XXIII Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2013
Oddział Gdański PTETiS
Referat nr 4

WSPOMAGANE KOMPUTEROWO OKREŚLANIE WYMAGANEGO POZIOMU NIENARUSZALNOŚCI BEZPIECZEŃSTWA Z WYKORZYSTANIEM AUTORSKIEJ APLIKACJI ProSIL

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 przedstawiony został autorski moduł oprogramowania ProSIL wspomagający zarządzanie bezpieczeństwem funkcjonalnym. W module ProSILen wykorzystuje się metody matrycy oraz grafów ryzyka. Referat nawiązuje w swej tematyce do zagadnień związanych z etapem określania specyfikacji wymagań bezpieczeństwa dla zidentyfikowanych funkcji bezpieczeństwa realizowanych przez systemy E/E/PE. Składa się ona z dwóch podstawowych grup wymagań: funkcjonalnych (zadania funkcji bezpieczeństwa) oraz na nienaruszalność bezpieczeństwa. Wymagania te dotyczą bezpośrednio określenia wymaganego poziomu nienaruszalności bezpieczeństwa SIL i ma bardzo ważne znaczenie w późniejszych etapach analizy systemów sterowania i zabezpieczeń w cyklu ich życia.

Słowa kluczowe: bezpieczeństwo funkcjonalne, poziom nienaruszalności bezpieczeństwa (SIL), graf ryzyka, ProSIL

1. OKREŚLANIE WYMAGAŃ BEZPIECZEŃSTWA FUNKCJONALNEGO

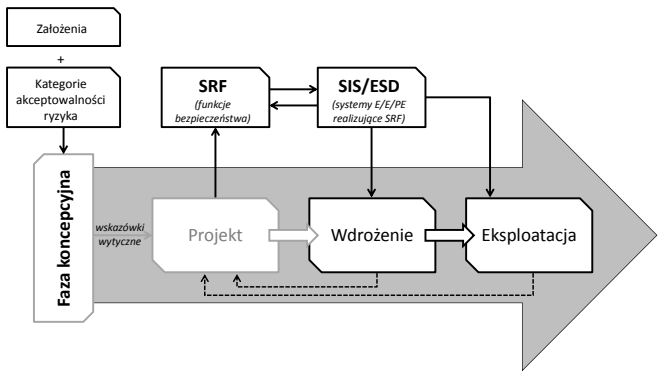
1.1. Wprowadzenie

Bezpieczeństwo funkcjonalne pełni jedną z kluczowych ról w procesie zarządzania bezpieczeństwem w cyklu życia systemu technicznego i dotyczy właściwego projektowania oraz późniejszego utrzymywania systemów technicznych związanych z bezpieczeństwem, wykonanych w technologii E/E/PE (elementy elektryczne / elektroniczne / elektroniczne programowalne) realizujących tzw. funkcje bezpieczeństwa. Mogą to być systemy BPCS (ang. *basic process control system*) lub SIS (ang. *safety instrumentem system*)

W ciągu ostatnich kilkunastu lat znaczenie bezpieczeństwa funkcjonalnego w przemyśle znacznie wzrosło, co wiąże się pośrednio także z opublikowaniem wielu dokumentów normatywnych związanych z tym zagadnieniem, m.in. podstawowej serii norm PN-EN 61508, PN-EN 61511 dla przemysłu procesowego, maszynowej normy PN-EN 62061 i szeregu innych (elektrownie jądrowe, kolejnictwo, transport samochodowy, rolnictwo, itd.). Tendencja do coraz szerszego korzystania z niezawodnych rozwiązań bezpieczeństwa funkcjonalnego przyczynia się dzisiaj bezpośrednio do zmniejszenia poziomu ryzyka związanego z pracą obiektów przemysłowych, ale jednocześnie wprowadza nowe problemy oraz wyzwania dla projektantów oraz inżynierów tworzących, jak również obsługujących systemy związane z bezpieczeństwem.

1.2. Fazy cyklu życia obiektu technicznego

Skupiając się na metodach analizy bezpieczeństwa funkcjonalnego należy umiejscowić je w odpowiednich fazach całkowitego cyklu życia bezpieczeństwa systemu technicznego. Wybrane fazy zostały zobrazowane na rys. 1.



Rys. 1. Wybrane fazy cyklu życia obiektu technicznego

Zidentyfikować można fazę koncepcyjną, w której tworzone są założenia projektowe dla nowopowstającego systemu technicznego. Na tym etapie powinny powstać wszelkie wytyczne dotyczące przeprowadzenia analizy ryzyka oraz analizy bezpieczeństwa funkcjonalnego, zwierające m.in. opis wymaganych do uwzględnienia kryteriów strat, kategorii akceptowalności ryzyka (np. poprzez zdefiniowanie macierzy ryzyka), spisu dopuszczonych metod oceny ryzyka, itp. Także wszelkie ograniczenia projektowe powinny na tym etapie być już zdefiniowane.

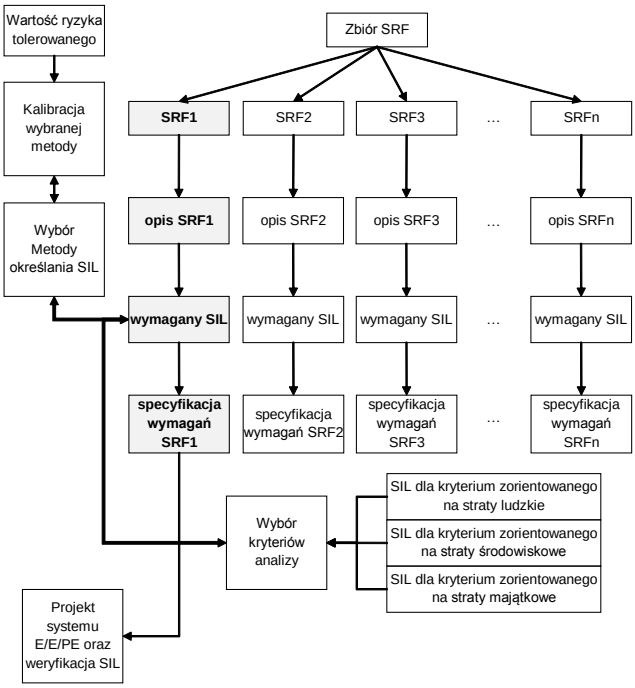
W fazie projektowej wykorzystuje się wytyczne, które powinny być określone w fazie koncepcyjnej, jak również wykonuje się najważniejsze zadania zarządzania bezpieczeństwem funkcjonalnym: zdefiniowanie funkcji bezpieczeństwa, określenie wymagań bezpieczeństwa (w tym wymagań na SIL) dla nich, stworzenie projektu systemu implementującego je, jak również zweryfikowanie spełnienia wymagań przez ten system. Dalsza część referatu dotyczyć będzie zagadnień definiowania funkcji bezpieczeństwa oraz określania wymagań SIL.

1.3. Określanie wymagań bezpieczeństwa funkcjonalnego

Wymagania bezpieczeństwa wiążą się ściśle z definicją ryzyka, które określa się jako kombinację prawdopodobieństwa lub częstości wystąpienia pewnego zdarzenia niebezpiecznego oraz wielkości straty, które to zdarzenie może spowodować

Podstawowa koncepcja określania wymaganego poziomu nienaruszalności bezpieczeństwa związana jest ściśle z fazą analizy i oceny ryzyka i zależna jest od następujących etapów [1, 2]:

- zdefiniowanie akceptowanego/ tolerowanego poziomu ryzyka (w kontekście różnych kryteriów strat) dla analizowanego systemu,
- zidentyfikowanie potencjalnych zagrożeń i scenariuszy awaryjnych,
- ustalenie aktualnego poziomu ryzyka na podstawie zidentyfikowanych zagrożeń,
- ustalenie wymaganego poziomu redukcji ryzyka,
- alokacja redukcji ryzyka na poszczególne warstwy zabezpieczeniowo-ochronne
- dla warstwy realizującej funkcje bezpieczeństwa wyrażenie wymaganego poziomu redukcji ryzyka za pomocą poziomów nienaruszalności bezpieczeństwa SIL.



Rys. 2. Struktura zbioru funkcji bezpieczeństwa [3]

Dla każdego scenariusza awaryjnego oznaczonego S_k wyznaczyć można dwa parametry: f_k - częstość wystąpienia k-tego scenariusza oraz n_k - skutki, które mogą być przyczyną wystąpienia potencjalnych szkód.

Koncepcję tą oddaje poniższy wzór:

$$\boldsymbol{R} = \{< S_k, f_k, n_k >\} \tag{1}$$

Każda zidentyfikowana funkcja bezpieczeństwa powinna zostać szczegółowo opisana wraz z uwzględnieniem specyfikacji jej działania pod względem funkcjonalnym. Informacje te stworzą w kolejnym etapie tzw. specyfikację funkcjonalną bezpieczeństwa. Natomiast określenie wymaganego poziomu nienaruszalności bezpieczeństwa dla każdej funkcji osobno na podstawie oceny ryzyka da możliwość przedstawienia specyfikacji wymagań na nienaruszalność bezpieczeństwa. Struktura ta została zaprezentowana na rys. 2.

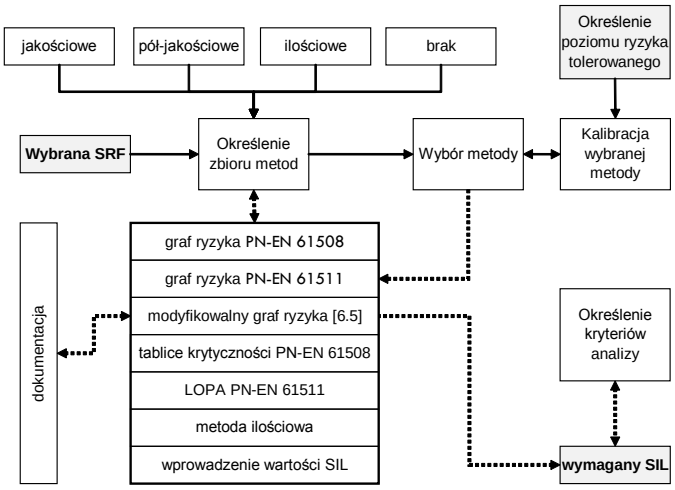
Podczas oceny ryzyka określić należy zakres analizy poprzez podanie kryteriów, dla których tworzone będą wymagania na nienaruszalność funkcji. Analizę tę można przeprowadzić dla trzech głównych kryteriów zorientowanych na straty:

- ludzkie,
- środowiskowe,
- majątkowe.

1.4. Metody określania wymagań SIL

Istnieje możliwość wyboru metody, za pomocą której przeprowadzona zostanie ocena ryzyka związanego z zagrożeniami, dla których projektowana jest funkcja bezpieczeństwa. Dostępne metody można podzielić wg rodzaju danych wykorzystywanych w procesie alokowania wymagań:

- jakościowe,
- pół-jakościowe, pół-ilościowe,
- ilościowe.



Rys. 3. Schemat wyboru metody określania wymaganego poziomu SIL [3]

Najczęściej wykorzystywanymi w praktyce inżynierskiej metodami są m.in. [4].:

- metoda grafu ryzyka zgodna z dokumentem PN-EN 61508 lub kalibrowanego grafu ryzyka (PN-EN 61511),
- zmodyfikowane grafy ryzyka,
- metoda tablic krytyczności zdarzenia zagrażającego opisana w PN-EN 61508,
- analiza warstw zabezpieczeń LOPA,
- metoda ilościowa.

Przy ocenie ryzyka wykorzystuje się wiedzę na temat skutków oraz częstości lub prawdopodobieństwa występujących zdarzeń awaryjnych. Skojarzone z nimi parametry ryzyka mogą posiadać pewne cechy opisujące ich charakter i umożliwiające lepsze oszacowanie wartości dla nich przypisanych. I tak, przykładowo dla parametru prawdopodobieństwa zajścia zdarzenia awaryjnego można rozważać takie cechy, jak:

- istnienie warstw zabezpieczeń,
- dane historyczne o występowaniu podobnych zdarzeń awaryjnych.

Rozważając z kolei taki parametr ryzyka, jak prawdopodobieństwo uniknięcia zagrożenia, można posłużyć się następującymi cechami:

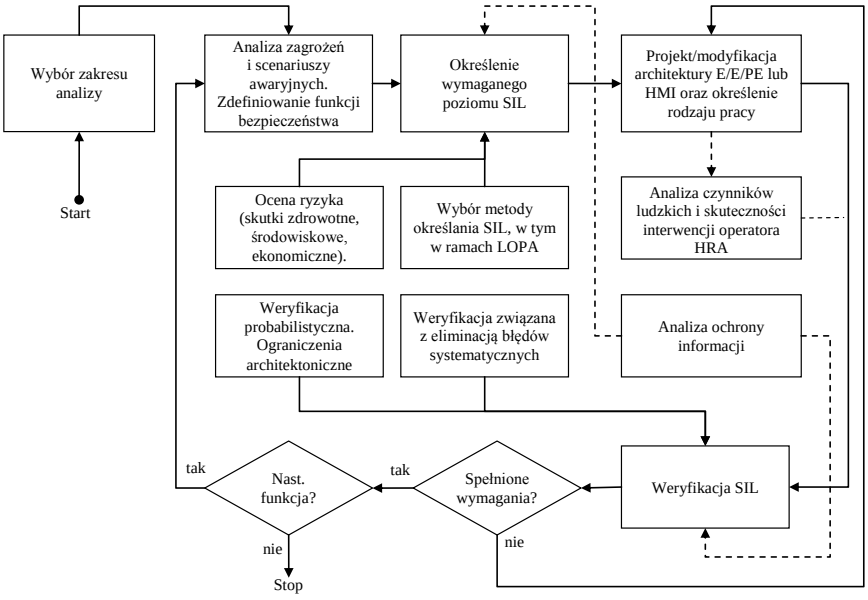
- dynamika procesu,
- czas, po jakim dojdzie do wystąpienia zdarzenia niebezpiecznego po utracie sterowania,
- lokalny dostęp do wskaźników stanu procesu przez operatorów,
- przeszkolenie personelu na wypadek zajścia zdarzenia niebezpiecznego,
- wydzielenie i utrzymywanie w wymaganym stanie dróg ewakuacji.

Dla każdego parametru ryzyka można więc stworzyć listę cech stanowiących zbiór kluczowych zagadnień, które należy uwzględnić w procesie oceny ryzyka dla analizowanej funkcji bezpieczeństwa.

2. APLIKACJA ProSIL

2.1. Ogólna struktura aplikacji

Aplikacja ProSIL została zaprojektowana w celu umożliwienia komputerowego wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym w cyklu życia systemów technicznych. Ogólne założenia projektowe tej aplikacji obejmują wspomaganie procesu projektowania systemów E/E/PE, BPCS i SIS zgodnie wymaganiami i kryteriami norm PN-EN 61508 i PN-EN 61511. Struktura omawianej aplikacji została zobrazowana na rys. 4.



Rys. 4. Ogólny schemat funkcjonalny aplikacji komputerowej ProSIL

Program ProSIL umożliwia wyznaczanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL na podstawie wymagań instytucji nadzorującej dla wyróżnionych funkcji bezpieczeństwa. ProSIL wyposażony jest także w moduł wspomagający komputerową weryfikację poziomu nienaruszalności bezpieczeństwa SIL dla rozważanych architektur sprzętu poszczególnych funkcji bezpieczeństwa. Zapewnia także wspomaganie w ocenie rozwiązań technicznych i organizacyjnych, jak również wpływu błędów systematycznych oprogramowania i błędów człowieka podczas eksploatacji systemów E/E/PE, BPCS i SIS [5].

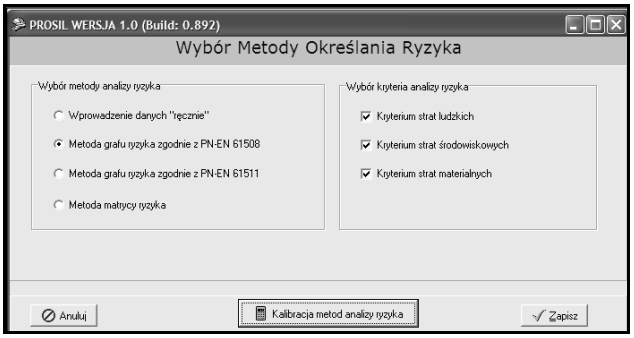
W aplikacji ProSIL przewidziano dodatkowo możliwość uwzględnienia zagadnień związanych z ochroną informacji w przemysłowych skomputeryzowanych rozproszonych systemach sterowania i zabezpieczeń w zarządzaniu bezpieczeństwem funkcjonalnym. Wpływ zagadnień związanych z ochroną informacji na określanie wymaganego poziomu nienaruszalności SIL oraz jego weryfikację jest zaimplementowany w najnowszej wersji aplikacji w sposób niezależny dla modułów ProSILen oraz ProSILer.

2.2. Moduł ProSILen

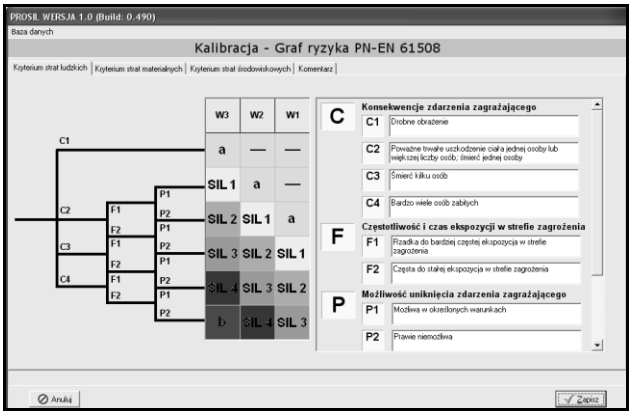
Oprogramowanie ProSIL umożliwia wprowadzenie zbioru funkcji bezpieczeństwa zidentyfikowanych wcześniej na etapie analizy zagrożeń. Każda analiza bezpieczeństwa funkcjonalnego dostępna w aplikacji ProSIL przeprowadzana jest dla odrębnych, zdefiniowanych w projekcie funkcji bezpieczeństwa z osobna. Dotyczy to zarówno procesu określania wymagań SIL jak i weryfikacji ich poziomu.

Moduł określania wymaganego poziomu SIL składa się z dwóch powiązanych ze sobą części funkcjonalnych. Pierwszym z nich jest moduł kalibracji wybranej metody oceny ryzyka. Zgodnie z założeniami funkcjonalnymi aplikacji, kalibracja taka dokonywana jest raz dla projektu zapisanego w ProSIL. Polega ona na wyborze jednej z kilku dostępnych w aplikacji metod, a następnie zdefiniowaniu części tabelarycznej metody oraz określeniu parametrów ryzyka oraz ich przedziałów kryterialnych. W przypadku metody grafu ryzyka jest to część tabelaryczna grafu oraz cztery parametry ryzyka C, P, F oraz W. Definicja części tabelarycznej polega na wyborze jednego z siedmiu dostępnych poziomów redukcji ryzyka, powiązanych z czterema poziomami SIL oraz braku wymagań lub wymagań szczegółowych. Okno wyboru metody przedstawione jest na rys. 5.

Druga część modułu określania wymaganego poziomu SIL jest związana z wykorzystaniem wybranej i skalibrowanej metody. Przy kalibracji określa się, względem których kryteriów strat wykonywana będzie analiza (rys. 6). Determinuje to możliwości wykorzystania tych kryteriów w procesie oceny ryzyka. Z oceny tej dla każdego z kryterium otrzymuje się wymagany poziom nienaruszalności bezpieczeństwa SIL. Jeżeli wybrano więcej jak jedno kryterium analizy, program wybiera najbardziej restrykcyjną (maksymalną) wartość SIL jako tą, która obowiązywać ma dla analizowanej funkcji bezpieczeństwa.



Rys. 5. Wybór metody określania wymaganego poziomu SIL



Rys. 6. Kalibracja metody grafu ryzyka PN-EN 61508 wg kryterium strat ludzkich

Zakładając, że proces oceny ryzyka i określenia wymagań SIL dla wybranej, przykładowej funkcji bezpieczeństwa, którą oznaczyć można jako „Ochrona reaktora przed eksplozją" zostały przeprowadzone z wykorzystaniem skalibrowanego grafu ryzyka dla dwóch wybranych kryteriów strat: majątkowych oraz ludzkich, otrzymano dwie wynikowe wartości wymaganego poziomu nienaruszalności bezpieczeństwa: SIL2 oraz SIL3. W takiej sytuacji, zgodnie z zasadą wyboru pesymistycznych wartości, należy wykorzystać wartość SIL3 jako wymaganą dla systemu E/E/PE, który będzie realizował rozpatrywaną funkcję bezpieczeństwa.

3. PODSUMOWANIE

Analizę bezpieczeństwa należy wykonywać wg wcześniej zdefiniowanych procedur, aby cały proces był wyczerpujący, dobrze zorganizowany oraz odpowiednio zarządzany. Poczynając od analizy zagrożeń, poprzez analizę ryzyka, jego ocenę oraz wyznaczenie wymaganego poziomu redukcji ryzyka uzyskuje się wymagania, jakie postawione zostaną projektantowi systemu związanego z bezpieczeństwem. Ocena ryzyka może dotyczyć strat związanych z utratą zdrowia lub życia pracowników i osób postronnych, szkodami majątkowymi oraz szkodami w środowisku naturalnym. Jest to więc bardzo ważne zagadnienie w procesie analizy bezpieczeństwa.

Stworzony moduł ProSILen do określania wymaganego poziomu nienaruszalności bezpieczeństwa dla wybranych funkcji bezpieczeństwa ma za zadanie wspomagać proces przeprowadzania analiz funkcji związanych z bezpieczeństwem oraz jednocześnie ułatwiać szybki i łatwy dostęp do wszystkich informacji na ich temat. Poprzez umożliwienie wyboru jednej z dostępnych metod służących do przeprowadzania oceny ryzyka, wśród nich także autorskiego rozwiązanie modyfikowalnych grafów ryzyka [6], aplikacja ProSIL jest uniwersalnym narzędziem wspomagającym osoby odpowiedzialne za kształtowanie poziomu bezpieczeństwa w systemach podwyższonego ryzyka. Jednocześnie dzięki prowadzonym dalszym pracom badawczym moduł ten zostanie wzbogacony o możliwość integrowania analizy bezpieczeństwa funkcjonalnego z analizą ochrony informacji obiektu technicznego [7].

4. BIBLIOGRAFIA

1. PN-EN 61508: Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów wiążących się z bezpieczeństwem, Części 1-7, PKN, Warszawa 2005
2. PN-EN 61511: Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3, PKN, Warszawa 2007
3. Barnert T.: Określanie wymaganego poziomu nienaruszalności bezpieczeństwa, Journal of Polish Safety & Reliability Association, s 35-43, Gdynia 2011
4. Missala, T.: Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa zawartych w normach bezpieczeństwa funkcjonalnego, normach związanych z nimi oraz literaturze. PIAP, Warszawa, 2009
5. Barnert T., Kosmowski, K.T., Śliwiński, M.: ProSIL software for functional safety management in life cycle, Journal of KONBiN, Warszawa 2013
6. Barnert, T., Kosmowski, K.T., Śliwiński, M.: A knowledge-based approach for functional safety management, Proceeding of ESREL Conference, Praga, Czechy 2010
7. 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. Proceeding of ESREL Conference, Rhodos, Grecja 2010

COMPUTER AIDED SAFETY INTEGRITY LEVEL SELECTION WITH ProSIL SOFTWARE

Key-words: functional safety, safety integrity level (SIL), risk graph, ProSIL

In this article a module for SIL deteremination in ProSIL software is discribed. This module consists of risk matrix and risk graphs methods.. In ProSIL the methods concerning functional safety analysis in the process of the design and operation of E/E/PE systems are implemented according to PN-EN 61508 and PN-EN 61511 standards. It is aimed mainly at safety requirements determining, which is divided into two groups: functional (what is the main scope of safety related function) and integrity requirements (how much risk reduction should be related with this function). The second requirement is very important, because it is connected with required safety integrity level (SIL) which will be used in next stages of analysis.