XXIV Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE 2014

Oddział Gdański PTETiS

WPŁYW POZIOMU OCHRONY INFORMACJI NA WYMAGANIA NIENARUSZALNOŚCI BEZPIECZEŃSTWA

Tomasz BARNERT[1], Emilian PIESIK[2], Marcin ŚLIWIŃSKI[3]

1. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: 58 347 14 35 fax: 58 347 24 87 e-mail: t.barnert@ely.pg.gda.pl
2. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: 58 347 14 35 fax: 58 347 24 87 e-mail: e.piesik@ely.pg.gda.pl
3. Politechnika Gdańska, ul. G. Narutowicza 11/12, 80-952 Gdańsk
   tel: 58 347 14 35 fax: 58 347 24 87 e-mail: m.sliwinski@ely.pg.gda.pl

Streszczenie: W referacie przedstawiono zagadnienia związane z etapem analizy i oceny ryzyka obiektu technicznego podwyższonego ryzyka. Opisano metody określania wymagań na nienaruszalność bezpieczeństwa SIL zidentyfikowanych funkcji bezpieczeństwa. Funkcje takie realizowane są przez systemy E/E/PE (BPCS i/lub SIS) i są częścią systemu bezpieczeństwa składającego się z wielu warstw zabezpieczeniowo-ochronnych. Zarówno w metodach jakościowych, jak i pół-ilościowych wyznaczenie wymaganego SIL opiera się na kilku podstawowych parametrach ryzyka. Są one związane z częstością wystąpienia zdarzenia awaryjnego oraz jego potencjalnymi konsekwencjami. W związku z tym, iż coraz częściej systemy techniczne budowane są w oparciu o architekturę rozproszoną, pojawiają się nowe zagrożenia, które do tej pory nie były uwzględnianie w analizach ryzyka. Mogą one mieć wpływ zarówno na zwiększenie częstości wystąpienia zdarzeń i scenariuszy awaryjnych, jak również mogą zwiększać prawdopodobieństwo niewypełnienia funkcji związanej z bezpieczeństwem na przywołanie. Oba te zagadnienia powinny być uwzględnione w procesie przypisania wymaganego poziomu nienaruszalności bezpieczeństwa do funkcji. Zaproponowano rozszerzenie stosowanych obecnie metod o aspekty związane z uwzględnieniem poziomu ochrony informacji systemu technicznego.

Słowa kluczowe: bezpieczeństwo funkcjonalne, SIL, ochrona informacji

1. WIADOMOŚCI OGÓLNE

1.1. Wprowadzenie

Na bezpieczeństwo systemu technicznego składa się wiele różnych aspektów. Wśród nich umiejscowić można dwa bardzo ważne ogniwa, które wpływać mogą bezpośrednio na stopień ryzyka występującego w badanym systemie. Są to bezpieczeństwo funkcjonalne, które należy traktować jako jeden z czynników zmniejszających ryzyko związane z działaniem systemu technicznego, oraz ochrona informacji.

Ważnym aspektem bezpieczeństwa obiektu przemysłowego jest zagadnienie ochrony informacji (w postaci ochrony danych, dokumentacji, dostępu do systemów informatycznych, sieci przewodowych i bezprzewodowych zarówno firmowych jak i przemysłowych, itp.) oraz dostępu (do terenów objętych zakazem wstępu, budynków, pomieszczeń służbowych, urządzeń, itp.). Tak szeroko pojęte zagadnienie wymaga również przeprowadzenia odpowiedniej analizy, która będzie miała za zadanie zidentyfikowanie potencjalnych zagrożeń występujących w analizowanym systemie bądź obiekcie, ocenę tego typu zagrożeń oraz zaproponowanie potencjalnych rozwiązań im przeciwdziałających.

W związku z tym, iż coraz częściej systemy techniczne (sterowania, bezpieczeństwa, itd.) wykorzystują infrastrukturę sieciową, rozbudowane systemy informatyczne, czy też teleinformatyczne, koniecznością staje się uwzględnienie ich potencjalnych podatności na zagrożenia w analizach (w tym przede wszystkim w analizach związanych z bezpieczeństwem funkcjonalnym) [1].

2. METODYKA OKREŚLANIA WYMAGAŃ SIL

2.1. Zagadnienie ochrony informacji w systemach technicznych

Analiza ryzyka odnosząca się do zagadnień ochrony informacji związana jest z kilkoma podstawowymi etapami, mającymi swoje odpowiedniki w analizie bezpieczeństwa funkcjonalnego. Pierwszym etapem, od którego należy rozpocząć analizę systemu technicznego pod względem ochrony jest identyfikacja zasobów, które są cenne dla przedsiębiorstwa i jednocześnie ich utrata wiązałaby się z możliwymi do oszacowania stratami. Zasobami takimi mogą być zarówno środki trwałe w postaci aktywów i pasywów firmy, takie jak np. infrastruktura, sprzęt, oprogramowanie, itp., jak również rzeczy trudniejsze do policzenia i wyceny, jak np. dane, informacje, wiedza pracowników, itp. Zakładając, że wymienione powyżej zasoby są cenne, powinny być chronione przez odpowiednio dobrane zabezpieczenia. Kolejnym krokiem w analizie ochrony jest identyfikacja zagrożeń przypisana do każdego zasobu oraz analiza podatności systemu na te zagrożenia. Na tym etapie należy przewidzieć, jakie są przyczyny (źródła) wystąpienia zidentyfikowanego zagrożenia oraz jak dane zagrożenie może wpłynąć na analizowany zasób. W nawiązaniu do teorii ochrony informacji można stwierdzić, iż straty związane z tego typu zagrożeniami można sklasyfikować w trzech kategoriach, tzn. utrata jawności,

utrata integralności oraz dostępności danych, informacji, itp. [6]. Mając zidentyfikowane podatności zasobów oraz zagrożenia z nimi związane należy przejść do etapu oceny ryzyka. Na tym etapie konieczne staje się oszacowania skutków wystąpienia zagrożenia, jak również prawdopodobieństwa jego zajścia. Na podstawie informacji, jak często dany zasób może być narażony na określone zagrożenie oraz sklasyfikowania skutków jego wystąpienia można przypisać wymagania, jakie będą stawiane systemowi ochrony. Po oszacowaniu poziomu ryzyka dla wszystkich zidentyfikowanych zagrożeń, pozostaje zaproponować pewne rozwiązania techniczne bądź organizacyjne, które będą miały na celu zredukowanie występującego ryzyka do poziomu akceptowalnego przez dane przedsiębiorstwo.

Kolejnym ważnym zagadnieniem związanym z analizami ochrony informacji jest klasyfikacja potencjalnych źródeł wystąpienia szkód w systemie technicznym. Źródła te związane mogą być z czterema kategoriami zagrożeń:

- naturalnymi,
- technicznymi,
- nieumyślnymi działaniami człowieka,
- celowymi działaniami człowieka.

Wszystkie cztery potencjalne źródła zagrożeń powinny być uwzględnione w kompleksowej analizie ochrony informacji, choć najwięcej źródeł zagrożeń można dopatrywać się ostatniej kategorii.

Koncepcja zarządzania oraz oceny ryzyka związana z ochroną informacji została zawarta m.in. w dokumencie normatywnym ISO/IEC 15408, mającym szczególne znaczenie przy certyfikacji przewidzianych zabezpieczeń [5]. Dokument ten wprowadza pojęcie poziomów uzasadnionego zaufania EAL (ang. *evaluation assurance level*). Poziomy EAL stanowią zbiór wymagań odnoszących się do całkowitego cyklu życia produktu, czyli w tym przypadku systemu informatycznego. Zdefiniowano 7 poziomów EAL, przy czym im wyższy poziom tym mniejsza możliwość wystąpienia negatywnych skutków niekorzystnego zdarzenia, które zależą od podatności systemu.

EAL 1 jest poziomem potwierdzającym spełnienie podstawowych wymagań ochrony informacji. Poziom EAL 7 jest najbardziej rygorystyczny i jednocześnie koszt jego implementacji i walidacji jest znacznie droższy. Aby osiągnąć odpowiedni poziom uzasadnionego zaufania należy spełnić oczywiście określone wymagania. Większość z tych wymagań odnosi się do dokumentacji i analizy projektu informatycznego czy też wnikliwych testów poprawnego działania. Im wyższy poziom EAL tym dokumentacja, wszelkie analizy i testy powinny mieć charakter bardziej szczegółowy. Idea poziomów EAL jest w pewnym sensie podobna do idei poziomów nienaruszalności bezpieczeństwa SIL, które są stosowane w ocenie bezpieczeństwa funkcjonalnego [5].

Podsumowując, rola ochrony różnej maści cennych zasobów przedsiębiorstwa, włączając w to informacje niejawne i inne dane, jest bardzo ważna. Zagadnienie to szczególnie widoczne staje się w przypadku systemów zdecentralizowanych, w których wykorzystuje się w znacznej mierze różnego rodzaju środki techniczne, mogące mieć wiele słabych punktów, a przez to sprzyjające występowaniu wielu zagrożeń, których we wcześniejszych analizach nie brano zupełnie pod uwagę.

2.2. Analiza bezpieczeństwa funkcjonalnego

Z drugiej strony ogólnej koncepcji bezpieczeństwa systemu technicznego istnieje zagadnienie związane z bezpieczeństwem funkcjonalnym, częściej niż ochrona informacji rozumianym jako jedna z gałęzi ogólnego bezpieczeństwa. Zależy ono przede wszystkim od poprawnego funkcjonowania systemów związanych z bezpieczeństwem, które muszą realizować funkcje bezpieczeństwa zgodnie z postawionymi im wymaganiami [8]. Koncepcja bezpieczeństwa funkcjonalnego została przedstawiona w dokumentach [9,10] i dotyczy głównie projektowania oraz utrzymywania systemów E/E/PE (elektrycznych, elektronicznych, elektronicznych programowalnych) związanych z bezpieczeństwem. To właśnie te systemy implementują specyficzne funkcje bezpieczeństwa mające na celu redukowanie i co także ważne utrzymywanie ryzyka związanego z pewnymi obiektami technicznymi na akceptowanym poziomie. W celu utrzymania ryzyka dla systemu na poziomie akceptowanym, należy zdefiniować pewne wymagania spełnienia odpowiednich funkcji przez system związany z bezpieczeństwem, czyli opisywanych już wcześniej funkcji bezpieczeństwa. Istnieją dwa typy wymagań, które konieczne są do osiągnięcia bezpieczeństwa funkcjonalnego:

- wymagania na nienaruszalność bezpieczeństwa, czyli prawdopodobieństwo, że dana funkcja bezpieczeństwa wykona się poprawnie,
- wymagania bezpieczeństwa, czyli jakie zadanie ma spełniać dana funkcja bezpieczeństwa.

Po zidentyfikowaniu funkcji bezpieczeństwa oraz przypisaniu im, każdej z osobna, wymagań na nienaruszalność bezpieczeństwa należy opisać specyfikację wymagań funkcjonalnych dla funkcji bezpieczeństwa. Opisują one logikę działania systemu, który będzie realizował tą funkcję. W praktyce specyfikacja ta przybiera postać tabelarycznego bądź opisowego dokumentu lub też zbioru dokumentów, na podstawie których przebiega następnie etap projektowania struktury sprzętowej, która będzie realizować poszczególne funkcje bezpieczeństwa. Informacje na temat specyfikacji bezpieczeństwa wykorzystywane są także na etapie weryfikacji, czyli sprawdzeniu czy zaprojektowana struktura sprzętowa rzeczywiście spełnia wymagania na nienaruszalność bezpieczeństwa.

Wymagania na nienaruszalność funkcji bezpieczeństwa określa się w trakcie oceny ryzyka w taki sposób, aby uzyskać redukcję ryzyka do poziomu akceptowanego lub przynajmniej tolerowanego. Wymagania dla funkcji bezpieczeństwa określane są za pomocą analizy zagrożeń, czyli co należy wykonać, aby uniknąć zdarzenia niebezpiecznego. Po połączeniu ich z wymaganiami na nienaruszalność bezpieczeństwa otrzymuje się całkowitą specyfikację bezpieczeństwa dla zbioru zdefiniowanych funkcji bezpieczeństwa.

Podstawowa koncepcja analizy związanej z określaniem wymaganego poziomu SIL przedstawia się następująco [2]:

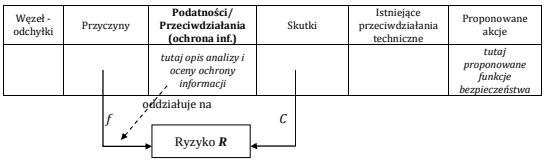
- zidentyfikowanie potencjalnych zagrożeń,
- określenie scenariuszy awaryjnych,
- zidentyfikowanie warstw zabezpieczeń,
- zdefiniowanie funkcji bezpieczeństwa,
- zdefiniowanie tolerowanego poziomu ryzyka dla analizowanego systemu (dla każdego z kryteriów oddzielnie),
- ustalenie aktualnego poziomu ryzyka dla zdefiniowanych scenariuszy awaryjnych oraz

koniecznych do implementacji funkcji bezpieczeństwa,
- ustalenie wymaganego poziomu redukcji ryzyka (na podstawie oceny ryzyka),
- wyrażenie wymaganego poziomu redukcji ryzyka za pomocą poziomów nienaruszalności bezpieczeństwa SIL.

Od poprawnego przeprowadzenia wymienionych czynności zależy właściwe określenie poziomu SIL, a co za tym idzie dobranie poprawnej architektury systemu zabezpieczeniowego.

2.3. Analiza bezpieczeństwa funkcjonalnego z uwzględnieniem czynników ochrony informacji

Biorąc pod uwagę definicję ryzyka, wykorzystywaną w procesie oceny ryzyka, przedstawianą jako kombinację częstości bądź prawdopodobieństwa wystąpienia zdarzenia awaryjnego oraz konsekwencji wystąpienia tego zdarzenia, zaproponowano poniżej metodę określania wymaganego poziomu SIL dla funkcji bezpieczeństwa, z uwzględnieniem aspektów ochrony informacji. Analiza taka bazuje oczywiście na informacji uzyskanej z procesu identyfikacji zagrożeń występujących w systemie technicznym, a także szacowaniu poziomu ryzyka z nim związanego.



Rys. 1. Dodatkowe informacje o poziomie ochrony informacji w analizie zagrożeń

Niektóre czynniki ryzyka, brane pod uwagę podczas przeprowadzania tego typu analiz, mają wpływ na oszacowaną wartość częstości bądź prawdopodobieństwa, niektóre na konsekwencje. Część ryzyka związana z parametrami częstości dotyczy najczęściej zagadnień niezawodności sprzętowej oraz niezawodności i pewności działania człowieka jako części systemu technicznego. Czynnik ryzyka związany z komunikacją i przesyłem danych pomiędzy poszczególnymi elementami systemu jest w takim przypadku pomijana. Jednakże może się okazać, iż w pewnych sytuacjach może ona mieć dość znaczny wpływ na rzeczywisty poziom ryzyka analizowanych scenariuszy awaryjnych [1].

Jak opisano powyżej ryzyko systemu definiuje się jako [9]:

$$R = f \times C \qquad (1)$$

przy czym częstość wystąpienia scenariusza awaryjnego powodującego wystąpienie określonych konsekwencji C jest zależna od szeregu czynników, m.in. niezawodności urządzeń technicznych pracujących w analizowanym systemie. Analizując taki system z punktu widzenia ochrony informacji można wykryć w nim istnienie pewnych podatności, które mogą wpływać na zwiększenie ryzyka związanego z pracą tego systemu. W większości przypadków będzie to oddziaływać na zwiększenie częstości wystąpienia zdarzenia awaryjnego, zatem zakładając, że współczynnik konsekwencji $C = const.$, można powiedzieć, iż:

$f \uparrow \rightarrow R \uparrow$, gdy podatność systemu będzie $\uparrow$

Podatność systemu może być mierzalna i wyrażona poprzez poziom ochrony informacji, oczywiście z uwzględnieniem wprowadzonych przeciwdziałań, które owe podatności systemu mają niwelować [5].

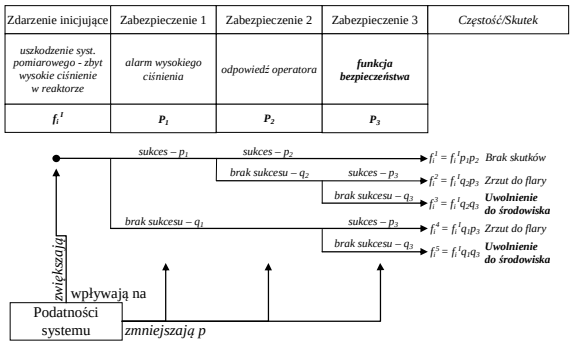
Wracając do etapu identyfikacji zagrożeń, który jest tak naprawdę kluczowy z punktu widzenia definiowania funkcji bezpieczeństwa, które będą implementowane w systemie technicznym, można stwierdzić, iż dla każdego zagrożenia, czy też scenariusza awaryjnego opisanego na tym etapie zapisuje się także przyczyny oraz skutki ich wystąpienia. Ochrona informacji, a raczej jej brak w analizowanym obiekcie, jak założono wcześniej będzie wpływała na część związaną z przyczynami. To tam zawarta będzie informacja o poziomie ochrony informacji oraz zwiększeniu częstości wystąpienia opisywanych scenariuszy awaryjnych. Skutki wystąpienia awarii pozostaną te same, chyba że rozważać będziemy działania sabotujące działanie np. barier, procedur postępowania awaryjnego, itp. Ale w niniejszym dokumencie aspekty te zostaną pominięte w dalszych rozważaniach. Wiedząc, że ograniczanie przyczyn wystąpienia sytuacji awaryjnych jest kluczowe z punktu widzenia bezpieczeństwa obiektu technicznego, ochrona informacji, która dotyczy właśnie tej części powinna być traktowana bardzo poważnie.

Dla metody identyfikacji zagrożeń HAZOP można zaproponować rozszerzenie tabeli o kolumnę dotyczącą zidentyfikowanych podatności systemu (np. sieci przemysłowej) oraz zastosowanych środków ochrony informacji. Dane te wpływały by bezpośrednio na częstość wystąpienia identyfikowanego zagrożenia, kalkulowanego na podstawie zdefiniowanych przyczyn. Przykład propozycji przedstawiono na rys. 1.

Poziom ochrony informacji, który ma być wykorzystywany w dalszej ocenie ryzyka związanego bezpośrednio z analizą bezpieczeństwa funkcjonalnego, musi być zdefiniowany w sposób umożliwiający jego ujęcie w szybki i prosty sposób w tych analizach. W zależności od metod wykorzystywanych w analizach bezpieczeństwa funkcjonalnego, wymagana będzie wartość liczbowa opisująca poziom ochrony informacji lub klasyfikacja jakościowa.

Rozpatrując scenariusze awaryjne i znając wartości liczbowe przypisane częstościom występowania zdarzeń je inicjujących, jak również wartości prawdopodobieństw zadziałania poszczególnych warstw zabezpieczeń istniejących lub projektowanych, można wykorzystać wartości liczbowe opisujące charakter ochrony informacji w analizowanym systemie i scenariuszu.

Zdefiniowane w scenariuszu zdarzenia inicjujące posiadają przypisaną im pewną wartość częstości wystąpienia, która wynika bezpośrednio z analiz przeprowadzonych w fazie analizy zagrożeń (np. metodą HAZOP). Zgodnie z założonym kryterium, częstość takich zdarzeń może wzrosnąć, w zależności od stopnia ochrony informacji (podatności, które nie są odpowiednio zabezpieczone). Poprzez analizę ochrony informacji, np. metodą drzew ataku, można oszacować wartość prawdopodobieństwa wystąpienia zagrożenia związanego z przypisanymi zdarzeniom inicjującym podatnościami systemu. W takim przypadku można określić wartość o jaką częstość zdarzeń inicjujących zostanie zwiększona.



Rys. 2. Przykładowe drzewo zdarzeń z określeniem częstości i konsekwencji poszczególnych sekwencji zdarzenia awaryjnego

Drugim aspektem tego typu analizy jest wpływ ochrony informacji na poprawne działanie poszczególnych analizowanych warstw zabezpieczeniowo-ochronnych. Może się zdarzyć sytuacja, w której istniejące podatności systemu spowodują możliwość ingerencji w funkcjonowanie warstw i ich destrukcję. W takim przypadku wartość ochrony informacji będzie wpływała bezpośrednio na wartości PFD_{avg} przypisane do poszczególnych warstw. Sytuacja taka została zobrazowana na rys. 2.

2.4. Poziom ochrony informacji jako czynnik ryzyka

W celu określenia wymaganego poziomu nienaruszalności bezpieczeństwa SIL wykorzystać można metodę grafu ryzyka. Biorąc pod uwagę jego rozszerzoną wersję [1] i możliwość jego elastycznego modyfikowania, istnieje możliwość dodania pewnych elementów związanych z czynnikiem ryzyka wynikającym z zastosowania, bądź nie zastosowania rozwiązań redukujących ryzyko odnoszące się do zagadnień ochrony informacji w systemie technicznym. W praktyce oznacza to, że do grafu ryzyka można dodać czynnik opisany za pomocą wyników oceny ryzyka ochrony informacji.

Jednocześnie można wykonać klasyfikację systemów technicznych pracujących z wykorzystaniem różnych kanałów komunikacyjnych [2]. Najbardziej narażone na wszelkiego rodzaju podatności są systemy wykorzystujące tylko zewnętrzne kanały przesyłu danych (III kategoria). Dla tych systemów założenie bardziej rygorystycznych przy ocenie ryzyka może być uzasadnione. Natomiast dla systemów, w których używa się wewnętrznych kanałów (I i II kategoria) wystosować można wersję bardziej tolerancyjną. Stąd rozwinięcie metody grafu ryzyka musi opierać się na czynniku ryzyka, klasyfikowanym wg podanej kategoryzacji systemów.

Wyniki analizy ochrony informacji dla np. systemu sterowania pracującego w obiekcie technicznym, można podzielić na kilka podstawowych przedziałów, np. z wykorzystaniem opisu jakościowego. Jeżeli analiza ochrony informacji przebiegałaby zgodnie z [5] określono by poziom EAL dla takiego systemu. Dzięki temu poziom EAL mógłby zostać uwzględniony w analizie bezpieczeństwa funkcjonalnego jako czynnik przypisany do parametru ryzyka w grafie.

Dla systemów III kategorii, czynnik ten będzie posiadał parametry podane w tablicy nr 1, natomiast dla systemów I i II kategorii, ocena ryzyka wykorzysta dane wg tablicy nr 2.

Poprawna kalibracja takiego grafu ma za zadanie zwiększenie wymagań, stawianych systemowi E/E/PE implementującemu funkcję bezpieczeństwa, w przypadku wykrycia zbyt niskiego poziomu ochrony informacji występującemu w analizowanym systemie. Oznacza to, że z im mniej bezpiecznym systemem pod względem ochrony informacji ma się do czynienia, tym większe jest prawdopodobieństwo wystąpienia zdarzeń awaryjnych, ponieważ oprócz standardowych przyczyn związanych z m.in. zawodnym działaniem sprzętu, dochodzą czynniki związane z możliwym celowym działaniem osób trzecich na szkodę takiego systemu [7].

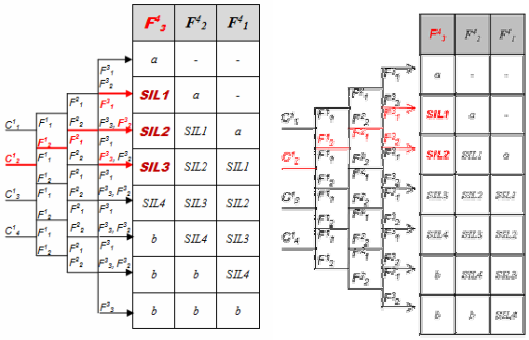
Tab. 1. Kategoryzacja poziomów ochrony inf. dla III kat. [12]

Poziom EAL	Poziom ochrony informacji	Parametr ryzyka i jego kategoria
EAL1	poziom niski	F^3_1
EAL2	poziom niski	F^3_1
EAL3	poziom średni	F^3_2
EAL4	poziom średni	F^3_2
EAL5	poziom wysoki	F^3_3
EAL6	poziom wysoki	F^3_3
EAL7	poziom wysoki	F^3_3

Tab. 2. Kategoryzacja poziomów ochrony inf. dla I i II kat.[12]

Poziom EAL	Poziom ochrony informacji	Parametr ryzyka i jego kategoria
EAL1	poziom niezadowalający	F^3_1
EAL2	poziom niezadowalający	F^3_1
EAL3	poziom zadawalający	F^3_2
EAL4	poziom zadawalający	F^3_2

Brak należytej ochrony informacji w analizowanym systemie, z punktu widzenia rozpatrywanego scenariusza awaryjnego, będzie miał istotny wpływ na zwiększenie wymaganego poziomu SIL dla funkcji bezpieczeństwa, co obrazują przykładowe graf ryzyka (rys. 3).

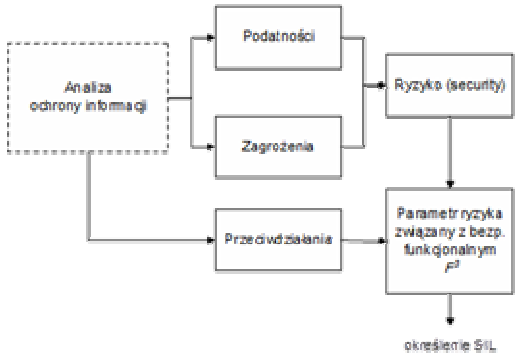


Rys. 3. Przykładowe grafy z dodatkowym parametrem ryzyka

W grafach tych, oprócz parametru F^3 opisującego możliwą podatność systemu z uwagi na zaimplementowany poziom ochrony informacji, wykorzystane są również następujące parametry ryzyka:

- C^1: opis skutków rozpatrywanego scenariusza,
- F^1: możliwość uniknięcia zagrożenia,
- F^2: częstość lub czas przebywania osób w strefie zagrożenia,
- F^4: częstość wystąpienia zdarzenia inicjującego.

Podsumowując, procedura zaproponowana w niniejszym artykule, opiera się w głównej mierze na wykorzystaniu wyników oceny poziomu ochrony informacji pewnego podatnego systemu jako danych wejściowych w ocenie wymagań bezpieczeństwa funkcjonalnego. Odbywa się to poprzez przypisanie dodatkowego parametru ryzyka w grafie ryzyka oraz skalibrowaniu go w sposób dostosowany do sklasyfikowanego systemu (I, II lub III kategoria). Podejście to przedstawiono na rysunku nr 4.



Rys. 4. Czynnik ochrony informacji w analizie bezpieczeństwa

3. PODSUMOWANIE

We współczesnych systemach technicznych wykorzystywane są zarówno wewnętrzne jak i zewnętrzne kanały transmisji danych. Zewnętrzne kanały umożliwiają zwiększenie funkcjonalności systemu, lecz mogą być źródłem pogorszenia stanu bezpieczeństwa, jeżeli nie zostaną we właściwy sposób zaprojektowane i eksploatowane. Przy projektowaniu rozproszonych skomputeryzowanych systemów sterowania, zabezpieczeń i monitoringu powinny być zatem uwzględnione wszystkie potencjalne zagrożenia. Aby tego dokonać powinna być przeprowadzona zintegrowana analiza bezpieczeństwa funkcjonalnego i ochrony informacji.

W związku z tym zaproponowano metodykę określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL z uwzględnieniem aspektów ochrony informacji,, która ma szczególne znaczenie w przypadku analizy różnego rodzaju systemów sterowania i zabezpieczeń działających w oparciu o architekturę rozproszoną.

4. BIBLIOGRAFIA

1. Barnert T., Kosmowski K.T., Śliwiński M., „A method for including the security aspects in the functional safety analysis of distributed control and protection systems", Proceedings of European Safety & Reliability Conference, Rhodos, Greece, 2010
2. Barnert T., Kosmowski K.T., Sliwinski M., Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issue, PSAM 2010, Seattle, USA, 2010
3. Barnert T., Kosmowski K.T., Śliwiński M., „ProSIL Software for Functional Safety Management in Life Cycle", Journal of KONBIN nr 21(1), 2012
4. Barnert T., Piesik E., Śliwiński M., „Wspomagane komputerowo określanie wymaganego poziomu nienaruszalności bezpieczeństwa z wykorzystaniem autorskiej aplikacji ProSIL", Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej, Gdańsk, 2013
5. ISO/IEC 15408:1999: Information technology — Security techniques — Evaluation criteria for IT security Part 1-3.
6. ISO/IEC 17779:2000: Information technology - Code of practice for information security management.
7. Kosmowski K.T., Sliwinski M., Barnert T. Functional safety and security assessment of the control and protection systems, European Safety & Reliability Conference, ESREL 2006 Estoril, Taylor & Francis Group, London, 2006
8. Kosmowski, K.T. (Ed.), „Functional Safety Management in Critical Systems". Gdansk University of Technology, Gdańsk, 2007
9. PN-EN 61508:2010. Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów wiążących się z bezpieczeństwem. Części 1-7. PKN, Warszawa
10. PN-EN 61511:2007. Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3, PKN, Warszawa

THE IMPACT OF THE INFORMATION SECURITY LEVEL ON THE SAFETY INTEGRITY REQUIREMENTS

Key-words: functional safety, SIL, information security

The paper presents the issues related to the risk assessment process of a technical object. It describes methods for determining the safety integrity requirements (SIL) for the identified safety functions. Such functions are performed by the E/E/PE (BPCS and/or SIS) system, and are part of the safety-related system included in the layers of protection concept. A required SIL determination using the methods based on qualitative and semi-quantitative analysis are related to the several basic parameters of risk. They are associated with the frequency of occurrence of a dangerous event and its potential consequences. Due to the fact that more and more technical systems are built based on a distributed architecture, there are some new threats that have not yet been taken into account in the risk analysis. They can affect both the increase in the incidence of events and risk scenarios, and can increase the probability of failure of safety-related functions for reference. Both of these issues should be taken into account in the assignment of the required safety integrity level for the safety-related functions. The paper proposes extension of the currently used methods of functional safety analyses. It can be done with inclusion of the level of information security assigned to the technical system.