Waldemar Nowakowski, Zbigniew Łukasik, Wojciech Bukalski

Metody oceny bezpieczeństwa systemów automatyki przemysłowej

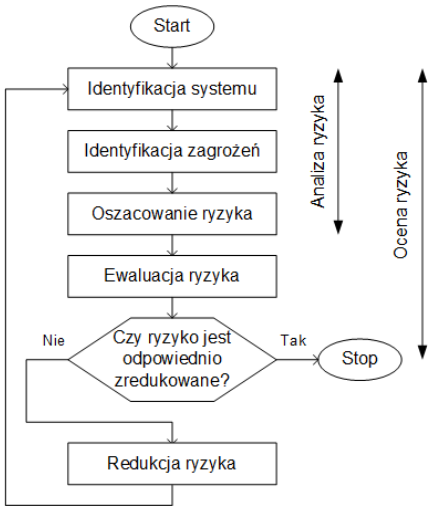
JEL: L94 DOI: 10.24136/atest.2018.375
Data zgłoszenia: 19.11.2018 Data akceptacji: 15.12.2018

Automatyka przemysłowa, jako dział automatyki zajmujący się automatyzacją procesów wytwarzania i procesów technologicznych, odgrywa istotną rolą w gospodarce. We współczesnym świecie trudno wyobrazić sobie nowoczesną fabrykę bez zrobotyzowanych linii produkcyjnych. Postęp ten związany jest jednak z potrzebą zapewnienia bezpieczeństwa. Znaczenie bezpieczeństwa w przemyśle stale rośnie i oczywiście dotyczy to również automatyki przemysłowej. Ma to swoje odzwierciedlenie w przepisach, w tym m.in. w dokumentach normatywnych. W artykule przedstawiono metody przeprowadzenia weryfikacji systemów automatyki przemysłowej bazując na dwóch podstawowych parametrach, jakimi są: poziom zapewnienia bezpieczeństwa PL (Performance Level) oraz poziom nienaruszalności bezpieczeństwa SIL (Safety Integrity Level).

Słowa kluczowe: bezpieczeństwo, PL, SIL, automatyka przemysłowa.

Wstęp

Jednym z istotnych elementów bezpieczeństwa w przemyśle jest bezpieczeństwo systemów automatyki przemysłowej. Ryzyko związane z działaniem systemów technicznych musi być na akceptowalnym poziomie [3, 4, 6, 7, 16]. Dlatego też zachodzi konieczność uwzględniania metod analizy ryzyka w czasie projektowania, budowania i utrzymania systemów automatyki przemysłowej. Pod pojęciem ryzyka rozumie się możliwość wystąpienia zdarzenia niepożądanego i związanych z tym strat, które ono spowoduje. Zdarzenie niepożądane, to takie zdarzenie (niesprawność, uszkodzenie, awaria, błąd ludzki), którego zajście powoduje powstanie zagrożenia. W każdym systemie technicznym, w różnym czasie mogą pojawiać się nowe zdarzenia niepożądane, które mogą wywołać ciąg zdarzeń wtórnych i przejście ze stanu zagrożenia do strat nazywanych wypadkiem lub katastrofą. Wielkość strat odnosi się najczęściej do życia i zdrowia ludzkiego, strat materialnych oraz strat ekologicznych [9, 10, 12]. W procesie oceny ryzyka (ang. risk assessment) można wyróżnić kilka podstawowych etapów. Pierwszym z nich jest identyfikacja systemu technicznego. Celem tego etapu jest dokładne poznanie obiektu badań, warunków jego pracy, sposobu obsługi itp. W naszym przypadku jest to wyodrębnienie wszystkich systemów automatyki przemysłowej. Następnie przeprowadzana jest identyfikacja zagrożeń (ang. hazard identification), w czasie której dokonywane jest rozpoznanie zdarzeń niebezpiecznych, które mogą wystąpić w trakcie eksploatacji systemu technicznego. W ramach tego etapu przygotowywany jest dokładny opis potencjalnych zdarzeń, identyfikowane są ich przyczyny, skutki oraz możliwe zabezpieczenia. Na podstawie zgromadzonych informacji dokonuje się oszacowania ryzyka (ang. risk estimation). Te trzy etapy wchodzą w skład analizy ryzyka (ang. risk analysis). Po oszacowaniu ryzyka powinna być przeprowadzona ewaluacja ryzyka (ang. risk evaluation) oraz podjęcie decyzji o akceptowalności lub nie występującego ryzyka. W przypadku braku akceptowalności ryzyka wymagane jest podjęcie działań mających na celu zmniejszenie ryzyka, określanych mianem funkcji bezpieczeństwa, a następnie powtórne przeprowadzenie całej procedury oceny (rys. 1) [5, 8,11].



Rys. 1. Proces oceny ryzyka systemu technicznego (opracowanie własne)

Poziom bezpieczeństwa systemów automatyki przemysłowej określa się za pomocą jednego z dwóch możliwych parametrów [13]:

- poziom zapewnienia bezpieczeństwa PL (ang. Performance Level) - możne być zastosowany w stosunku do elektrycznych, mechanicznych, pneumatycznych oraz hydraulicznych rozwiązań służących poprawie bezpieczeństwa,
- poziom nienaruszalności bezpieczeństwa SIL (ang. Safety Integrity Level) - może być zastosowany wyłącznie w do oceny elektrycznych, elektronicznych i programowalnych rozwiązań służących poprawie bezpieczeństwa.

1.Poziom zapewnienia bezpieczeństwa PL

Parametr PL przyjmuje pięć poziomów: a, b, c, d, e, przy czym poziom e jest najwyższym poziomem bezpieczeństwa (tabela 1) [1, 2].

Tab. 1. Klasyfikacja PL [15]

PL	PFH_d
a	$\geq 10^{-5}$ do $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ do $< 10^{-5}$
c	$\geq 10^{-6}$ do $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ do $< 10^{-6}$
e	$\geq 10^{-8}$ do $< 10^{-7}$

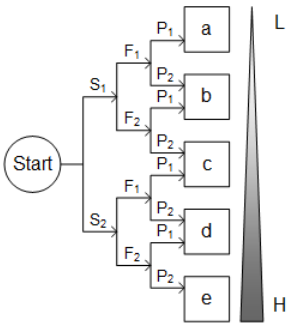
gdzie: PFH_d - prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę.

Ocenę ryzyka systemu automatyki przemysłowej należy rozpocząć od zidentyfikowania źródeł ryzyka. Następnie dla każdego z nich określa się ryzyko na podstawie trzech czynników:

1. **S** - stopień obrażeń:
   - S1 - lekkie (nietrwałe),
   - S2 -poważny (trwałe obrażenia lub śmierć).
2. **F** - częstotliwość narażenia na ryzyko:
   - F1 - rzadko do okazjonalnie i/lub czas narażenia jest krótki,
   - F2 - często do ciągle i/lub czas narażenia jest długi.

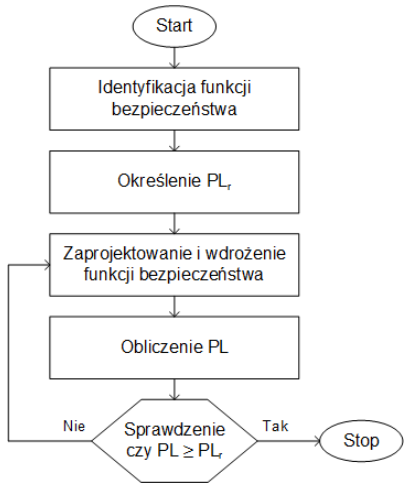
3. **P** - możliwość uniknięcia niebezpieczeństwa lub ograniczenia szkód:
   - P1 - możliwe pod pewnymi warunkami,
   - P2 - niemal niemożliwe.

Pozwala to na uzyskanie odpowiedzi, czy istnieje konieczność redukcji ryzyka, czy też zapewnione jest wystarczające bezpieczeństwo. W sytuacji kiedy należy zredukować ryzyko, dla każdej zastosowanej funkcji bezpieczeństwa niezbędne jest określenie PLr (ang. Performance level required). Do tego celu stosuje się graf ryzyka przedstawiony na rys. 2.



Rys. 2. Oszacowanie wymaganego PL (opracowanie własne na podstawie [15])

Następnie projektowane i wdrażane jest rozwiązanie techniczne funkcji bezpieczeństwa, po czym można obliczyć jego poziom PL. Jednocześnie należy upewnić się, że obliczone PL jest co najmniej tak wysokie jak PLr (rys. 3).



Rys. 3. Procedura weryfikacji funkcji bezpieczeństwa (opracowanie własne)

Podczas obliczania PL najprościej jest podzielić system na podsystemy, na przykład: wejście, blok logiki i wyjście. Jeśli znamy PL dla każdego z podsystemów (np. zdefiniowane przez producentów), wówczas PL systemu wynika z najniższego PL dla podsystemu i liczby podsystemów (tabela 2).

Natomiast w przypadku, gdy PL podsystemu jest nieznany musimy go wyliczyć samodzielnie na podstawie:
- struktury układu (kategorii),
- wartości średniego czasu pomiędzy niebezpiecznymi uszkodzeniami ($MTTF_d$),
- pokrycia diagnostycznego (DC),
- odporności na uszkodzenia spowodowane wspólną przyczyną (CCF).

Tab. 2. Wyznaczanie PL systemu na podstawie znajomości PL podsystemów [15]

Najniższy PL podsystemu	Liczba podsystemów posiadających taki PL	Maksymalny możliwy do uzyskania PL
a	>3	niedozwolony
	≤ 3	a
b	>2	a
	≤ 2	b
c	>3	b
	≤ 3	c
d	>3	c
	≤ 3	d
e	>3	d
	≤ 3	e

Wyróżnia się następujące kategorie: B, 1, 2, 3, 4, przy czym trzy pierwsze kategorie dotyczą układów jednokanałowych. Różnica między kategorią 1 a 2 jest taka, że kategoria 1 dotyczy podsystemów zbudowanych z wypróbowanych elementów z uwzględnieniem sprawdzonych zasad bezpieczeństwa, natomiast kategoria 2 obejmuje podsystemy z detekcją uszkodzeń. Kategoria 3 i 4 dotyczy podsystemów z redundancją i diagnostyką. W kategorii 3 zakłada się, że pojedyncza usterka nie prowadzi do utraty funkcji bezpieczeństwa, a w kategorii 4, że pojedyncza usterka zostanie wykryta w czasie lub przed następnym użyciem funkcji bezpieczeństwa.

Wartość średniego czasu pomiędzy niebezpiecznymi uszkodzeniami oblicza się z uwzględnieniem rodzaju elementów podsystemu. Dla części mechanicznych i hydraulicznych można ten parametr ustalić na podstawie normy [15]. W przypadku części pneumatycznych, mechanicznych i elektromechanicznych $MTTF_d$ wyznacza się na podstawie wzoru:

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$
$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3600\,s/h}{t_{cycle}} \quad (1)$$

gdzie: B_{10d} - średnia ilość cykli roboczych, osiągniętych przed czasem, w którym 10% urządzeń testowych ulegnie defektowi prowadzącemu do niebezpiecznego uszkodzenia, n_{op} - średnia ilość cykli na rok, d_{op} - średni czas pracy w dniach na rok, h_{op} - średni czas pracy w godzinach na dzień, t_{cycle} - średni czas pomiędzy rozpoczęciem dwóch kolejnych cykli w sekundach na cykl.

Natomiast dla elementów elektronicznych wyznacza się ze wzoru:

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} \quad (2)$$

gdzie: N - liczba elementów.

Następnie, dla tak wyznaczonego parametru ustala się jeden z trzech zakresów: krótki, średni, długi (tabela 3).

Tab. 3. Różne metody obliczania lub szacowania $MTTF_d$ [15]

$MTTF_d$	
Oznaczenie każdego kanału	Zakres każdego kanału
niski	3 lata ≤ $MTTF_d$ < 10 lat
średni	10 lata ≤ $MTTF_d$ < 30 lat
wysoki	30 lata ≤ $MTTF_d$ < 100 lat

Pokrycie diagnostyczne DC dla podsystemu określane jest jako stosunek intensywności wykrywalnych niebezpiecznych uszkodzeń do intensywności wszystkich niebezpiecznych uszkodzeń:

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{DD} + \sum \lambda_{DU}} \quad (3)$$

gdzie: λ_{DD} - intensywność wykrywalnych niebezpiecznych uszkodzeń, λ_{DU} - intensywność niewykrywalnych niebezpiecznych uszkodzeń.

Natomiast dla całego systemu ze wzoru:

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_n}{MTTF_{dn}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dn}}} \quad (4)$$

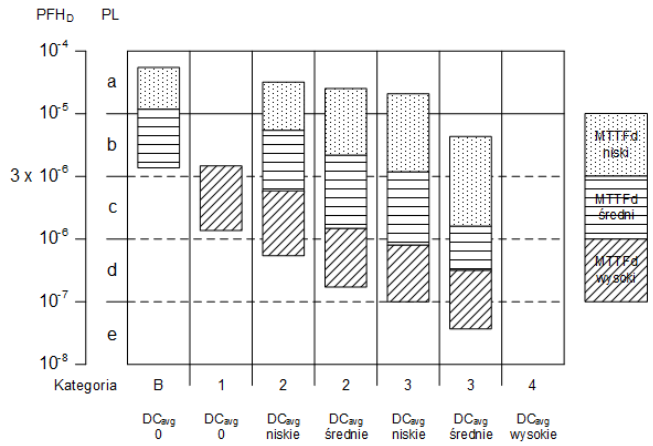
W praktyce pokrycie diagnostyczne szacuje się na podstawie normy, przy czym DC_{avg} przyjmuje wartość w przedziałach określonych w tabeli 4.

Tab. 4. Zakresy pokrycia diagnostycznego DC_{avg} [15]

Kwalifikacja	Pokrycie diagnostyczne DC
brak	DC <60%
niski	60% ≤ DC <90%
średni	90% ≤ DC <99%
wysoki	99% ≤ DC

Parametr CCF określa odporność systemu na zdarzenia, które powodują jednoczesne awarie dwóch lub więcej oddzielnych kanałów w systemie wielokanałowym, co może prowadzić do niepowodzenia w funkcji związanych z bezpieczeństwem. Skala odporności CFF jest punktowa z maksymalna liczbą punktów 100. Sprawdzenie CFF polega na zastosowaniu odpowiednich środków ochronnych i zsumowaniu przyznanych dla nich punktów. Wymaganie uznaje się za spełnione, gdy minimalna liczba tych punktów wyniesie 65.

Po oszacowaniu wszystkich czterech, wcześniej omówionych parametrów, można przystąpić do określenia PL podsystemu korzystając z rys. 4.



Rys. 4. Relacje między: kategoriami, DC_{avg}, $MTTF_d$, a PL podsystemu (opracowanie własne na podstawie [15])

W celu określenia PL całego systemu korzysta się jak poprzednio z tabeli 2. Jeśli otrzymany PL z tabeli 2 jest większy lub równy od wymaganego dla funkcji bezpieczeństwa PLr, to stwierdza się, że układ bezpieczeństwa spełnia wymagania odpornością na uszkodzenia.

2.Poziom nienaruszalności bezpieczeństwa SIL

W celu określenia docelowego SIL należy wyznaczyć [1, 2]:

1. Dotkliwość potencjalnej szkody Se,
2. Prawdopodobieństwo zaistnienia szkody:
   - częstotliwość i czas trwania narażenia Fr,
   - prawdopodobieństwo wystąpienia zdarzenia niebezpiecznego Pr,
   - prawdopodobieństwo uniknięcia lub ograniczenia szkody Av.

Parametr Se jest określany z uwzględnieniem ciężkości obrażeń lub uszczerbku na zdrowiu. Klasyfikacja jest przedstawione w tabeli 5.

Tab. 5. Klasyfikacja dotkliwości potencjalnej szkody Se [14]

Konsekwencje	Se
Nieodwracalne: śmierć, utrata oka lub ręki	4
Nieodwracalne: złamania kończyn, utrata palców	3
Odwracalne: wymagana interwencja personelu medycznego	2
Odwracalne: wymagana pierwsza pomoc	1

Częstotliwość i czas trwania narażenia Fr jest związany z potrzebą uzyskania dostępu do stref niebezpiecznych, co zostało przedstawione w tabeli 6.

Tab. 6. Klasyfikacja częstotliwości i czasu trwania narażenia Fr [14]

Częstotliwość lub czas przebywania	Fr
≤ 1 h	5
> 1h do ≤ 1 dzień	5
> 1 dzień do ≤ 2 tygodnie	4
> 2 tygodnie do ≤ 1 rok	3
> 1 rok	2

Przy wyznaczaniu parametru Pr (tabela 7) muszą być brane pod uwagę dwa uwarunkowania:

- przewidywalność niebezpiecznych elementów maszyny w różnych trybach pracy (praca normalna, konserwacja, naprawa).
- zachowanie osób, które wchodzą w interakcje z maszyną, takie jak stres, zmęczenie, brak doświadczenia itp.

Tab. 7. Klasyfikacja prawdopodobieństwa wystąpienia zdarzenia niebezpiecznego Pr [14]

Prawdopodobieństwo wystąpienia	Pr
Bardzo wysokie	5
Dogodne	4
Możliwe	3
Rzadkie	2
Pomijalne	1

Ostatni z parametrów Av uwzględnia prawdopodobieństwo uniknięcia lub ograniczenia szkody i jest związany z konstrukcją systemu (tabela 8).

Tab. 8. Klasyfikacja prawdopodobieństwa uniknięcia lub ograniczenia szkody Av [14]

Prawdopodobieństwo wystąpienia	Av
Niemożliwe	5
Rzadkie	3
Prawdopodobne	1

Suma parametrów: Fr, Pr i Av określa klasę prawdopodobieństwa Cl. Oszacowanie SIL dokonuje się za pomocą tabeli 9.

Tab. 9. Matryca przypisywania SIL [14]

	Klasa Cl				
Se	3 - 4	5 - 7	8 - 10	11 - 13	14 - 15
4	SIL2	SIL2	SIL2	SIL3	SIL3
3	-	-	SIL1	SIL2	SIL3
2	-	-	-	SIL1	SIL2
1	-	-	-	-	SIL1

Jeśli analizowany system zbudowano z podsystemów dla których są określone parametry:
- SILCL - najwyższy SIL dla danej architektury podsystemu,
- PFH_d - prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę,

wówczas SIL całego systemu jest wyznaczany z uwzględnieniem szeregowego połączenia wszystkich podsystemów:

$$PFH_d = PFH_{d1} + PFH_{d2} + ... + PFH_{dn} + PTE \quad (5)$$

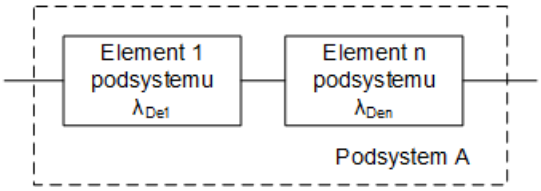
gdzie: PTE - prawdopodobieństwo niebezpiecznego błędu transmisji W tabeli 10 przedstawiono poziomy SIL w zależności od sumarycznej wartości PFH_d.

Tab. 10. Sprawdzanie wymaganego SIL [14]

SIL	PFH_d
1	≥ 10^{-6} to <10^{-5}
2	≥ 10^{-7} to <10^{-6}
3	≥ 10^{-8} to <10^{-7}

Następnie należy sprawdzić, czy SIL całego systemu jest nie mniejszy niż docelowy SIL wyznaczony z pomocą tabeli 9. Jeśli ten warunek nie jest spełniony wówczas należy dokonać zmian konstrukcyjnych i całą procedurę powtórzyć.

W sytuacji, kiedy nie jest znany SIL któregoś z podsystemów, niezbędne jest jego wyznaczenie. W tym celu należy określić architekturę logiczną podsystemu, przy czym zdefiniowano cztery ich rodzaje (A, B, C, D). Podsystemowe architektury logiczne z towarzyszącymi wzorami przedstawiono na rysunkach od 5 do 8.

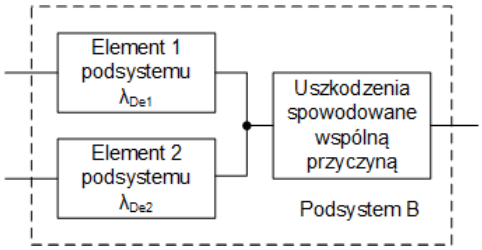


Rys. 5. Architektura logiczna podsystemu typu A [14]

$$\lambda_{DssA} = \lambda_{De1} + ... + \lambda_{Den}$$
$$PFH_{DssA} = \lambda_{DssA} \times 1h \quad (6)$$

λ_D jest intensywnością uszkodzeń niebezpiecznych. λ_{DssA}, jest intensywnością uszkodzeń niebezpiecznych podsystemu A. Jest to suma intensywności uszkodzeń poszczególnych elementów: e_1, e_2, ..., e_n. Średnią częstotliwość uszkodzeń niebezpiecznych PFH_{DssA} wyznacza się dla 1 godziny. λ można określić dla każdego komponentu podsystemu, używając następujących formuł:
$\lambda = 1/MTTF$ (elementy elektroniczne),
$\lambda = 0{,}1*C/B_{10}$ (elementy elektromechaniczne).

Rysunek 6 pokazuje pojedynczy podsystem odporny na błędy bez funkcji diagnostycznej.

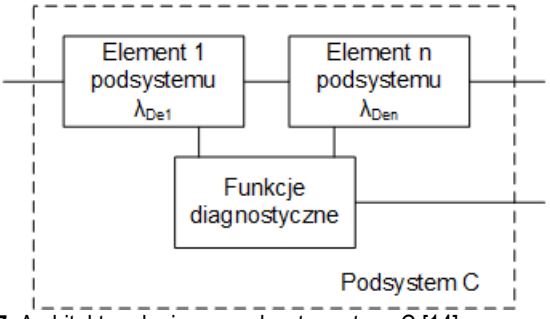


Rys. 6. Architektura logiczna podsystemu typu B [14]

$$\lambda_{DssB} = (1-\beta)^2 \cdot \lambda_{De1} \cdot \lambda_{De2} \cdot T_1 + \beta \cdot (\lambda_{De1} + \lambda_{De2})/2$$
$$PFH_{DssB} = \lambda_{DssB} \times 1h \quad (7)$$

gdzie β - współczynnik wrażliwości na uszkodzenia spowodowane wspólną przyczyną, T_1 - odstęp między testami sprawdzającymi lub czasem życia (w zależności od tego, która z wartości jest mniejsza).

Rysunek 7 pokazuje funkcjonalną reprezentację układu odpornego na błędy z funkcją diagnostyczną. Pokrycie diagnostyczne służy do zmniejszenia prawdopodobieństwa wystąpienia niebezpiecznych awarii sprzętu. Testy diagnostyczne są wykonywane automatycznie.

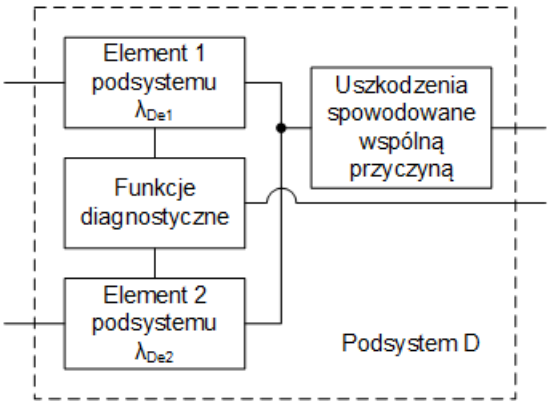


Rys. 7. Architektura logiczna podsystemu typu C [14]

$$\lambda_{DssC} = \lambda_{De1}(1-DC_1) + ... + \lambda_{Den}(1-DC_n)$$
$$PFH_{DssC} = \lambda_{DssC} \times 1h \quad (8)$$

gdzie: DC - pokrycie diagnostyczne dla każdego z elementów podsystemu.

Ostatni przykład architektury podsystemu pokazano na rysunku 8. Podsystem ten jest połączeniem równoległym dwóch elementów (jak na rysunku 6) i dodatkowo zawiera funkcję diagnostyczną.



Rys. 8. Architektura logiczna podsystemu typu D [14]

Jeśli elementy podsystemu są różne w każdym kanale, używana jest formuła (9). W przeciwnym razie używana jest formuła (10).

$$\lambda_{DssD} = (1-\beta)^2 \cdot \{[\lambda_{De1} \cdot \lambda_{De2} \cdot (DC_1 + DC_2)] \cdot T_2 / 2 + [\lambda_{De1} \cdot \lambda_{De2} \cdot (2 - DC_1 - DC_2)] \cdot T_1 / 2\} + \beta \cdot (\lambda_{De1} + \lambda_{De2}) / 2 \quad (9)$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

$$\lambda_{DssD} = (1-\beta)^2 \cdot \{[\lambda_{De}^2 \cdot 2 \cdot DC] \cdot T_2 / 2 + [\lambda_{De}^2 \cdot (1 - DC)] \cdot T_1\} + \beta \cdot \lambda_{De} \quad (10)$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

gdzie: T_2 – odstęp między testami diagnostycznymi

Podsumowanie

Bezpieczeństwo systemów automatyki przemysłowej staje się przedmiotem coraz większej uwagi. Dlatego też istotne jest rozwijanie metod ocena poziomu bezpieczeństwa oraz wybór możliwości, a także skutecznych sposobów wpływania na jego poziom. Autorzy artykułu przedstawili koncepcję oceny ryzyka systemów automatyki przemysłowej. Szczegółowo zostały omówione dwie koncepcje zapewnienia bezpieczeństwa przez układy automatyki tj. metoda wyznaczania PL (Performance Level) oraz SIL (Safety Integrity Level).

Bibliografia:

1. Bornemann A., Froese Y., Landi, L. et al., Probabilities in safety of machinery-Part 1: Risk profiling and farmer matrix, Safety and Reliability: Methodology and Applications, CRC Press, pp. 1933-1942, 2015.
2. Bornemann A., Froese Y., Landi L. et al., Probabilities in safety of machinery-Part 2: Theoretical and practical de-sign, Safety and Reliability: Methodology and Applications, CRC Press, pp. 1943-1950, 2015.
3. Kornaszewski M., Chrzan M., Olczykowski Z., Implementation of New Solutions of Intelligent Transport Systems in Railway Transport in Poland, Book Series: Communications in Computer and Information Science, Volume 715, pp. 282-292, 2017.
4. Lewinski A., Perzyński T., The Reliability and Safety of Railway Control Systems Based on New Information Technologies, Book Series: Communications in Computer and Information Science, Volume 104, pp. 427-433, 2010.
5. Łukasik Z., Nowakowski W., Kuśmińska-Fijałkowska A., Zarządzanie bezpieczeństwem infrastruktury krytycznej, Logistyka 4/2014, str. 758-763, 2014.
6. Łukasik Z., Nowakowski W., Zarządzanie bezpieczeństwem w transporcie kolejowym, Infrastruktura Transportu, nr 6/2013, str. 46-48, 2013.
7. Nowakowski W., Diagnostyka systemów automatyki kolejowej jako metoda poprawy bezpieczeństwa. Wydawnictwo Uniwersytetu Technologiczno-Humanistycznego im. K. Pułaskiego w Radomiu. Seria Monografie, Nr 218. Radom 2018.
8. Nowakowski W., Bojarczak P., Łukasik Z., Verification and Validation of Railway Control Systems Using an Expert System. In: Kováčiková T., Buzna Ľ., Pourhashem G., Lugano G., Cornet Y., Lugano N. (Eds.), Intelligent Transport Systems – From Research and Development to the Market Uptake (INTSYS 2017), Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol 222, pp. 43-50, Springer, Cham, 2018.
9. Nowakowski W., Ciszewski T., Łukasik Z., Metody oceny wpływu czynnika ludzkiego na bezpieczeństwo w transporcie. Autobusy: technika, eksploatacja, systemy transportowe, 6/2018, str. 180-184, 2018.
10. Nowakowski W., Ciszewski T., Łukasik Z., The Human as the Weakest Link in Ensuring Technical Safety. Proceedings of the 17th International Scientific Conference Globalization and Its Socio-Economic Consequences, Rajecke Teplice, Slovakia, Part IV, pp. 1788-1795, 2017.
11. Nowakowski W., Łukasik Z., Bojarczak P., Technical safety in the process of globalization, Proceedings of the 16th International Scientific Conference Globalization and Its Socio-Economic Consequences, Rajecke Teplice, Slo-vakia, 2016, Part IV, pp. 1571-1578, 2016.
12. Nowakowski W., Łukasik Z., Łukomski K., Diagnostyka urządzeń sterowania ruchem kolejowym. Autobusy: technika, eksploatacja, systemy transportowe, 6/2018, str. 632-635, 2018.
13. Piggin R., What's happening with machine safety stand-ards and networks?, Assembly Automation, Volume 26, Issue 2, pp. 104-110, 2006.
14. PN-EN 62061 - Bezpieczeństwo maszyn - Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.
15. PN EN ISO 13849-1 - Bezpieczeństwo maszyn - Elementy systemów sterowania związane z bezpieczeństwem.
16. Ruud S., Skjetne R., Verification and Examination Management of Complex Systems, Modeling Identification and Control, Volume 35, Issue 4, pp. 333-346, 2014.

Methods for assessing the safety of industrial automation systems

Industrial automation as the machine control section handling the automation of generating processes and technological processes, plays a significant role in economy. In the contemporary world it is difficult to imagine a modern plant without robotic assembly lines. This progress is connected to the need of ensuring safety. The significance of security in the industry is constantly raising and naturally concerns also the industrial automation. It is reflected in the regulations, including, among others, normative documents. This article presents methods of conducting verification of industrial automation systems basing on two basic parameters, which are: the level of ensuring Performance Level and the level of Safety Integrity Level.

Keywords: safety, PL, SIL, industrial automation.

Autorzy:

dr hab. inż. **Waldemar Nowakowski** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, w.nowakowski@uthrad.pl

prof. dr hab. inż. **Zbigniew Łukasik** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, z.lukasik@uthrad.pl

mgr inż. **Wojciech Bukalski** – eSeRKa, wojciech.bukalski@eserka.pl