Wykrywanie usterek i tolerowalny poziom intensywności zagrożeń na przykładzie systemu UniAC1

Michał BIGUS[1], Wojciech ULATOWSKI[2]

Streszczenie
W artykule przedstawiono metody analizy zagrożeń z uwzględnieniem różnych rodzajów uszkodzeń. Opisano rozwiązania analityczne umożliwiające obliczenie intensywności zagrożeń 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. Wstęp

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 umożliwiają zliczanie i bilansowanie osi 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 UniAC1 obejmowała wiele obszarów, które producent musiał wziąć pod uwagę podczas obliczania wskaźnika intensywności zagrożeń (ang. *hazard rate*) [1, 4]. Kluczowym zadaniem było przeprowadzenie szczegółowej identyfikacji rodzajów uszkodzeń, opracowanie testów sprawności podzespołów systemu, a także uwzględnienie czasów wykrywania uszkodzeń w analizie zagrożeń [2, 3]. Taka złożona struktura elektroniczna charakteryzuje się różną dynamiką bloków przetwarzania i co za tym idzie różnymi czasami wykrywania poszczególnych usterek [6].

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 [5] (tablica A.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 – optymistyczne lub pesymistyczne [1]. Podejście optymistyczne zakłada, że nie wszystkie uszkodzenia spowodują niemożliwość przejścia systemu do stanu bezpiecznego, to znaczy, że nie wszystkie uszkodzenia są niebezpieczne.

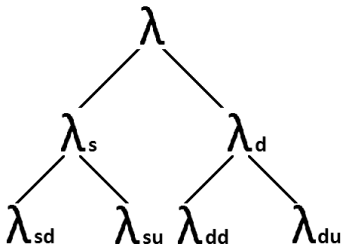
Podejście pesymistyczne zakłada, że wszystkie uszkodzenia spowodują niemożliwość przejścia systemu do stanu bezpiecznego.

W przypadku niewielkiej wiedzy o rodzajach i skutkach uszkodzeń, wybór pomiędzy podejściami: optymistycznym i pesymistycznym jest wyborem pomiędzy skrajnościami. Zastosowanie podejścia

[1] Mgr inż.; voestalpine SIGNALING Sopot; e-mail:michal.bigus@voestalpine.com.
[2] Dr inż.; Były pracownik voestalpine SIGNALING Sopot.

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 [5]. Zdecydowano się zastosować podejście, którego wynik będzie mieścił się pomiędzy rozwiązaniem pesymistycznym a optymistycznym. Nazwano je podejściem racjonalnym.

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



Rys. 1. Różne rodzaje intensywności uszkodzeń [opracowanie własne]:

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.

Kluczem do dalszych prac jest przeprowadzenie analizy rodzajów i skutków uszkodzeń zgodnie z normą [5]. Korzyści płynących z tej 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. 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 jako **i** – z nimi jest związana intensywność uszkodzeń niebezpiecznych wykrywanych inherentnych **ddi**.
2. Uszkodzenia wykrywane testami przez każdy kanał – dalej oznaczane jako **t** – 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 (tablica 1). Na jego podstawie można stwierdzić, że uszkodzenia niebezpieczne wykrywalne dzielą się w rzeczywistości jak na rysunku 2.

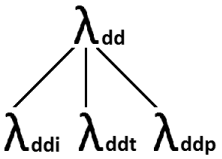
Tablica 1

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	

[źródło: opracowanie własne]

Takie uszczegółowienie umożliwia łatwiejsze zarządzanie zabezpieczeniem konkretnego elementu, ale komplikuje obliczenie wynikowej intensywności zagrożeń HR.



Rys. 2. Dekompozycja rodzajów uszkodzeń niebezpiecznych wykrywalnych [źródło: opracowanie własne]

4. Obliczenie czasu ujawniania usterek pojedynczych

Norma [5] zaleca, aby łączny czas wykrycia i blokowania t_{sf} w przypadku pojedynczych defektów w odpowiednich obiektach nie przekraczał wartości:

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

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

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

5. Obliczenie THR

Intensywność zagrożeń HR można obliczyć na podstawie wzoru A.1 normy [5]:

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

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 współczynnikiem bezpiecznego wyłączenia SDR, następnie policzyć *HR* dla grup i wyniki sumować.

Na potrzeby analizy systemu UniAC1 należało przede wszystkim rozszerzyć wzór (2) o intensywności uszkodzeń niebezpiecznych niewykrywalnych

$$HR = HR_{\mathrm{DD}} + HR_{\mathrm{DU}}$$

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

$$HR = HR_{\mathrm{DDi}} + HR_{\mathrm{DDt}} + HR_{\mathrm{DDp}} + HR_{\mathrm{DU}} \tag{4}$$

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

$$HR_{\mathrm{UniAC1}} \approx \frac{\lambda_{\mathrm{DD1}i}}{SDR_{1i}} \times \frac{\lambda_{\mathrm{DD2}i}}{SDR_{2i}} \times \left(SDR_{1i} + SDR_{2i}\right) + \lambda_{\mathrm{DU}} \tag{5}$$

gdzie:

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

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

$\lambda_{\mathrm{DDl}i}$ – całkowita intensywność uszkodzeń i-tej grupy kanału przetwarzającego 1 wykrytych podczas testowania i/lub przejazdu taboru w h^{-1},

$\lambda_{\mathrm{DD2}i}$ – 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

Przedstawione rozwiązania pokazują jak obliczyć intensywność zagrożeń dla złożonego systemu elektronicznego. Z punktu widzenia praktycznej aplikacji udało się opracować podejście racjonalne, 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 kosztuje bezpieczeństwo 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.

Literatura

1. Adams F.: *Specific Background Information on EN ISO 13849-1:2006 for Schmersal / Alan Sales & Technical Staff and for Interested Customers*, Wuppertal / Wettenberg, April 2009, Germany.
2. Cichocki T., Górski J.: *Analiza bezpieczeństwa przemysłowych zastosowań informatyki z wykorzystaniem metody FMEA*. W: III Krajowa Konferencja Naukowo-Techniczna 7–10 wrzesień, 1998, Jurata k. Gdańska, Diagnostyka Procesów Przemysłowych, Wrzesień 1998, Gdańsk, s. 213-219.
3. Lewiński A., Perzyński T., Bester L.: *Komputerowe wspomaganie analizy bezpieczeństwa w systemach sterowania ruchem kolejowym*, W: Prace Naukowe Politechniki Warszawskiej – Transport, Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Marzec 2013, s. 259–271.
4. Missala T.: *Bezpieczeństwo funkcjonalne – awers i rewers*, W: Pomiary Automatyka Robotyka 1/2008, Styczeń 2008, Warszawa, s. 12–17.
5. PN-EN 50129:2007: Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem.
6. Seymour B.: *MTTF, Failrate, Reliability and Life Testing*, W: Burr-Brown Application Bulletin, Tuscon, USA, December 1993.

Fault Detection and Tolerable Hazard Rate in UniACl System

Summary
In the presentation, the hazard analysis methods considering different types of failures and a difference between optimistic and pessimistic approach are presented. It shows analytic solutions helpful in calculation of hazard rate for complex electronic structure, which is characterized by different dynamic of processing blocks and different fault detection times. What is more the presentation shows a method of adding hazard rate of undetected failures.

Keywords: safety, railway safety, axle counting system, railway signaling, hazard analysis

Обнаружение дефектов и допускаемый уровень интенсивности угроз на примере системы UniAC1

Резюме
В статье представлены методы анализа угроз с учетом разных видов повреждений. Описапы аналитические решения которые позволяют вычислить интенсивность угроз для сложной электронной структуры обладающей разновидной динамикой блоков обработки, и следовательно разными временами обнаружения отдельных дефектов. Представлены также способ учета интенсивности угроз вытекающих из необнаружываемых дефектов.

Ключевые слова: безопасность, безопасность на железной дороге, системы подсчета осей, управление движением, анализ угроз