolei, system liczenia osi, sterowanie ruchem kolejowym, automatyka kolejowa

1. Wprowadzenie

Pierwszy system projektowany zgodnie z wymaganiami norm bezpieczeństwa kolejowego CENELEC zaczął powstawać w 2002 roku. System o nazwie SARPO przeznaczono do sterowania rozrządem w strefie torów docelowych górki rozrządowej. W wyniku przeprowadzonej analizy zagrożeń dla systemu SARPO, zdefiniowano jako wymagany drugi poziom nienaruszalności bezpieczeństwa (SIL2).

Od tego czasu opracowano i wdrożono wiele nowatorskich rozwiązań w zakresie bezpieczeństwa, z których część zaimplementowano w systemie liczenia osi UniAC1. System UniAC1 charakteryzuje się czwartym poziomem nienaruszalności bezpieczeństwa SIL. Wszystkie moduły systemu, w tym głowica torowa UniAS1, opracowano i wdrożono zarówno w obszarze sprzętu, jak i oprogramowania.

2. Rozwiązania zapewniające najwyższy poziom bezpieczeństwa

W systemie liczenia osi UniAC1 zastosowano zdywersyfikowaną architekturę dwa z dwóch wraz z następującymi metodami zapewniającymi bezpieczeństwo:
1) zróżnicowanie jednostek centralnych w dwóch kanałach przetwarzających dane,
2) fizyczna niezależność między kanałami,
3) zróżnicowanie zestawu układów elektronicznych,
4) zdywersyfikowanie oprogramowania,
5) skrośna ocena sygnałów wyjściowych pomiędzy kanałami.

2.1. Rozwiązania sprzętowe

Każdy z modułów wykonanych w różnych technologiach przetwarzających dane, wchodzących w skład systemu, zawiera dwa niezależne kanały realizujące taką samą funkcjonalność:
- kanał 1 – układ PLD (układ elektroniczny o programowalnej strukturze) wspierany mikrokontrolerem 8-bitowym,
- kanał 2 – mikrokontroler 16-bitowy.

Zróżnicowana architektura kanałów minimalizuje prawdopodobieństwo wystąpienia okoliczności powstania zagrożenia w wyniku uszkodzenia się elementu lub podsystemu.

Drugą istotną cechą stosowanej architektury jest skrośna ocena sygnałów wyjściowych przez oba kanały. Wyjścia z obu kanałów są przesyłane do drugiego kanału w celu porównania.

Inną stosowaną metodą jest weryfikacja pracy każdego z układów programowych (mikroprocesorów oraz układów PLD) przez pozostałe układy. Realizowane jest to przez sygnał *heartbeat*, który w zdefiniowanej jednostce czasu musi zmienić swój stan na przeciwny określoną liczbę razy. Jeżeli liczba ta jest za duża lub za mała, każdy z kanałów jest w stanie wprowadzić podejrzany kanał w stan bezpieczny przez oddziaływanie bezpośrednio na jego wyjścia sprzętowe (np. przepalenie bezpiecznika i wyłączenie napięcia zasilania cewki przekaźnika).

W obszarze rozwiązań sprzętowych dodatkowo zastosowano następujące metody zapewniające bezpieczeństwo:

[1] Dr inż.; voestalpine TENS Sp. z o.o.; Sopot; e-mail: wojciech.ulatowski@tens.pl.

1) separacja kanałów,
2) separowane zasilacze dla każdego z kanałów,
3) brak powiązań funkcjonalnych, które umożliwią jednemu kanałowi zmianę stanu drugiego,
4) porównywanie konfiguracji swojego kanału oraz kanału drugiego.

Podsumowując, w celu zapewnienia czwartego poziomu nienaruszalności bezpieczeństwa w systemie UniAC1, zastosowano podwójne struktury elektroniczne ze złożonym *fail-safety* z bezpieczną komparacją. Oznacza to, że działają one na zasadzie „bezpieczny w razie uszkodzenia". Skutki usterek fizycznych oraz defekty w oprogramowaniu lub zakłócenia rozprzestrzeniają się na wyjście, a każda rozbieżność między wyjściami dwóch kanałów jest wykryta w wyniku porównania skrośnego. Na wyjściach będzie ustawiony stan bezpieczny.

2.2. Rozwiązania programowe

Urządzenia oraz systemy sterowania ruchem kolejowym przetwarzają informacje dwukanałowo. Do ich poprawnej pracy potrzebna jest prawidłowa i zgodna w czasie praca obu kanałów. Stosowanie w obu kanałach różnych technologii przetwarzania danych wymusza użycie różnych narzędzi programowych do opracowania oprogramowania aplikacyjnego. Takie rozwiązanie zmniejsza prawdopodobieństwo wystąpienia błędów systematycznych, ponieważ zarówno na etapie projektowania, jak i kompilacji lub wgrywania programu do pamięci układu są stosowane inne narzędzia. Błąd narzędzia oraz błąd mogący ujawnić się w jednej technologii nie przenosi się na drugi kanał. Stosowanie dwóch takich samych technologii (np. mikroprocesorów), nawet od różnych producentów, nie zapewnia takiej pewności zabezpieczenia przed błędami systematycznymi.

Oprócz różnorodnych technologii, drugą metodą zapewaniającą najwyższy poziom bezpieczeństwa jest odpowiednia wymiana informacji pomiędzy kanałami. W systemie UniAC1 zastosowano wymianę:
- sygnałów „życia" *heartbeat* – kontrola działania pętli głównej,
- sygnałów wyjściowych będących skutkiem przetwarzania informacji w każdym z kanałów.

Cykliczne odczytywanie wyjść drugiego kanału i porównywanie ich z aktualnym stanem swoich wyjść, pozwala zminimalizować prawdopodobieństwo błędnego zadziałania jednego z kanałów. W przypadku negatywnego wyniku porównania (niezgodności) zostaje wygenerowana informacja o błędzie i system przechodzi w stan bezpieczny.

W obszarze rozwiązań programowych zastosowano dodatkowo metody zapewniające bezpieczeństwo:
- cykliczne sprawdzanie sumy kontrolnej programu,
- mechanizmy autotestowania wykrywające i sygnalizujące ewentualne uszkodzenia i niesprawności w działaniu urządzeń.

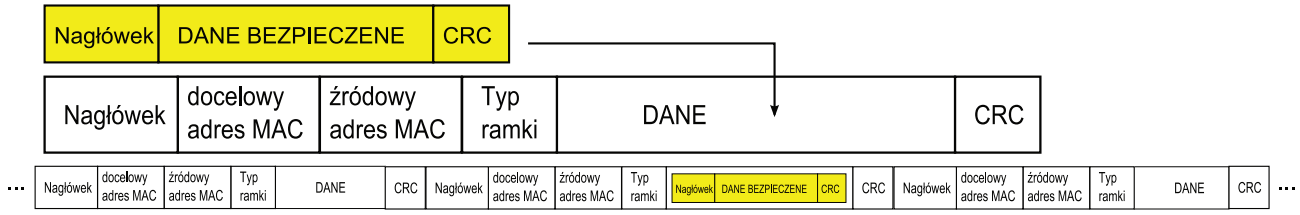
2.3. Transmisja danych

Transmisja danych w systemach związanych z bezpieczeństwem obejmuje przesyłanie danych:
- bezpiecznych – wpływających na bezpieczeństwo,
- pozostałych – nieistotnych z punktu widzenia bezpieczeństwa.

Ramki z danymi bezpiecznymi są krytyczne i są przesyłane z najwyższym priorytetem. Monitorowany jest czas ich dostarczenia do odbiornika. Protokół transmisji modułu komunikacji opracowano na podstawie protokołu ARQ (*Automatic Repeat reQuest*). Protokół ARQ bazuje na potwierdzaniu poprawności lub niepoprawności danych otrzymanych przez odbiornik lub w przypadku braku potwierdzenia na automatycznej retransmisji przez nadajnik ostatnio wysłanej ramki. Retransmisja wymaga zmiany nagłówka ramki tak, aby retransmitowana ramka była odróżniona przez odbiornik. Ramki z danymi nieistotnymi są przesyłane do odbiornika gdy jest wolna linia transmisyjna. Ramkę transmisyjną pokazano na rysunku 1.

3. Analiza bezpieczeństwa

Analiza oddziaływania uszkodzeń na pracę systemu związanego z bezpieczeństwem ma na celu wykazanie, że przypadkowe uszkodzenia sprzętu nie powodują sytuacji niebezpiecznych. W takich przypadkach system musi przejść do zdefiniowanego stanu bezpiecznego, w którym musi pozostawać. Podczas opracowywania



Rys. 1. Ramka transmisyjna

systemu liczenia osi UniAC1 zastosowano wzajemnie uzupełniające się metody analizy bezpieczeństwa:
1) analiza ryzyka HazOp – wykorzystywana do identyfikacji potencjalnych zagrożeń występujących w systemie,
2) analiza drzewa defektów FTA – wykorzystywana w celu odnalezienia elementów, których uszkodzenie może być niebezpieczne; celem metody jest wykrycie potencjalnych hazardów i defektów wynikających z odchyleń od zamierzeń projektowych,
3) analiza uszkodzeń o wspólnej przyczynie CCF,
4) grafy Markowa – wykorzystywane w celu potwierdzenia poziomu intensywności uszkodzeń, przy którym jest możliwy do osiągnięcia wymagany poziom nienaruszalności bezpieczeństwa.

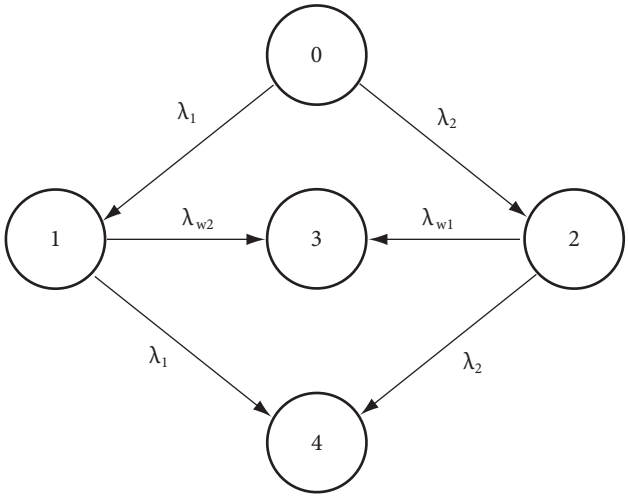
Dodatkowo zastosowano zasadę polegającą na przeprowadzaniu analiz bezpieczeństwa w dwóch etapach:
1) pierwszy etap – oceniający założenia projektowe wraz z akceptacją lub rekomendacją zmian,
2) drugi etap – ocena przyjętych zabezpieczeń oraz ocena ryzyka.

Wymienione metody HazOp, FTA oraz diagramy Markowa są wysoko rekomendowane przez normę EN-50129.

3.1. Grafy Markowa

Ze względu na fakt, że struktura systemu jest dwukanałowa i zdywersyfikowana, nie można było zastosować tradycyjnych wzorów dla struktur *k* z *n*. W wielu publikacjach z zakresu analizy bezpieczeństwa można znaleźć sposoby obliczania współczynników PFH lub THD dla struktur dwukanałowych, ale przy założeniu, że kanały są jednakowe. Ze względu na dywersyfikację, THD obliczono według grafu Markowa.

Ocenę ilościową zawodności bezpieczeństwa działania systemu liczenia osi UniAC1, mogącego znajdować się w kilku stanach, wykonano za pomocą modelu niezawodności bezpieczeństwa według Markowa (rys. 2). Założono, że wszystkie części składowe systemu mają stałe w czasie intensywności uszkodzeń λ_i. Na rysunku 2 przyjęto następujące oznaczenia:
0 – stan zdatności systemu,
1 – uszkodzony pierwszy kanał przetwarzający,
2 – uszkodzony drugi kanał przetwarzający,
3 – stan bezpieczny (system wyłączony – co najmniej jeden przekaźnik torowy odwzbudzony),
4 – stan niebezpieczny (oba przekaźniki torowe wzbudzone),
λ_1 – intensywność uszkodzeń pierwszego kanału przetwarzającego,
λ_2 – intensywność uszkodzeń drugiego kanału przetwarzającego,
λ_{w1} – intensywność wyłączeń systemu przez nieuszkodzony pierwszy kanał przetwarzający,
λ_{w2} – intensywność wyłączeń systemu przez nieuszkodzony drugi kanał przetwarzający.



Rys. 2. Graf bezpieczeństwa systemu UniAC1

Model grafów Markowa niezawodności bezpieczeństwa opisuje następujące fakty:
1. Moduły są nienaprawialne. Nie występuje naprawa lecz wymiana uszkodzonego modułu na sprawny.
2. Uszkodzenie któregokolwiek kanału (1 lub 2) prowadzi do stanu bezpiecznego (3). Złożenie uszkodzeń w dwóch kanałach może prowadzić do stanu niebezpiecznego (4).
3. Do stanu bezpiecznego prowadzi wyłączenie przez pierwszy lub drugi kanał przetwarzający. Warunkiem jest sprawny pierwszy lub drugi kanał przetwarzający.
4. Brak wyjścia ze stanu bezpiecznego – stan bezpieczny jest trwały.
5. Brak przejścia ze stanu uszkodzenia (1, 2) do stanu zdatności systemu (0) – urządzenie nie naprawia się samoczynnie.
6. Brak przejścia ze stanu bezpiecznego do stanu niebezpiecznego.

W tablicy 1 zestawiono wyniki obliczeń prawdopodobieństwa P4, któremu odpowiada wymagany w normie poziom THR.

Tablica 1

Obliczenia THR (P4)

Typ modułu	Nazwa modułu	λ1	λ2	P4 = THR
UniAS1	Głowica torowa	1,35E-06	1,35E-06	4,86E-11
ASM	Moduł wartościujący	7,64E-07	9,76E-07	3,08E-11
ACM	Moduł liczący osie	3,74E-07	4,54E-07	1,47E-11
AIM	Moduł interfejsów	2,30E-06	3,24E-06	9,67E-11

4. Podsumowanie

Zastosowane rozwiązania w systemie liczenia osi UniAC1 spełniają wymagania bezpieczeństwa na poziomie SIL4. Struktura systemu, oparta na dwukanałowym przetwarzaniu na poziomie sprzętu z bezpiecznymi komparatorami sygnałów sterujących oraz monitorowaniem skrośnym sygnałów wyjściowych, zapewnia najwyższy poziom nienaruszalności bezpieczeństwa SIL4 przewidziany dla urządzeń i systemów sterowania ruchem kolejowym.

Należy podkreślić istotne zróżnicowanie kanałów. W jednym z kanałów przetwarzanie jest realizowane na mikrokontrolerze, w drugim zaś na układzie programowalnym PLD. Pociąga to za sobą również zróżnicowanie oprogramowania oraz narzędzi programowych.

Literatura

1. PN-EN 50126:2002: Zastosowania kolejowe – Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (oryg.)
2. PN-EN 50126:2002/AC:2006: Zastosowania kolejowe – Specyfikowanie i wykazywanie Nieuszkadzalności, Gotowości, Obsługiwalności i Bezpieczeństwa (RAMS) – Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia (oryg.).
3. PN-EN 50126:2002/AC:2011: Zastosowania kolejowe – Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (oryg.).
4. PKN-CLC/TR 50126-2:2007: Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for safety (oryg.).
5. PN-EN 50128:2011: Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Oprogramowanie kolejowych systemów sterowania i zabezpieczenia (oryg.).
6. PN-EN 50129:2007: Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem.
7. PN-EN 50129:2007/AC:2010: Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem.
8. PN-EN 50159:2011: Zastosowania kolejowe – Systemy łączności, sterowania ruchem i przetwarzania danych – Łączność bezpieczna w systemach transmisyjnych (oryg.).
9. PN-EN 61025:2007: Analiza drzewa niezdatności (FTA) (oryg.).

Methods of Providing Safety for the Interlocking Systems on the Example of Axle Counter System UniAC1

Summary

The paper presents methods providing fulfillment of the top-level Safety Integrity Level (SIL4) for the railway interlocking systems. The paper describes equipment and programmatic solutions implemented in the axle counter system UniAC1 which possesses the SIL4 certificate, including the safe communication solutions. The paper describes also the safety analysis carried out using the method of Markov graphs and presents the results for the UniAC1 system.

Keywords: safety, safety on the railway network, axle counter system, interlocking systems, railway automation

Методы гарантирующие безопасность системы сигнализации на примере счетника осей UniAC1

Резюме

В докладе представлены методы гарантирующие самый высокий уровень неприкосновенности безопасности устройствам СЦБ. Описано оборудование и программирование введено в системе учета осей UniAC1 имеющие сертификат SIL4, в том числе сертификат безопасной коммуникации. Описан также анализ безопасности проведен при использовании метода графов Маркова и представлены результаты для системы UniAC1.

Ключевые слова: безопасность, безопасность в ж-д транспорте, система учета осей, СЦБ