Tomasz BARNERT, Kazimierz KOSMOWSKI, Marcin ŚLIWIŃSKI
POLITECHNIKA GDAŃSKA, WYDZIAŁ ELEKTROTECHNIKI I AUTOMATYKI, KATEDRA AUTOMATYKI

Analiza bezpieczeństwa funkcjonalnego i ochrony informacji w rozproszonych systemach komputerowych pełniących funkcje sterowania i zabezpieczeń

Mgr inż. Tomasz BARNERT

Absolwent Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej na kierunku Automatyka i Robotyka ze specjalnością Automatyka i Informatyka Techniczna (2004). Słuchacz Studium Doktoranckiego na tym wydziale od 2005 roku. Zajmuje się zagadnieniami bezpieczeństwa funkcjonalnego programowalnych systemów sterowania i zabezpieczeń oraz ochrony informacji w przemysłowych sieciach komputerowych.

e-mail: t.barnert@ely.pg.gda.pl

Dr hab. inż. Kazimierz KOSMOWSKI

W 1972 roku ukończył studia na Wydziale Elektrycznym Politechniki Gdańskiej. W roku 1981 obronił rozprawę doktorską, a rozprawę habilitacyjną w 2003 roku. Profesor nadzw. Politechniki Gdańskiej. Od 2006 roku pełni funkcję Kierownika Katedry Automatyki. Zajmuje się zagadnieniami niezawodności i bezpieczeństwa systemów technicznych, bezpieczeństwa funkcjonalnego programowalnych systemów sterowania i automatyki zabezpieczeniowej oraz niezawodności człowieka – operatora.

e-mail: k.kosmowski@ely.pg.gda.pl

Dr inż. Marcin ŚLIWIŃSKI

W 2001 roku ukończył studia na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej. W roku 2006 uzyskał stopień doktora nauk technicznych w zakresie automatyki i robotyki. Od 2006 roku pracuje na stanowisku adiunkta w Katedrze Automatyki na Wydziale Elektrotechniki i Automatyki Politechniki Gdańskiej. Zajmuje się zagadnieniami bezpieczeństwa funkcjonalnego oraz badaniem i modelowaniem probabilistycznym nadmiarowych systemów sterowania i zabezpieczeń.

e-mail: m.sliwinski@ely.pg.gda.pl

Streszczenie

W niniejszym artykule przedstawiona została problematyka związana z analizą bezpieczeństwa funkcjonalnego rozproszonych systemów sterowania i automatyki zabezpieczeniowej z uwzględnieniem zagadnień ochrony informacji. Powinny być one rozpatrywane w sposób zintegrowany w zależności od rodzaju komunikacji stosowanej do transmisji danych. W tym celu zaproponowano podział analizowanych systemów na trzy kategorie. Zaproponowane podejście zilustrowano na przykładzie rozproszonego systemu monitoringu i sterowania, który może korzystać z różnych kanałów przesyłu informacji.

Słowa kluczowe: bezpieczeństwo funkcjonalne, ochrona informacji, poziom nienaruszalności bezpieczeństwa SIL, poziom uzasadnionego zaufania EAL.

Functional safety and security analysis in the distributed computer systems performing the control and protection functions

Abstract

The aim of this paper is to present some issues of the functional safety analysis of the distributed control, monitoring and protection systems including information security aspects. These aspects should be considered in an integrated way depending on the types of communication channels used. The classification of analyzed systems into three categories is proposed. The conventional functional safety assessment based on IEC 61508 and integrated with some information security aspects, based on ISO/IEC 15408, are presented. Proposed approach is illustrated by an example of distributed, monitoring, control and protection system using different communication channels.

Keywords: functional safety, information security, safety integrity level SIL, evaluation assurance level EAL.

1. Wprowadzenie

Zagadnienia związane z analizą bezpieczeństwa funkcjonalnego systemów elektrycznych, elektronicznych i programowalnych elektronicznych (E/E/PE) przedstawiono w normie międzynarodowej IEC 61508 [1], która ma charakter ogólny (dotyczy różnych zastosowań) oraz normach sektorowych, np. IEC 61511 [2], opracowanej z uwzględnieniem specyfiki przemysłu procesowego.

Ostatnio podkreśla się znaczenie ochrony informacji w systemach komputerowych, szczególnie tych, które pełnią odpowiedzialne funkcje monitorowania, sterowania i zabezpieczeń. Ogólne wymagania dotyczące zagadnień ochrony informacji w takich systemach zawarte są w normie międzynarodowej ISO/IEC 15408 [3].

Istnieje potrzeba integrowania zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji [4, 5, 6]. W niniejszym artykule przedstawiono propozycję integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji z uwzględnieniem zaproponowanej klasyfikacji systemów rozproszonych. Przyjęto, że wymienione normy stanowią dobre odniesienie do dalszych badań zorientowanych na zintegrowaną analizę, łączącą aspekty bezpieczeństwa funkcjonalnego i ochrony informacji (*safety & security*).

2. Aspekty bezpieczeństwa funkcjonalnego i ochrony informacji w systemach programowalnych

2.1. Wymagania dotyczące bezpieczeństwa funkcjonalnego

W analizie bezpieczeństwa funkcjonalnego systemu E/E/PE istotne znaczenie ma określenie wymaganego poziomu nienaruszalności bezpieczeństwa SIL (*safety integrity level*). Poziom ten wynika z oceny ryzyka. Ocenę ryzyka można przeprowadzić stosując metodę o charakterze jakościowym za pomocą grafu ryzyka lub metodę ilościową. Średnie prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie P_{FDavg} przez system E/E/PE wyznacza się na podstawie wymaganego zmniejszenia ryzyka do poziomu tolerowanego według wzoru [1, 7]:

$$P_{FDavg} \le R_t / R_{np} = r^R \tag{1}$$

gdzie: R_{np} – miara ryzyka (rozumiana jako iloczyn częstości i strat związanych ze zdarzeniem awaryjnym) bez zastosowania systemu zabezpieczeniowego; R_t - ryzyko tolerowane; r^R - względna redukcja ryzyka.

W normach [1, 2] definiuje się cztery poziomy nienaruszalności bezpieczeństwa (SIL). Mają one związek z rodzajem pracy systemu E/E/PE. Poszczególnym SIL systemu odpowiadają ilościowe kryteria probabilistyczne, które zestawiono w tab. 1. Występuje w niej średnie prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie (P_{FDavg}). Kryteria te są przedziałami liczbowymi.

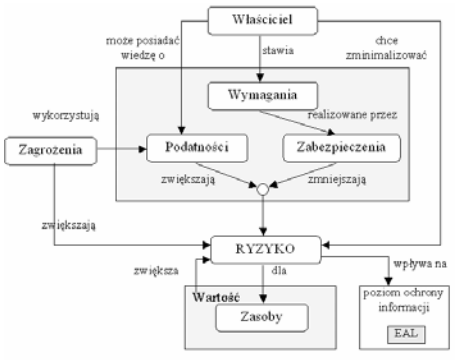
Weryfikowanie SIL projektowanego systemu E/E/PE powinno być przeprowadzane metodą ilościową na podstawie odpowiedniego modelu probabilistycznego. W przypadku braku danych niezawodnościowych norma [1] dopuszcza stosowanie metody jakościowej polegającej na „zwijaniu" schematu blokowego analizowanego systemu związanego z bezpieczeństwem.

Tab. 1. Poziomy nienaruszalności bezpieczeństwa SIL i przedziałowe kryteria probabilistyczne dla systemów E/E/PE według IEC 61508
Tab. 1. Safety integrity levels (SILs) and the interval probabilistic criteria for E/E/PE systems according to IEC 61508

SIL	Przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie P_{FDavg}
4	$[10^{-5}, 10^{-4})$
3	$[10^{-4}, 10^{-3})$
2	$[10^{-3}, 10^{-2})$
1	$[10^{-2}, 10^{-1})$

2.2. Wymagania dotyczące ochrony informacji

Koncepcję analizy zagadnień i oceny ryzyka, związaną z ochroną informacji, zawarto w dokumencie normatywnym ISO/IEC 15408, mającym szczególne znaczenie przy certyfikacji przewidzianych zabezpieczeń w systemie komputerowym. Wprowadza on pojęcie poziomów uzasadnionego zaufania EAL (*evaluation assurance level*). Poziomy EAL stanowią zbiór wymagań odnoszących się do całkowitego cyklu życia produktu, jakim jest system informatyczny. Zdefiniowano 7 poziomów EAL, przy czym im wyższy poziom tym mniejsza możliwość wystąpienia negatywnych skutków niekorzystnego zdarzenia. Zakres skutków zależy od podatności systemu. Poziomem potwierdzającym spełnienie podstawowych wymagań ochrony informacji jest EAL 1, który jest najtańszy w implementacji. Najwyższy poziom EAL 7 jest najbardziej rygorystyczny, a związane z nim rozwiązania ochrony informacji są znacznie droższe w implementacji. Aby osiągnąć odpowiedni poziom uzasadnionego zaufania należy spełnić określone wymagania. Większość z tych wymagań odnosi się do dokumentacji i analizy projektu informatycznego, testów funkcjonalności, czy też wnikliwych testów poprawnego działania. Istotę ochrony informacji oraz czynniki wpływające na poziom tej ochrony przedstawiono na rys. 1.



Rys. 1. Koncepcja ochrony informacji i relacje
Fig. 1. Information security concept and relationships

Idea poziomów EAL jest w pewnym sensie podobna do idei poziomów nienaruszalności bezpieczeństwa SIL, które są stosowane w ocenie bezpieczeństwa funkcjonalnego. Wymagania dla systemu informatycznego posiadającego odpowiedni poziom EAL zestawiono syntetycznie na podstawie ISO/IEC 15408 w tab. 2.

Tab. 2. Poziomy uzasadnionego zaufania EAL [3]
Tab. 2. Evaluation assurance levels (EALs)

Poziom	Charakterystyka rozwiązania na danym poziomie
EAL 1	przetestowany funkcjonalnie
EAL 2	przetestowany strukturalnie
EAL 3	przetestowany metodycznie i sprawdzony
EAL 4	przetestowany, zaprojektowany i zweryfikowany metodycznie
EAL 5	zaprojektowany i przetestowany pół formalnie
EAL 6	przetestowany, zaprojektowany i zweryfikowany pół formalnie
EAL 7	przetestowany, zaprojektowany i zweryfikowany formalnie

Dzięki certyfikatowi określającemu spełnienie przez system informatyczny danego EAL użytkownik ma możliwość określenia czy system, który chce użytkować jest wystarczająco bezpieczny w konkretnym zastosowaniu. Czynnikami wpływającymi na określany poziom ochrony informacji mogą być między innymi zdarzenia spowodowane przez czynniki naturalne (np. powódź, wyładowania atmosferyczne), przyczyny techniczne (np. zanik zasilania, przegrzanie, zwarcie) lub nieprzyjazne działania człowieka (np. ataki hakerów, wirusy, akty sabotażu) [8]. W takich systemach należy chronić: dane, oprogramowanie, instalacje sieciowe, itd.

3. Propozycja integracji rozwiązań bezpieczeństwa funkcjonalnego z ochroną informacji

3.1. Klasyfikacja rozproszonych systemów monitorowania, sterowania i zabezpieczeń

Klasyfikacja skomputeryzowanych systemów monitorowania, sterowania i zabezpieczeń jest podstawą do integrowania koncepcji bezpieczeństwa funkcjonalnego i ochrony informacji. Proponuje się podział takich systemów na trzy kategorie [6]:

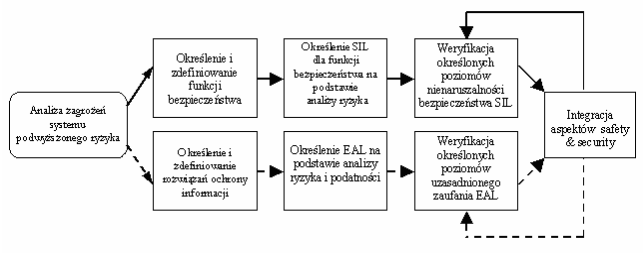
I. Systemy zainstalowane na obiektach krytycznych (np. rafinerie, instalacje chemiczne), wykorzystujące wyłącznie wewnętrzne kanały przesyłu informacji (np. sieć lokalna LAN),
II. Systemy zainstalowane na krytycznych obiektach skupionych lub rozproszonych (np. rurociągi, gazociągi, system energetyczny), w których istnieją wewnętrzne kanały transmisji informacji i mogą być również wykorzystywane zewnętrzne kanały przesyłania danych,
III. Systemy zainstalowane na obiektach i w systemach infrastruktury krytycznej (np. systemy transportowe - kolej, lotnictwo, transport morski, system ochrony oraz monitoringu w ruchu drogowym), w których wykorzystywane są wyłącznie zewnętrzne kanały transmisji danych.

Proponowana klasyfikacja opiera się na identyfikacji sposobu transmisji danych pomiędzy poszczególnymi elementami systemu monitorowania, sterowania i zabezpieczeń. Jeżeli ważne dane są przesyłane wyłącznie poprzez sieć wewnętrzną systemu wówczas rozważany system należy do kategorii I. Jeśli przy transferze danych mogą być wykorzystywane również zewnętrzne kanały (np. stacjonarna sieć telefoniczna, gsm, łączność radiowa lub satelitarna) wówczas system należy do II kategorii. Natomiast w przypadku wyłącznego wykorzystywania zewnętrznych kanałów transmisji danych system zalicza się do III kategorii.

3.2. Analiza aspektów bezpieczeństwa funkcjonalnego i ochrony informacji

Jak wspomniano, w procesie projektowania i użytkowania programowalnego systemu sterowania i automatyki zabezpieczenio-

wej wykorzystującego różne kanały przesyłu informacji powinny być rozpatrzone aspekty bezpieczeństwa funkcjonalnego i ochrony informacji. Ideę integracji tych dwóch aspektów przedstawiono na rys. 2.

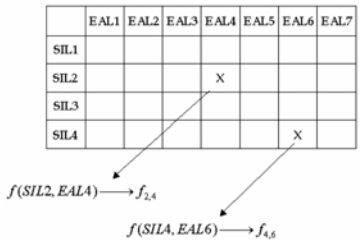


Rys. 2. Idea integracji rozwiązań bezpieczeństwa funkcjonalnego i ochrony informacji
Fig. 2. Idea of integration of the functional safety solutions and information security integration

Wymaga ona dalszych badań, których rezultatem będą odpowiednie wskazania wspomagające projektowanie i użytkowanie rozproszonych systemów programowalnych.

3.3. Propozycja integracji aspektów bezpieczeństwa funkcjonalnego i ochrony informacji

W oparciu o przedstawioną wcześniej klasyfikację systemów monitorowania, sterowania i zabezpieczeń w obiektach i systemach infrastruktury krytycznej zaproponowano podejście integrowania analiz związanych z bezpieczeństwem funkcjonalnym i ochroną informacji. W przypadku systemów I kategorii, wykorzystujących wyłącznie wewnętrzne kanały transmisji danych (np. Ethernet, światłowód, itp.), proponuje się przeprowadzanie niezależnych od siebie analiz bezpieczeństwa funkcjonalnego i ochrony informacji. Gdyby w systemie występowało powiązanie z siecią zewnętrzną np. Internet, wówczas system należy rozpatrywać jako kategorii II. W przypadku, gdy dane przesyłane są z wykorzystaniem zewnętrznych kanałów informacji (system II lub III kategorii) pojawia się problem zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji. Na rys. 3. przedstawiona jest idea określenia wymagań w ramach zintegrowanej analizy z uwzględnieniem poziomów SIL oraz EAL [6].



Rys. 3. Określanie wymagań w ramach zintegrowanej analizy bezpieczeństwa funkcjonalnego z uwzględnieniem zagadnień ochrony informacji dla systemów II i III kategorii
Fig. 3. Determining requirements within integrated safety and security analysis with regard to information security for systems of II and III category

Każdy system należący do II lub III kategorii musi posiadać zdefiniowany poziom nienaruszalności bezpieczeństwa SIL oraz poziom uzasadnionego zaufania EAL. W tym wypadku poziom EAL jest związany z typem ochrony danych przesyłanych zewnętrznymi kanałami. Z połączenia tych dwóch parametrów powstaje dwuargumentowa funkcja wymagań dla analizowanego systemu. Zakładając, że poziom EAL odnosi się do całego sytemu, natomiast poziom SIL do konkretnych funkcji bezpieczeństwa realizowanych przez system sterowania i/lub zabezpieczeniowy, funkcja dwuparametrowa $f_{i,j}$ jest wykorzystywana przy weryfikacji określonych wymagań (zwłaszcza poziomu SIL) zaprojektowanego systemu monitorowania, sterowania i zabezpieczeń.

4. Przykład zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji

Przykładowy system monitorowania, sterowania i zabezpieczeń przedstawiono na rys. 4. System składa się ze sterowników programowalnych PLC, czujników, elementów wykonawczych oraz stacji operatorskich w ramach systemu nadrzędnej kontroli i akwizycji danych SCADA (*supervisory control and data acquisition*). Niektóre z podsystemów mogą mieć strukturę nadmiarową, co związane jest z zapewnieniem wymaganego poziomu nienaruszalności bezpieczeństwa SIL.

Rys. 4. System monitorowania, sterowania i zabezpieczeń z różnymi kanałami komunikacji
Fig. 4. Monitoring, control and protection system with different communication channels

Biorąc pod uwagę rodzaj wykorzystywanego kanału przesyłu informacji pomiędzy sterownikiem programowalnym PLC a stacją operatorską, przedstawiono kilka przykładów zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji dla obiektu krytycznego, jakim jest gazociąg. Rozpatrzone zostały trzy przypadki dla trzech kategorii rozproszonych systemów monitorowania, sterowania i zabezpieczeń (I, II, III kategorii).

Na podstawie analizy ryzyka przeprowadzonej dla danego obiektu, określono metodą ilościową wymagania dla przykładowego systemu zabezpieczeń na poziomie SIL3 ($P_{FDavg} = 3.24 \cdot 10^{-4}$).

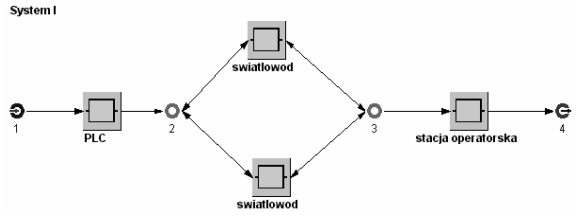
W tab. 3 zawarto specyfikację zintegrowanych wymagań, obejmujących aspekty bezpieczeństwa funkcjonalnego i ochrony informacji w postaci dwuparametrowej funkcji $f_{i,j}$. Przykładowy system sterowania i zabezpieczeń gazociągu powinien spełniać poziom nienaruszalności bezpieczeństwa SIL3. Podane w tab. 3 poziomy EAL są przyjęte przykładowo. Służą one pokazaniu, że wraz z wprowadzaniem zewnętrznych kanałów komunikacji do systemu wzrasta możliwość wystąpienia niepożądanego wpływu otoczenia na działanie systemu. Dlatego należy zwiększyć poziom ochrony informacji w rozważanych systemach.

Tab. 3. Określenie wymagań poziomów SIL i EAL dla systemów kategorii I, II, III
Tab. 3. Determining SIL and EAL for systems of category I, II and III

System	Wymagania projektowe	
I	SIL3	EAL2
II	$f_{3,4}$	
III	$f_{3,5}$	

W przypadku systemu I kategorii tj. takiego, w którym nie występują zewnętrzne kanały komunikacji, a co za tym idzie nie istnieje możliwość ingerencji z zewnątrz do danych dotyczących stanu obiektu, wymagania projektowe potraktowano oddzielnie.

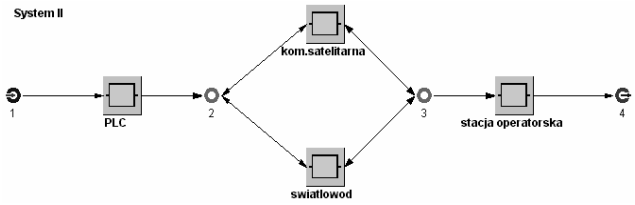
Na rys. 5. przedstawiono system I kategorii, w którym wykorzystywane są wyłącznie wewnętrzne kanały przesyłu danych (sieć światłowodowa z redundancją kanałów transmisji danych).



Rys. 5. Przykład systemu monitorowania, sterowania i zabezpieczeń I kategorii
Fig. 5. An example of monitoring, control and protection system of I category

W tym przypadku wymagania dotyczące poziomów SIL oraz EAL są określane niezależnie. Przedstawiony system na podstawie przeprowadzonej wcześniej analizy ryzyka powinien spełniać wymagania SIL 3 oraz EAL 2. Poziom EAL jest w danym przypadku związany z komunikacją, w której dane nie mogą zostać przechwycone przez użytkowników nie posiadających autoryzacji, dlatego też poziom uzasadnionego zaufania EAL może być niski np. EAL 2 – przetestowany strukturalnie (tab. 2).

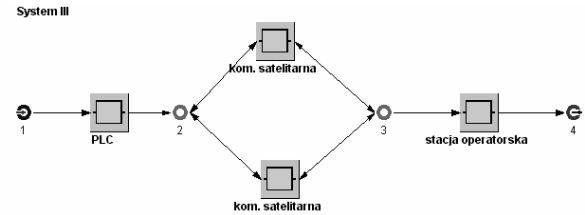
Drugi przykład (rys. 6) przedstawia system II kategorii. W transferze danych pomiędzy sterownikiem a stacją operatorską wykorzystywana jest wewnętrzna sieć światłowodowa oraz zewnętrzna komunikacja satelitarna. W danym przypadku rezultatem zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji jest dwuparametrowa funkcja $f_{3,4}$ łącząca poziomy SIL 3 oraz EAL 4.



Rys. 6. Przykład systemu monitorowania, sterowania i zabezpieczeń II kategorii
Fig. 6. An example of monitoring, control and protection system of II category

Poziom uzasadnionego zaufania określono jako EAL 4, ponieważ ważne dane mogą być przesyłane z wykorzystaniem łączności satelitarnej. Dlatego też nieautoryzowany dostęp jest technicznie możliwy. Proponowany poziom uzasadnionego zaufania EAL 4 oznacza, że system informatyczny obsługujący kanały komunikacyjne został przetestowany, zaprojektowany i zweryfikowany metodycznie (tab. 2).

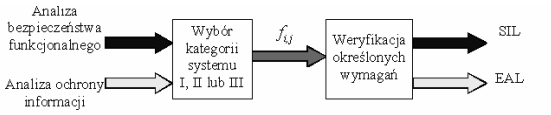
Ostatni przykład (rys. 7) przedstawia system III kategorii, z redundancją kanałów transmisji danych pomiędzy sterownikiem PLC a stacją operatorską, z wykorzystaniem komunikacji satelitarnej.



Rys. 7. System monitorowania, sterowania i zabezpieczeń III kategorii
Fig. 7. Monitoring, control and protection system of III category

W tym przykładzie funkcja $f_{3,5}$ wskazuje na wymagania stawiane systemowi przy wykorzystaniu wyłącznie zewnętrznych kanałów komunikacji (łączność satelitarna). Ryzyko nieautoryzowanego dostępu do przesyłanych danych (np. atak hakerów, sabotaż, szpiegostwo przemysłowe itd.) jest duże, a ochrona informacji stanowi bardzo ważny czynnik dla ogólnego stanu bezpieczeństwa systemu. Z tego powodu poziom uzasadnionego zaufania został określony jako EAL5 (tab. 2), który wskazuje na znaczną odporność systemu na potencjalne ataki z zewnątrz.

Na rys. 8 przedstawiony został sposób zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji w rozproszonych systemach komputerowych poprzez określenie wymagań w postaci dwuparametrowej funkcji $f_{i,j}$, która brana jest pod uwagę w procesie weryfikacji SIL.



Rys. 8. Wyznaczanie funkcji $f_{i,j}$ oraz weryfikacja wymagań
Fig. 8. Determining of function $f_{i,j}$ and verification of requirements

W zintegrowanej analizie bezpieczeństwa funkcjonalnego i ochrony informacji dla rozproszonych systemów monitorowania, sterowania i zabezpieczeń istotnym zagadnieniem jest weryfikacja określonych uprzednio wymagań dotyczących SIL oraz EAL. Ponieważ poziomy SIL odnoszą się do konkretnych funkcji bezpieczeństwa, a poziomy EAL do ochrony informacji całego systemu monitorowania, sterowania i zabezpieczeń, można założyć, że niepożądane zdarzenia i działania z zewnątrz przy niskim poziomie ochrony informacji EAL mogą wpływać na niewypełnienie przez system funkcji bezpieczeństwa. Tak więc niski poziom uzasadnionego zaufania EAL przy weryfikacji określonego poziomu SIL może skutkować jego obniżeniem. W tab. 4 przedstawiono propozycję takiej zależności dla systemów II oraz III kategorii. W nawiasie znajdują się zmodyfikowane poziomy SIL dla systemu III kategorii.

Tab. 4. Wynikowe SIL z uwzględnieniem poziomu EAL dla systemów II kategorii (III kategorii)
Tab. 4. SIL that can be claimed for determined EAL for systems of II category (III category)

Określony		Weryfikowany SIL dla systemu II kat. (III kat.)			
ochrona informacji		*bezpieczeństwo funkcjonalne*			
EAL	poziom	1	2	3	4
1	podstawowy	- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
2		- (-)	SIL1 (-)	SIL2 (1)	SIL3 (2)
3	średni	SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4		SIL1 (-)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	wysoki	SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
6		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
7		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)

Biorąc pod uwagę rozważany powyżej system monitorowania, sterowania i zabezpieczeń kategorii II (rys. 6) określono dla niego wymagania w postaci funkcji $f_{3,4}$. Na podstawie tej funkcji przeprowadzona została weryfikacja wymagań SIL, w wyniku której stwierdza się, że system ten spełnia wymagania dla poziomu SIL 3 (tab. 4).

5. Podsumowanie

Przy projektowaniu rozproszonych skomputeryzowanych systemów sterowania, zabezpieczeń i monitoringu powinny być

uwzględnione wszystkie potencjalne zagrożenia, wynikające z zastosowania różnych kanałów transmisji danych. W niniejszym artykule dokonano klasyfikacji systemów w celu przeprowadzenia zintegrowanej analizy bezpieczeństwa funkcjonalnego i ochrony informacji. Przyszłe prace badawcze powinny być skierowane na projektowanie systemów z bazą wiedzy wspomagających określanie poziomów SIL i EAL i ich weryfikację w sposób zintegrowany na podstawie analiz ryzyka uwzględniających systematyczną ocenę czynników ryzyka.

6. Literatura

[1] IEC 61508:1998: Functional safety of electrical/ electronic/ programmable electronic safety-related systems, Parts 1-7. International Electrotechnical Commission (IEC), 1998.

[2] IEC 61511:2000: Functional safety: Safety Instrumented Systems for the process industry sector. Parts 1-3. International Electrotechnical Commission.

[3] ISO/IEC 15408:1999: Information technology — Security techniques — Evaluation criteria for IT security Part 1÷3.

[4] Grotan T.O.: Secure safety in remote operations, ESREL, Estoril, 2006.

[5] Kosmowski K.T.: Functional safety and security management in critical systems, TEHOSS 2005, pp. 323/332, Gdansk, 2005.

[6] Kosmowski K.T., Śliwiński M., Barnert T.: Functional safety and security assessment of the control and protection systems, ESREL, Estoril, 2006.

[7] Kosmowski K.T.: Functional safety concept for hazardous systems and new challenges, Journal of Loss Prevention in the Process Industries 19(2006), pp. 298/305, 2006.

[8] Shriver R., Wold G.: Risk Analysis Techniques, Disaster Recovery Journal, vol. 7/3 1997.

Artykuł recenzowany

KONFERENCJE NAUKOWO-TECHNICZNE

KONGRES METROLOGII

Drogie Koleżanki i Koledzy Metrolodzy,

Serdecznie zapraszamy Państwa do udziału w kolejnym Kongresie Metrologii, który odbędzie się w dniach od 9 do 13 września 2007 roku w Krakowie. Będziecie Państwo Gośćmi Akademii Górniczo-Hutniczej im. Stanisława Staszica, która w roku 2009 obchodzić będzie 90-lecie istnienia. Organizatorem Kongresu jest Katedra Metrologii na Wydziale Elektrotechniki Automatyki Informatyki i Elektroniki, której także **"stuknęło" już 50 lat**.

Hasło Kongresu brzmi: **Metrologia - narzędziem poznania i drogą rozwoju**. W tematyce Kongresu chcemy szczególnie zaakcentować: nowe kierunki rozwoju metrologii, nowe narzędzia poznawania mierzonych procesów, obiektów i sygnałów oraz nowe obszary zastosowań metrologii. W naszym zamiarze nowość oraz interdyscyplinarność i oryginalność tematyki powinna być głównym wyróżnikiem naszych prac, które po recenzjach opublikujemy w materiałach Kongresu. Liczymy na mobilizację Państwa energii w przygotowaniu interesujących i odważnych tematów wystąpień oraz na Państwa udział w ożywionej i rzeczowej dyskusji. Tematyka Kongresu przedstawia się następująco:

I. Współczesne problemy metrologii
1. Mikrosystemy pomiarowe; zagadnienia sprzętowe i projektowe, nowe technologie
2. Systemy rozproszone i bezprzewodowe; interfejsy i protokoły, kompresja i transmisja danych
3. Fuzja danych pomiarowych; identyfikacja modeli złożonych procesów i obiektów
4. Metody i algorytmy analizy danych
5. Nowe problemy przetwarzania a/c; granice szybkości i rozdzielczości
6. Czujniki i przetworniki z modulacją światła, czujniki elektrochemiczne i inne

II. Nowe metody pomiarowe w zastosowaniach
1. Pomiary biomedyczne; metody diagnostyki i analizy medycznej
2. Pomiary konwencjonalnych i nie konwencjonalnych źródeł i przetworników energii
3. Pomiary technologiczne i transportowe; obiekty "inteligentne"
4. Pomiary środowiskowe; rozpoznawanie stanów zagrożenia
5. Pomiary i diagnostyka obiektów mechanicznych, pomiary akustyczne
6. Pomiary w zastosowaniach militarnych

III. Współczesne problemy podstaw metrologii; dydaktyka metrologii
1. Teoria i modelowanie systemów pomiarowych
2. Wzorce i wielkości odniesienia; pomiary dokładne, wzorcowanie i metrologia prawna
3. Pomiary kwantowe, wzorce kwantowe
4. Błędy, niepewności, wrażliwość
5. Dydaktyka metrologii; plany studiów, nowe treści w podręcznikach

Mamy nadzieję, że rozproszeni w różnych branżach znajdziemy chwilę czasu na spotkanie przy tematyce, która nas łączy. To jest główny cel, dla którego Kongres organizujemy.

Jest jednak i cel drugi, równie istotny. Ten cel - to Kraków, miasto stare i tajemnicze, po którym krążą duchy przeszłości i w którym mieszka geniusz tego Narodu. Chcemy dać Państwu okazję do dotknięcia ponad 600-letnich murów krakowskiej Almae Matris - wszak my wszyscy z Niej! Chcemy dać okazję do spaceru ulicami, po których chodził Kopernik oraz do chwili zadumy nad przeszłością w komnatach Wawelu.

Jest i cel trzeci, bo przecież nie tylko poważną strawą duchową człowiek, a zwłaszcza metrolog żyje. Zachęcamy Państwa do udziału w spotkaniach o charakterze towarzyskim.

Jesteśmy przekonani, że w ciągu tych dni kongresowych nudzić się Państwo nie będziecie. Przeciwnie - zyskacie Państwo nie tylko satysfakcję zawodową, obywatelską i towarzyską, ale i miłe wspomnienia.

Zatem - do zobaczenia!

Przewodniczący Komitetu Naukowego Kongresu Metrologii 2007
Prof. Michał Szyper

Przewodniczący Kongresu
Prof. Janusz Gajda