WYKRYWANIE USTEREK I TOLEROWALNY POZIOM INTENSYWNOŚCI ZAGROŻEŃ NA PRZYKŁADZIE SYSTEMU UniAC[1]

Wojciech Ulatowski
dr inż., voestalpine SIGNALING Sopot Sp. z o. o., e-mail: wojciech.ulatowski@tens.pl

Michał Bigus
mgr inż., voestalpine SIGNALING Sopot Sp. z o. o., e-mail: michal.bigus@tens.pl

Streszczenie. *W referacie przedstawiono metody analizy zagrożeń z uwzględnieniem różnych rodzajów uszkodzeń, a także różnice w stosowaniu podejścia optymistycznego i pesymistycznego. Opisano rozwiązania analityczne pozwalające obliczyć intensywność zagrożeń dla złożonej struktury elektronicznej charakteryzującej się różną dynamiką bloków przetwarzania i co za tym idzie różnymi czasami wykrywania poszczególnych usterek. Przedstawiono także sposób uwzględnienia intensywności zagrożeń pochodzącej od usterek niewykrywalnych.*

Słowa kluczowe: *bezpieczeństwo, bezpieczeństwo na kolei, system liczenia osi, sterowanie ruchem kolejowym, analiza zagrożeń*

1. Kilka słów o systemie

System liczenia osi UniAC1 jest systemem wskazującym stan zajętości odcinka torowego (odcinków) w obrębie swojego działania. W celu określenia stanu odcinka torowego system kontroluje sygnały pochodzące od głowic torowych umieszczonych przy szynie. Informacje o przejeździe koła nad głowicą torową oraz informacja o kierunku przejazdu pozwalają zliczać i bilansować osie na kontrolowanym odcinku toru.

System składa się z kilku kart przetwarzających sygnały. Wszystkie karty są dwukanałowe, a w kanałach występują różne technologie.

Analiza bezpieczeństwa systemu liczenia osi UniAC obejmowała wiele obszarów, które producent musiał wziąć pod uwagę podczas obliczania wskaźnika intensywności zagrożeń (*ang. hazard rate*). Kluczowym zadaniem było przeprowadzenie szczegółowej identyfikacji rodzajów uszkodzeń, opracowanie testów sprawności podzespołów systemu, a także uwzględnienie czasów wykrywania uszkodzeń w analizie zagrożeń. Taka złożona struktura elektroniczna charakteryzuje się różną dynamiką bloków przetwarzania i co za tym idzie różnymi czasami wykrywania poszczególnych usterek.

1 Wkład procentowy poszczególnych autorów: Ulatowski W. 50%, Bigus M. 50%

2. Cel i założenia do analizy

Najważniejszym celem analizy bezpieczeństwa systemu liczenia osi UniAC1 była ocena intensywności zagrożeń HR systemu. Zgodnie z PN-EN 50129:2007 [1] (tab. 1), dopuszczalna intensywność zagrożeń THR dla poziomu bezpieczeństwa SIL-4 nie powinna być większa niż 10^{-8} h^{-1}. Analizę oparto na dekompozycji modularnej systemu. Już wstępna dekompozycja pozwoliła wyodrębnić elementy przetwarzające sygnały związane z bezpieczeństwem, składające się na ścieżkę krytyczną. Za stan niebezpieczny przyjęto stan niezajętości po wjechaniu zestawu kołowego na odcinek torowy. Dopilnowano, aby bloki przetwarzające sygnał, które znalazły się na ścieżce krytycznej, zostały wykonane z elementów, które są sprawdzone i/lub mają zadeklarowane przez producenta intensywności uszkodzeń.

3. Podejście optymistyczne i pesymistyczne

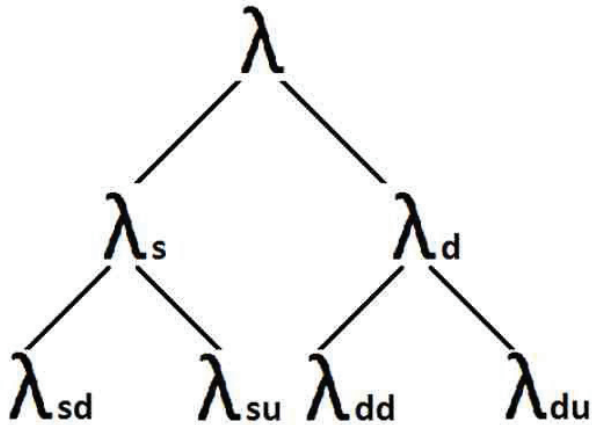
Możliwe jest zastosowanie dwóch podejść, jeżeli chodzi o skutki uszkodzeń – pesymistyczne lub optymistyczne. Podejście optymistyczne zakłada, że nie wszystkie uszkodzenia spowodują niemożliwość przejścia systemu do stanu bezpiecznego. To znaczy, że nie wszystkie uszkodzenia są niebezpieczne.

Podejście pesymistyczne zakłada, że wszystkie uszkodzenia spowodują niemożliwość przejścia systemu do stanu bezpiecznego.

W przypadku niewielkiej wiedzy o rodzajach i skutkach uszkodzeń, wybór pomiędzy podejściami optymistycznym i pesymistycznym jest wyborem pomiędzy skrajnościami. Zastosowanie podejścia optymistycznego można podważyć jako takie, które może pominąć niektóre rodzaje uszkodzeń niebezpiecznych. Zastosowanie podejścia pesymistycznego jest bardzo surowe i w efekcie może się okazać, że wynikowa intensywność zagrożeń jest zbyt wysoka, aby spełnić wymagania normy[1]. Zdecydowano się zastosować podejście, którego wynik będzie mieścił się pomiędzy rozwiązaniem pesymistycznym, a optymistycznym. Nazwano je podejściem optymalnym.

Warto uwzględnić w analizie, że nie wszystkie uszkodzenia są niebezpieczne. Wszystko zależy od aplikacji. Należy pamiętać, że nie wszystkie intensywności uszkodzeń są niebezpieczne. W wielu opracowaniach spotyka się ich rozbicie intensywności uszkodzeń na: bezpieczne i niebezpieczne, a dalej każde z nich na wykrywalne i niewykrywalne (rys. 1).

Kluczem do dalszych prac jest przeprowadzenie analizy rodzajów i skutków uszkodzeń zgodnie z normą [1] . Korzyści płynących z tejże analizy jest wiele. Najważniejsze z nich, to możliwość świadomego zarządzania bezpieczeństwem każdego elementu w jego otoczeniu i w warunkach pracy. Analiza w przejrzysty sposób porządkuje rodzaje uszkodzeń elementów, które są inherentnie bezpieczne oraz takie, które wymagają testowania.



Rys. 1. Różne rodzaje intensywności uszkodzeń

λ_{sd} – całkowita intensywność uszkodzeń bezpiecznych wykrywalnych,
λ_{su} – całkowita intensywność uszkodzeń bezpiecznych niewykrywalnych,
λ_{dd} – całkowita intensywność uszkodzeń niebezpiecznych wykrywalnych,
λ_{du} – całkowita intensywność uszkodzeń niebezpiecznych niewykrywalnych.

Analiza rodzajów i skutków uszkodzeń ujawniła, że uszkodzenia niebezpieczne, które mogą pojawić się podczas pracy systemu można podzielić na:

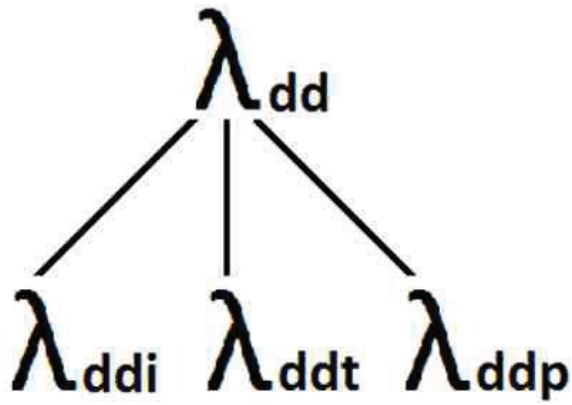
1. Uszkodzenia inherentnie bezpieczne – dalej oznaczane jakoi – z nimi jest związana intensywność uszkodzeń niebezpiecznych wykrywanych inherentnych **ddi**.
2. Uszkodzenia wykrywane testami przez każdy kanał – dalej oznaczane jakot – z nimi jest związana intensywność uszkodzeń niebezpiecznych wykrywanych testem **ddt**.
3. Uszkodzenia wykrywane podczas przejazdu przez sąsiedni kanał – dalej oznaczane jako **p** – z nimi jest związana intensywność uszkodzeń niebezpiecznych wykrywanych podczas przejazdu **ddp**.
4. Uszkodzenia niewykrywalne – dalej oznaczane jako **u** – z nimi jest związana intensywność uszkodzeń niebezpiecznych niewykrywanych **du**.

Cztery powyższe kategorie są widoczne w arkuszu (tab. 1). Na jego podstawie można powiedzieć, że uszkodzenia niebezpieczne wykrywalne dzielą się w rzeczywistości jak na rys. 2.

Takie uszczegółowienie pozwala łatwiej zarządzać zabezpieczeniem konkretnego elementu, ale komplikuje obliczenie wynikowej intensywności zagrożeń HR.

Tabela 1. Widok arkusza z różnymi rodzajami wykrywania uszkodzeń

Oznaczenie	Nazwa	lambda	i	t	p	u	ddi	ddt	ddp	du
C209	Kondensator (1812)	2,26E-08	1				2,26E-08			
C211	Kondensator (1206)	5,66E-09				1				5,66E-09
C213	Kondensator (1206)	5,66E-09		1				5,66E-09		
C215	Kondensator (0603)	5,87E-09	1				5,87E-09			
C227	Kondensator (0603)	3,39E-09	1				3,39E-09			
D201	Dioda szybka (SMA)	1,03E-08	1				1,03E-08			
D203	Transil (SMC)	1,39E-09	1				1,39E-09			
D205	Dioda Schottky (SC-70-3)	5,99E-09	1				5,99E-09			
Q205	Tranzystor NPN (SOT-23-3)	2,43E-09	1				2,43E-09			
R201	Rezystor (0603)	1,00E-10	1				1,00E-10			
R205	Rezystor (0603)	1,00E-10				1				1,00E-10
U205	Wzm. Izolacyjny (SOIC-8)	2,20E-10				1				2,20E-10
U207	Komparator (TSOT-23-6)	2,20E-10	1				2,20E-10			
U211	Wzm. op. (TSSOP-14)	1,74E-10				1				1,74E-10
U213	Izolator (WSO-16)	6,13E-10	1				6,13E-10			
R607	Rezystor (0603)	1,00E-10			1				1,00E-10	
R611	Rezystor (0603)	1,00E-10			1				1,00E-10	
R613	Rezystor (0603)	1,00E-10			1				1,00E-10	
R615	Rezystor (0603)	1,00E-10			1				1,00E-10	
R617	Rezystor (0603)	1,00E-10			1				1,00E-10	



Rys. 2. Dekompozycja rodzajów uszkodzeń niebezpiecznych wykrywalnych

4. Obliczenie czasu ujawniania usterek pojedynczych

Norma [1] zaleca, aby łączny czas wykrycia i blokowania t_{sf} w przypadku pojedynczych defektów w odpowiednich obiektach nie przekraczał wartości:

$$t_{sf} \leq \frac{k}{1000 * a} \tag{1}$$

gdzie: $k = 1$ dla systemów o architekturze 2 z 2, zaś a jest to suma intensywności uszkodzeń wszystkich elementów dla jednego kanału przetwarzania.

Należy traktować wynikowyczas jako najdłuższy z możliwych, wiedząc że znaczna większość uszkodzeń elementów jest wykrywana w czasie rzędu kilku sekund lub minut.

5. Jak policzyć THR?

Intensywność zagrożeń HR można obliczyć w oparciu o wzór A.1 normy[1]:

$$HR \approx \frac{\lambda_1}{SDR_1} \times \frac{\lambda_2}{SDR_2} \times (SDR_1 + SDR_2) \tag{2}$$

Współczynnik bezpiecznego wyłączenia *SDR* jest określony następującą zależnością:

$$SDR = \frac{1}{\frac{T}{2} + czas\_blokowania} \tag{3}$$

gdzie: *T* oznacza czas między dwoma kolejnymi testami.

Przypadek opisany w normie jest o tyle idealny, że nie uwzględnia różnych czasów wykrywania usterek oraz nie zawiera intensywności zagrożeń pochodzących od uszkodzeń niewykrywalnych.

W rzeczywistości, różna dynamika przetwarzania sygnałów powoduje, że dla różnych elementów, których usterki są wykrywalne, mamy różne czasy testowania i, co za tym idzie, różne wartości współczynnika bezpiecznego wyłączenia SDR. Warto zatem grupować elementy o takim samym współczynniku bezpiecznego wyłączenia SDR, następnie policzyć HR dla grup i wyniki sumować.

Na potrzeby analizy systemu UniAC1 należało przede wszystkim rozszerzyć powyższy wzór o intensywności uszkodzeń niebezpiecznych niewykrywalnych:

$$HR = HR_{DD} + HR_{DU} \tag{4}$$

a po uszczegółowieniu analizą rodzajów i skutków uszkodzeń rozbić HR_{DD} na kolejne trzy rodzaje uszkodzeń, więc można zapisać, że:

$$HR = HR_{DDi} + HR_{DDt} + HR_{DDp} + HR_{DU} \tag{5}$$

Część HR_{DD} wzoru będzie pogrupowana na różne grupy (i) zależne od czasu wykrywania usterek. W efekcie można zapisać, że:

$$HR_{UniAC1} \approx \frac{\lambda_{DD1i}}{SDR_{1_i}} \times \frac{\lambda_{DD2i}}{SDR_{2i}} \times (SDR_{1i} + SDR_{2i}) + \lambda_{DU} \tag{6}$$

gdzie:

HR_{DU} – intensywność zagrożeń pochodząca od uszkodzeń niebezpiecznych i niewykrywalnych,

HR_{DD} – intensywność zagrożeń pochodząca od uszkodzeń niebezpiecznych i wykrywalnych,

λ_{DD1i} – całkowita intensywność uszkodzeń i-tej grupy kanału przetwarzającego 1, wykrytych podczas testowania i/lub przejazdu taboru w h^{-1},

λ_{DD2i} – całkowita intensywność uszkodzeń i-tej grupy kanału przetwarzającego 2, wykrytych podczas testowania i/lub przejazdu taboru w h^{-1},
λ_{DU} – całkowita intensywność uszkodzeń niebezpiecznych i niewykrywalnych,
SDR_{1i} – współczynnik bezpiecznego wyłączenia i-tej grupy dla kanału przetwarzającego 1, w h^{-1},
SDR_{2i} – współczynnik bezpiecznego wyłączenia i-tej grupy dla kanału przetwarzającego 2, w h^{-1}.

6. Wnioski

Otrzymane wyniki pokazują jak obliczyć intensywność zagrożeń dla złożonego systemu elektronicznego. Z punktu widzenia praktycznej aplikacji udało się opracować podejście optymalne, korzystniejsze od podejścia pesymistycznego. Pierwszą korzyścią jest uporządkowanie rodzajów i skutków uszkodzeń oraz uszczegółowienie tych obszarów, które wymagają testowania – zarządzanie uszkodzeniami elementu elektronicznego w jego warunkach pracy staje się czytelne i relatywnie proste. Po drugie, czytelne i łatwe zarządzanie uszkodzeniami stwarza możliwość optymalizowania poziomu ryzyka. Producent może zacząć zadawać sobie pytania, ile bezpieczeństwo kosztuje i precyzyjnie lokować lepsze (droższe) zabezpieczenia tak, aby otrzymać największą korzyść z dodatkowo wydanych pieniędzy. Po trzecie, otrzymana wynikowa wartość intensywności zagrożeń jest bliższa rzeczywistej, dzięki pominięciu uszkodzeń nieistotnych bądź nierealnych z punktu widzenia analizy.Co najważniejsze, analiza przeprowadzona w taki sposób również spełnia wymagania poziomu nienaruszalności bezpieczeństwa SIL4.

Bibliografia

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