

Barnert Tomasz

Kacprzak Przemysław

Kosmowski Kazimierz

Kozyra Maciej

Porzeziński Michał

Śliwiński Marcin

Zawalich Jacek

Politechnika Gdańska, Gdańsk, Polska

ProSIL software for computer aided functional safety management Program komputerowy ProSIL do wspomagania zarządzaniem bezpieczeństwa funkcjonalnego

Keywords / Słowa kluczowe

functional safety, computer aided management, safety-related functions, safety integrity
bezpieczeństwo funkcjonalne, zarządzanie wspomaganie komputerowo, funkcje bezpieczeństwa,
nienaruszalność bezpieczeństwa

Abstract

In this article a prototype ProSIL software system for computer-aided functional safety management is described. The software consists of three modules for: determination of the required SIL level (ProSILen), verification of the SIL level (ProSILver), and layer of protection analysis (ProSIL/LOPA). In ProSIL the methods concerning functional safety analysis in the process of the design and operation of Safety Instrumented Systems (SIS) are implemented according to PN-EN 61508 and PN-EN 61511 standards, and some new methods, e.g. the calibrated risk graph method for determining required safety integrity level (SIL) based on the risk assessment. Moreover, methods of verifying the SIL level of SIS. The Layer of Protection Analysis (LOPA) method with regard to Human Reliability Analysis (HRA) are also included in the software.

1. Wprowadzenie

Aplikacja ProSIL w obecnej wersji została zaprojektowana do wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym w cyklu życia. Ogólne założenia projektowe tej aplikacji obejmują wspomaganie procesu projektowania systemów E/E/PE, BPCS i SIS zgodnie z wymaganiami i kryteriami norm PN-EN 61508 i PN-EN 61511. Program ProSIL umożliwia wyznaczenie wymaganego poziomu nienaruszalności bezpieczeństwa SIL metodą grafu ryzyka lub wprowadzanie SIL na podstawie wymagań instytucji

nadzorującej dla wyróżnionych funkcji bezpieczeństwa.

ProSIL wyposażony jest 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 (poprzez uwzględnienie różnych czynników) sprzyjających redukcji wpływu błędów systematycznych oprogramowania i błędów człowieka-operatora podczas eksploatacji systemów E/E/PE, BPCS i SIS. W oprogramowaniu ProSIL wprowadzono możliwość uwzględnienia wpływu

błędów człowieka w modelowaniu probabilistycznym warstw zabezpieczeń metodą LOPA. W aplikacji ProSIL dokumentowane są na bieżąco projekty analizy bezpieczeństwa funkcjonalnego, możliwe jest drukowanie części zgromadzonych danych w ramach projektu i finalnego raportu. Program komputerowy ProSIL w wersji prototypowej przeznaczony jest do pracy jako indywidualne stanowisko robocze z możliwością zainstalowania na komputerach klasy IBM-PC (Rysunek 1).

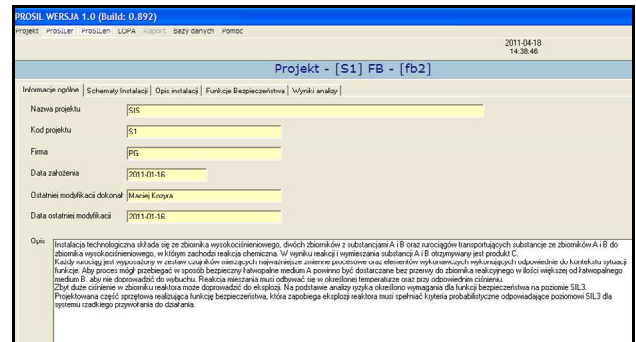


Rysunek 1. Oprogramowanie ProSIL

Jako minimalne wymaganie w zakresie platformy systemowej przyjęto Microsoft Windows XP Professional® z poprawką Service Pack 3. Program ProSIL powstał w środowisku programowania RAD (Rapid Application Development) Delphi®. Jest to jedno z czołowych środowisk RAD dla programistów, w tym twórców aplikacji bazodanowych.

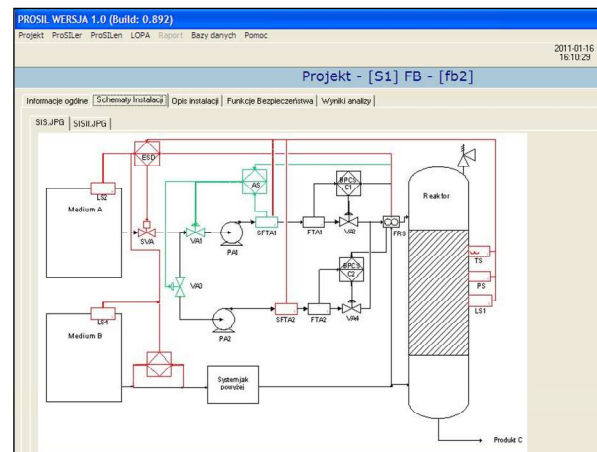
2. Okno główne aplikacji ProSIL

Aplikacja ProSIL składa się z trzech głównych modułów: określania SIL (ProSILen), weryfikacji SIL (ProSILer) oraz modułu analizy LOPA. Na Rysunku 2 znajduje się główne okno projektu w oprogramowaniu ProSIL. Na górnym pasku użytkownik ma do wyboru bezpośrednie przejście do modułów określania, weryfikacji i analizy LOPA. Każdy nowoprowadzony projekt posiada szczegółowy opis, który jest przechowywany w bazie danych aplikacji ProSIL.



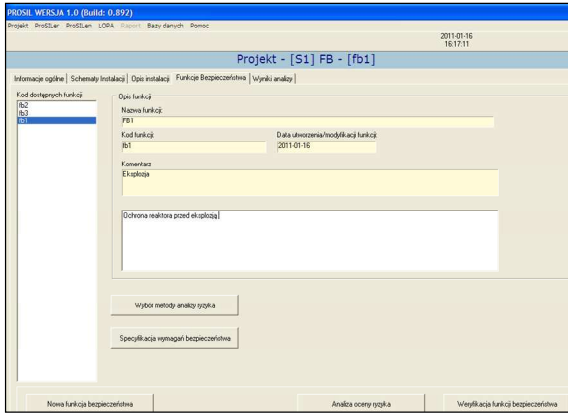
Rysunek 2. Główne okno projektu

Z okna głównego projektu użytkownik ma wgląd do: informacji ogólnych dotyczących projektu oraz opisu instalacji, dla której projektowane są funkcje bezpieczeństwa, a także schematów aktualnie opracowywanych instalacji (Rysunek 3).



Rysunek 3. Schemat instalacji

Oprogramowanie Pro-SIL umożliwia wprowadzenie zbioru funkcji bezpieczeństwa zidentyfikowanych wcześniej na etapie analizy zagrożeń (Rysunek 4). Metody pozwalające na identyfikację zagrożeń, takie jak np. HAZOP nie zostały jedna zaimplementowane z uwagi na utrzymanie prostoty i przejrzystości interfejsu. Ta możliwość została jednak przewidziana w kolejnej, rozbudowanej wersji programu.



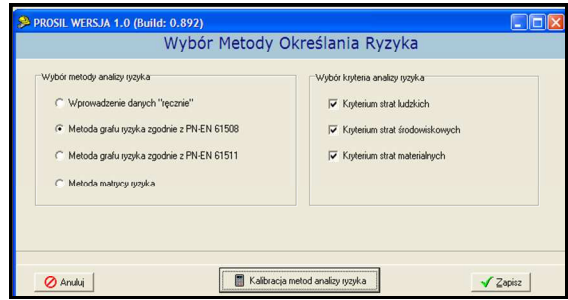
Rysunek 4. Definiowanie funkcji bezpieczeństwa

Mając jednak na uwadze konieczność powiązania informacji wynikowych z procesu analizy zagrożeń i informacji wejściowych dla procesu oceny ryzyka umożliwiono załączenie tych informacji do programu w postaci dokumentów tekstowych (będących jednocześnie załącznikami do dokumentacji określania wymaganego poziomu SIL).

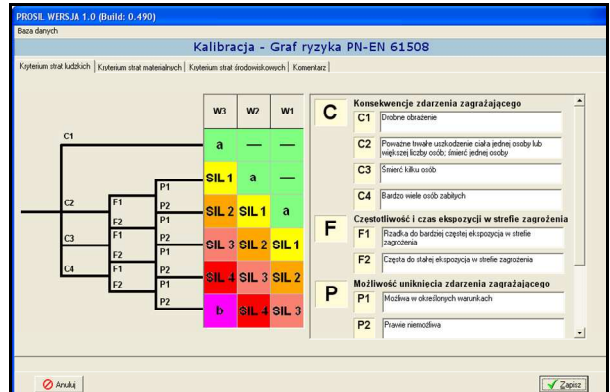
3. Moduł określania poziomu SIL

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 metod, a następnie zdefiniowaniu części tabelarycznej metody oraz określeniu parametrów ryzyka oraz ich przedziałów kryterialnych.

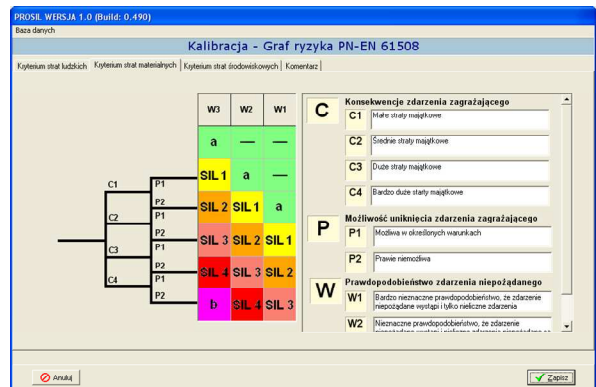
W przypadku metody grafu ryzyka jest to część tabelaryczna grafu oraz cztery parametry ryzyka C, P, F oraz W. Definicja części tabelarycznej polega na wyborze jednego z siedmiu dostępnych poziomów redukcji ryzyka, powiązanych z czterema poziomami SIL oraz braku wymagań. Okno wyboru metody przedstawione jest na Rysunku 5, natomiast okno zasadnicze kalibracji wybranej metody na Rysunku 6-10.



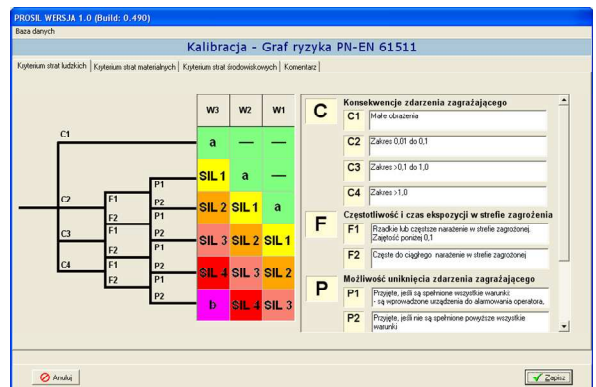
Rysunek 5. Wybór metody określania wymaganego poziomu SIL



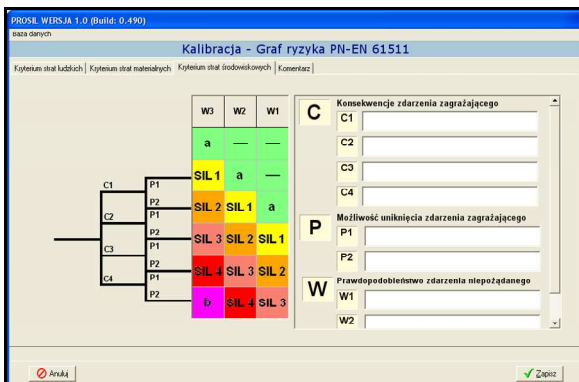
Rysunek 6. Kalibracja metody grafu ryzyka PN-EN 61508 wg kryterium strat ludzkich



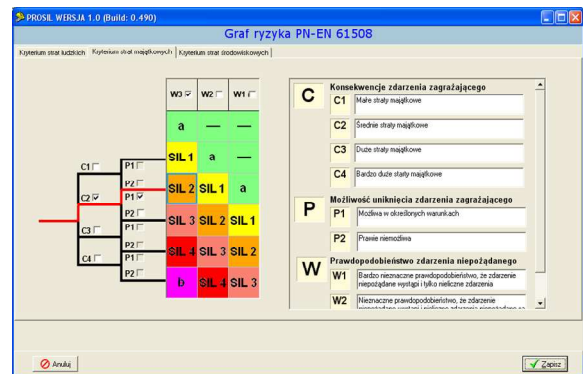
Rysunek 7. Kalibracja metody grafu ryzyka PN-EN 61508 wg kryterium strat materialnych



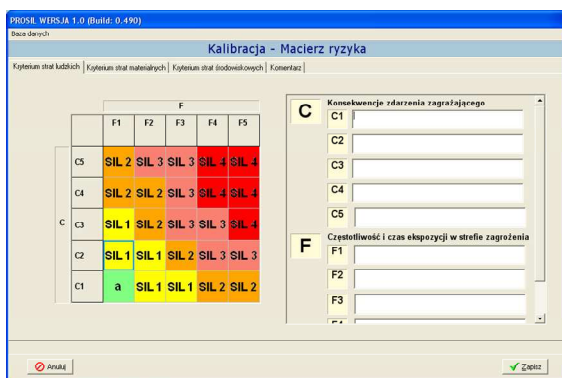
Rysunek 8. Kalibracja metody grafu ryzyka PN-EN 61511 wg kryterium strat ludzkich



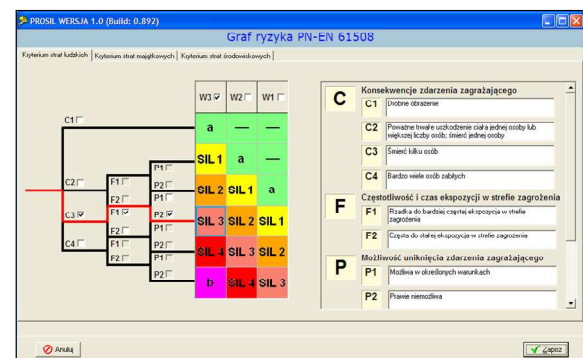
Rysunek 9. Kalibracja metody grafu ryzyka PN-EN 61511 wg kryterium strat środowiskowych



Rysunek 11. Określenie wymaganego poziomu SIL (kryterium strat majątkowych)



Rysunek 10. Kalibracja metody macierzy ryzyka PN-EN 61511 wg kryterium strat ludzkich

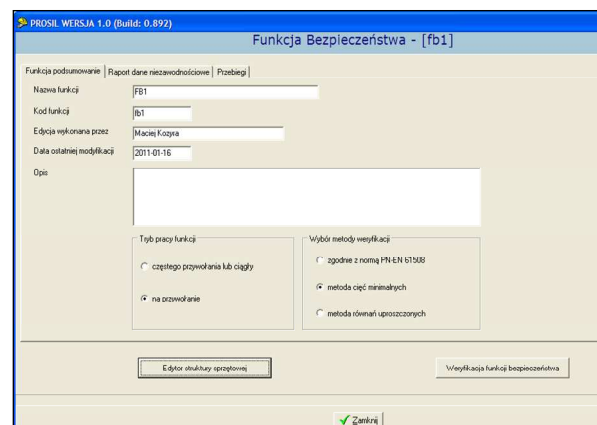


Rysunek 12. Określenie wymaganego poziomu SIL na podstawie grafu ryzyka wg 61508 dla kryterium strat ludzkich

Druga część modułu określania wymaganego poziomu SIL jest związana już z wykorzystaniem wybranej i skalibrowanej metody. Przy kalibracji określa się, względem których kryteriów start wykonywana będzie analiza (patrz Rysunek 5). 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. Na kolejnych Rysunek 11-12 przedstawiono przykładowe okno modułu oceny ryzyka – określania wymaganego poziomu SIL.

4. Moduł wspomagający weryfikację SIL

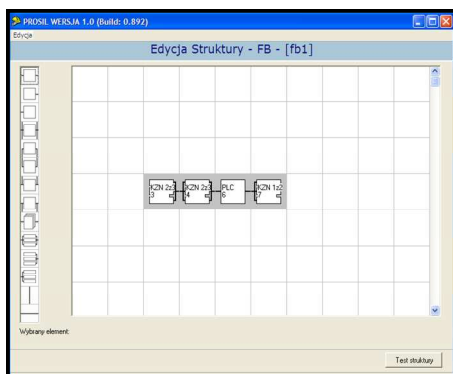
Oprogramowanie ProSIL pozwala na zamodelowanie systemu E/E/PE o dowolnej konfiguracji sprzętowej. Podsystemy mogą mieć strukturę k z n oraz mogą się składać z różnych elementów. Na Rysunku 13 przedstawiono okno główne modułu weryfikacji SIL (ProSILer).



Rysunek 13. Okno główne modułu wspomagającego weryfikację SIL

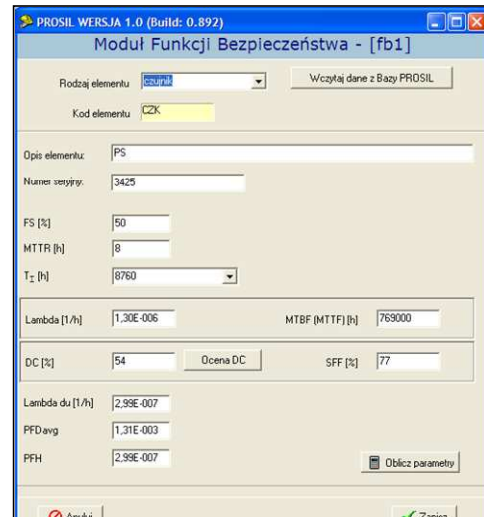
W oknie głównym modułu weryfikacji SIL aplikacji ProSIL należy wprowadzić nazwę funkcji bezpieczeństwa realizowanej przez warstwę SIS, kod funkcji, dane osoby odpowiedzialnej za wprowadzenie modelu struktury sprzętowej funkcji bezpieczeństwa oraz datę ostatniej modyfikacji. Można dodatkowo wprowadzić szerszy opis projektowanej funkcji bezpieczeństwa. Następnie należy wybrać tryb pracy systemu realizującego funkcję bezpieczeństwa tj. „częstego przywołania lub ciągły” lub „na przywołanie”. Projektant ma do wyboru trzy metody weryfikacji SIL: zgodnie z normą PN-EN 61508, metodą cięć minimalnych oraz równań uproszczonych. Po odznaczeniu w odpowiednim polu okna głównego wybiera się rodzaj metody, według której będzie pracował algorytm obliczeniowy. W następnym kroku należy przejść do okna projektowego struktury sprzętowej funkcji bezpieczeństwa, wybierając przycisk „Edytor struktury sprzętowej”.

Projektowana funkcja bezpieczeństwa przedstawiona jest w postaci schematów blokowych dla struktury sprzętowej z wyraźnym podziałem na części podsystemów: pomiarowych (czujniki, detektory), przetwarzania danych (sterowniki PLC lub ESD wraz z modułami wejść/wyjść, CPU, separatorami, i modułami komunikacyjnymi) i wykonawczych. Projektant ma do dyspozycji szereg modułów i elementów, które musi wprowadzić do okna projektowego. Po wprowadzeniu należy dokonać testu połączeń bloków, wybierając przycisk „Test struktury” (Rysunek 14).



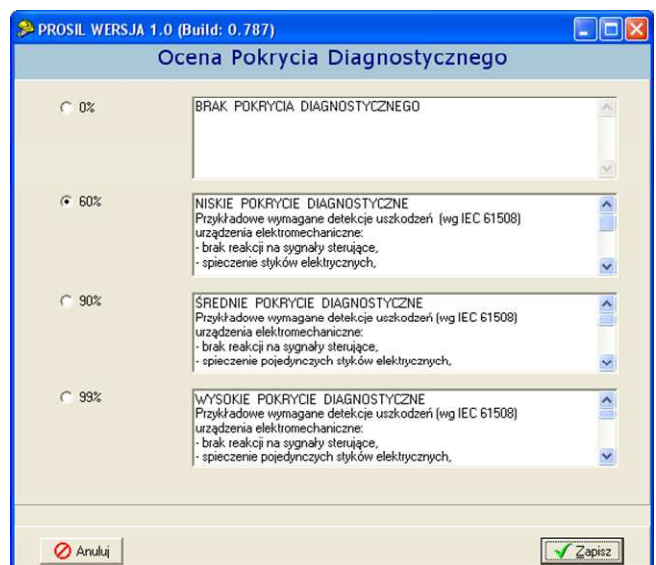
Rysunek 14. Edytor graficzny struktury warstwy sprzętowej funkcji bezpieczeństwa

Na Rysunku 15 przedstawiono edytor graficzny pojedynczego elementu struktury sprzętowej funkcji bezpieczeństwa.



Rysunek 15. Wprowadzanie danych niezawodnościowych dla pojedynczego elementu

Dane niezawodnościowe dla pojedynczego elementu funkcji bezpieczeństwa np. czujnika temperatury, mogą być wprowadzone do systemu ręcznie przez projektanta lub automatycznie bazy danych ProSILcdb. Użytkownik posiadający dokładne dane odnośnie wartości pokrycia diagnostycznego ma możliwość bezpośredniego jej wpisania w odpowiednie pole oznaczone symbolem „DC [%]”. W przypadku, gdy użytkownik nie ma takich danych i potrzebuje dodatkowych informacji, program ProSIL umożliwia otwarcie następnego okna dialogowego poprzez kliknięcie na przycisk „Ocena DC” (Rysunek 16).

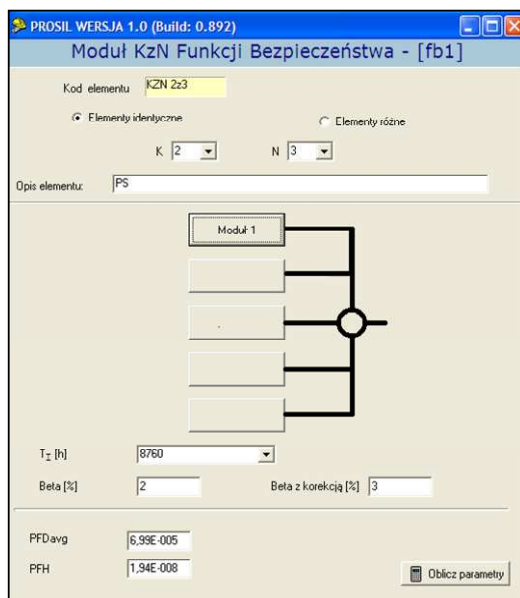


Rysunek 16. Okno dialogowe modułu oszacowania pokrycia diagnostycznego DC

Okno pod nazwą: „Ocena pokrycia diagnostycznego” pozwala na przedziałowe określenie pokrycia diagnostycznego na podstawie

znajomości właściwości analizowanego podsystemu realizującego daną funkcję bezpieczeństwa. Ocena DC polega na wyborze odpowiedniego przedziału zakresu: 0% – brak pokrycia diagnostycznego, 60% – niskie pokrycie diagnostyczne, 90% – średnie pokrycie diagnostyczne oraz 99% – wysokie pokrycie diagnostyczne. Każdy z czterech przedziałów użytkownik wybiera na podstawie przeanalizowania możliwości przeprowadzenia testów diagnostycznych, które przykładowo podane są przy każdej wybranej procentowej wartości DC. Zaznaczenie odpowiedniego przedziału wartości DC oraz zatwierdzenie przyciskiem „Zapisz” wprowadza wybrane oszacowanie DC w kontekście analizowanej funkcji bezpieczeństwa. Przy DC = 0% program nie podaje przykładowych testów. Przy niskim pokryciu diagnostycznym użytkownik ma dostępną pomoc w postaci listy przykładowych uszkodzeń, które mogą być wystarczające do uzyskania DC = 60%, 90% lub 99%. W oknie dialogowym zastosowano podział całego podsystemu realizującego funkcje bezpieczeństwa, na elementy pomiarowe, wykonawcze oraz na sprzęt cyfrowy.

Po kliknięciu prawym klawiszem myszy na symbol graficzny struktury k z n pojawia się okno przedstawione na Rysunku 17.

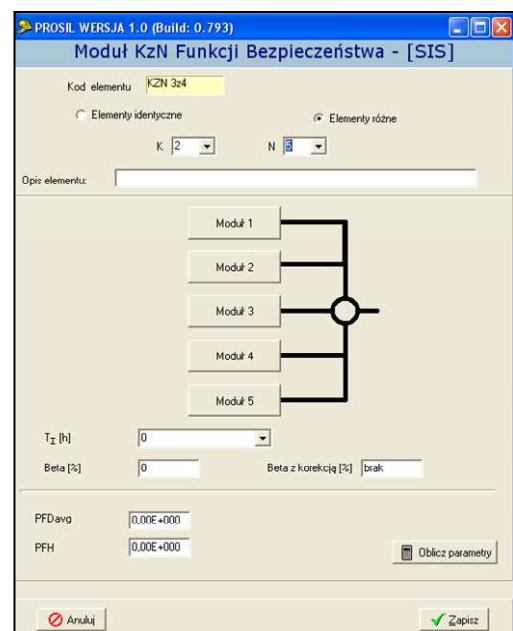


Rysunek 17. Moduł weryfikacji SIL – struktura k z n identyczne elementy

Struktura k z n ma wyższy poziom w hierarchii od pojedynczego elementu. Zawiera pojedyncze elementy o określonym modelu probabilistycznym.

Struktura k z n może składać się z jednakowych bądź różnych elementów (Rysunek 18).

Poszczególne elementy (zawory, pompy, czujniki, siłowniki, moduły wejść/wyjść, procesory) z których składają się podsystemy (część pomiarowa, układ przetwarzania danych, część wykonawcza) stanowiące cały system – układ zabezpieczeniowy układ sterowania, połączone są ze sobą za pomocą punktów węzłowych. Przebieg sygnału następuje od wejścia do wyjścia. Po wprowadzeniu danych niezawodnościowych i przetestowaniu poprawności połączeń struktury sprzętowej należy uruchomić algorytm obliczeniowy naciskając w oknie głównym modułu weryfikacji SIL przycisk „Weryfikacja funkcji bezpieczeństwa”. Po uruchomieniu weryfikacji pojawia się tablica raportu z weryfikacji SIL w aplikacji ProSIL (osobno dla trybu pracy „częstego przywołania lub ciągłej” lub „na przywołanie”) (Rysunek 19).

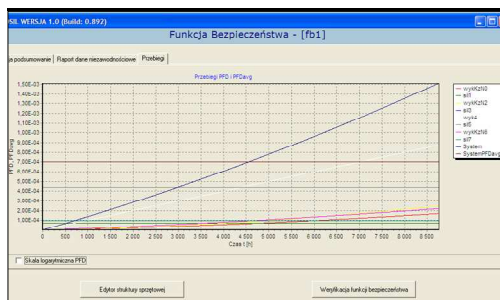


Rysunek 18. Moduł weryfikacji SIL – struktura k z n różne elementy

Element ID	K z N	Lambda [1/h]	T [h]	MTR [h]	Beta [%]	DC [%]	SFF [%]	Lambda du [1/h]	PFDAvg [1/h]	SIL	PFDAvg [%]
SYSTEM									7,01E-004	3	100,0
KzN	2z3		8760		3				6,99E-005	4	10,0
CKZ 23	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
CKZ 23	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
CKZ 23	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
KzN	2z3		8760		3				9,99E-005	4	13,6
CKZ 5	kzn	1,76E-006	8760	8	-	66	83	2,99E-007	1,31E-003	2	
CKZ 5	kzn	1,76E-006	8760	8	-	66	83	2,99E-007	1,31E-003	2	
CKZ 5	kzn	1,76E-006	8760	8	-	66	83	2,99E-007	1,31E-003	2	
PLC 6	-	2,00E-006	8760	8	-	90	95	1,00E-007	4,39E-004	3	62,6
KzN	1z2		8760		2				9,72E-005	4	13,9
WYK 8	kzn	2,10E-006	8760	8	-	24	62	7,98E-007	3,50E-003	2	

Rysunek 18. Okno raportu weryfikacji SIL

Po dokonaniu weryfikacji wyznaczone zostają wartości PFD(t), PFD_{avg} , PFH dla wszystkich elementów systemu (czujniki, zawory, moduły wejść/wyjść, układy CPU), podsystemów i systemu. Wartości te przedstawione są w postaci raportu – plik tekstowy (zawierający wynikowe dane oraz schemat analizowanej struktury). Na *Rysunku 19* znajduje się okno do wyznaczania i graficznej reprezentacji przebiegu prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie PFD(t). natomiast *Rysunek 20* przedstawia te same przebiegi w skali logarytmicznej.



Rysunek 19. Reprezentacja graficzna przebiegów PFD(t), PFD_{avg}



Rysunek 20. Reprezentacja graficzna przebiegów PFD(t), PFD_{avg} w skali logarytmicznej

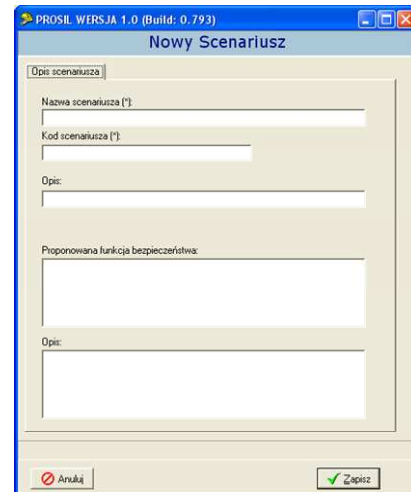
Na *Rysunku 21* przedstawiono zbiorcze wyniki dla wszystkich funkcji bezpieczeństwa uwzględnionych w projekcie.

Funkcja	Określenie metody	Składowe SIL	Weryfikacja model	Weryfikacja SIL
B2	Goal sygn. PN EN 61508	3	Metoda elementów ograniczonych	3
B3	Goal sygn. PN EN 61508	3	Zgodnie z normą PN EN 61508	3
B4	Goal sygn. PN EN 61508	3	Metoda opcji minimalnych	3

Rysunek 21. Wyniki analizy BF

5. Moduł wspomagający przeprowadzenie analizy LOPA

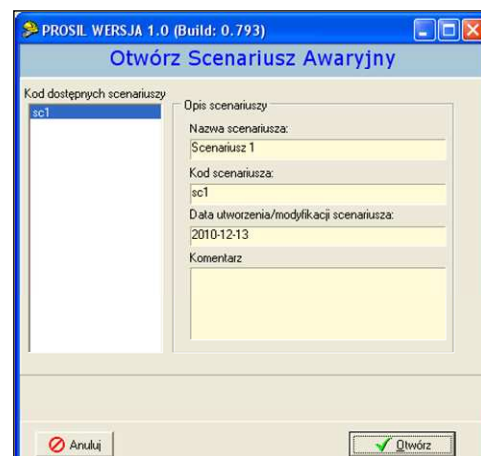
W niniejszym rozdziale przedstawiono moduł wspomagający przeprowadzenie analizy LOPA w aplikacji ProSIL. Na poniższym rysunku zaprezentowano wygląd okna służącego do przeprowadzania analizy warstw zabezpieczeń LOPA w wersji podstawowej (*Rysunek 22*).



Rysunek 22. Analiza LOPA nowy scenariusz

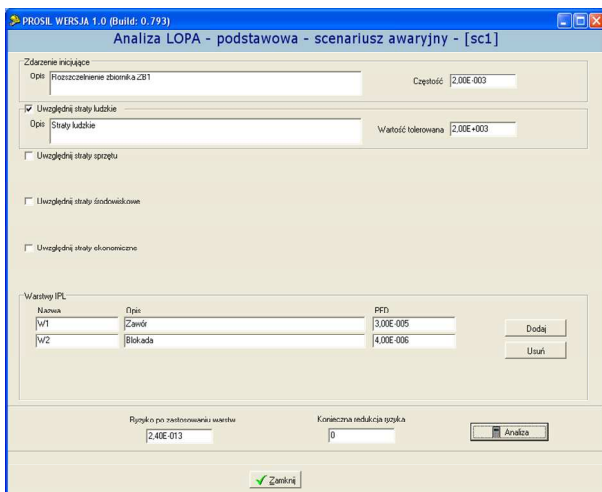
Podczas definiowania nowego scenariusza możliwe jest wpisanie nazwy scenariusza, jego kodu, opisu scenariusza oraz zaproponowanie funkcji bezpieczeństwa w ramach systemu automatyki zabezpieczeniowej SIS.

Analizę LOPA można przeprowadzać dla kilku scenariuszy awaryjnych. Po wpisaniu niezbędnych danych w oknie zaprezentowanym na poprzednim rysunku zdefiniowany scenariusz można zapisać i przechowywać w pamięci programu. W przypadku konieczności wyszukaniażądanego, zdefiniowanego i zapisanego wcześniej scenariusza możliwy jest jego wybór za pomocą kodu scenariusza (*Rysunek 23*).



Rysunek 23. Analiza LOPA wybór scenariuszy
Po zdefiniowaniu scenariusza analizy można przystąpić do właściwej analizy. Okno do

przeprowadzania analizy LOPA w wersji podstawowej w aplikacji ProSIL (Rysunek 24).



Rysunek 24. Okno podstawowej analizy LOPA

W oknie występują wszystkie elementy niezbędne do wykonania analizy. Należy zdefiniować zdarzenie inicjujące mogące doprowadzić do poważnej awarii, określić poziom krytyczności skutków dla dostępnych kategorii (przypisanie wartości tolerowanej) oraz przyporządkować warstwy zabezpieczające powstaniu poważnej awarii przemysłowej wraz z wartościami odnośnie do prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na żądanie przez każdą z nich PFD. Ryzyko po zastosowaniu warstw zostaje porównane z wartościami ryzyka tolerowanego dla przewidywanych skutków i w oparciu o wynik porównania generowana jest informacja, czy konieczna jest dalsza redukcja ryzyka. Jeśli nie kryteria zostały spełnione. Jeśli tak konieczne jest rozważenie dodatkowych warstw zabezpieczeniowych w celu spełnienia kryteriów.

6. Podsumowanie

W niniejszym artykule przedstawiono możliwości prototypowego oprogramowania ProSIL do wspomagania zarządzania bezpieczeństwem funkcjonalnym. Narzędzie komputerowe ProSIL zawiera odpowiednie moduły i bazy danych do prowadzenia projektów analizy bezpieczeństwa funkcjonalnego dla danego obiektu złożonego lub instalacji procesowej. Umożliwia definiowanie scenariuszy awaryjnych bazujących na wynikach metody HAZOP lub uproszczonej metody drzew zdarzeń ET z uwzględnieniem występujących zagrożeń i zdarzeń inicjujących.

Użytkownik programu ProSIL ma możliwość definiowania matrycy ryzyka do przedstawienia poziomów ryzyka związanego z wyróżnionymi scenariuszami. W aplikacji istnieje biblioteka grafów ryzyka z możliwością definiowania i modyfikowania parametrów związanych z ryzykiem. Aplikacja ProSIL pozwala na definiowanie zbioru funkcji bezpieczeństwa w ramach danego projektu (konkretny obiekt złożony lub instalacja w projektowaniu lub eksploatacji). Wyznaczanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla wybranej funkcji bezpieczeństwa odbywa się za pomocą modułów: grafu ryzyka lub matrycy ryzyka z odpowiednimi interfejsami graficznymi. Architektura sprzętu realizującego funkcję bezpieczeństwa jest przedstawiana za pomocą schematów blokowych z wyróżnieniem podsystemów i elementów.

Modelowanie probabilistyczne systemów przeprowadzane jest na podstawie modeli probabilistycznych podsystemów traktowanych ogólnie jako systemy „k z n” składające się z jednakowych oraz z różnych elementów. Oprogramowanie ProSIL zawiera bibliotekę modeli probabilistycznych podsystemów zgodnie z PN-EN 61508 oraz modeli w wersji rozszerzonej wyznaczonych metodami cięć minimalnych (uzyskanych na przykład na podstawie metody schematów blokowych RDB lub drzew niezdatności FT) i grafów Markowa.

W wersji podstawowej aplikacji dostępna jest ogólna baza danych niezawodnościowych i innych parametrów modeli probabilistycznych wyróżnionych kategorii elementów (lub podsystemów) z możliwością jej aktualizacji; aplikacja pozwala użytkownikowi na wprowadzenie własnych danych niezawodnościowych, w tym również danych z istniejących baz danych niezawodnościowych z podaniem źródła informacji. Aplikacja umożliwia optymalizowanie czasów testowania nieautomatycznego elementów (lub podsystemów) w systemie E/E/PE lub SIS.

Moduł weryfikacji SIL pozwala na wyznaczenie i graficzną reprezentację przebiegu w czasie prawdopodobieństwa niezadziałania na przywołanie PFD(t) oraz obliczanie przeciętnego prawdopodobieństwa PFD_{avg} podsystemów i systemów E/E/PE i SIS dla rodzaju pracy. W programie ProSIL warstwy zabezpieczeń są analizowane w nawiązaniu do metodyki LOPA oraz wymagań zawartych w normie PN-EN 61511.

Aplikacja komputerowa ProSIL w wersji wdrożeniowej będzie w przyszłości poddana

weryfikacji i ocenie na spełnienie wymagań dotyczących narzędzi do stosowania w analizach i zarządzaniu bezpieczeństwem funkcjonalnym.

Podziękowanie

Autorzy niniejszego artykułu dziękują Ministerstwu Nauki i Szkolnictwa Wyższego za wsparcie badań oraz Centralnemu Laboratorium Ochrony Pracy – Państwowemu Instytutowi Badawczemu za współpracę w przygotowaniu projektu badawczego VI.B.10 do realizacji w latach 2011-13 dotyczącego zarządzania bezpieczeństwem funkcjonalnym w obiektach podwyższonego ryzyka z włączeniem zagadnień zabezpieczeń / ochrony i niezawodności człowieka.

Literatura

- [1] Barnert, T., Kosmowski, K. & Śliwiński, M. (2006). Methodological aspects of functional safety assessment. *Zagadnienia Eksploatacji Maszyn*. Instytut Technologii Eksploatacji - Państwowy Instytut Badawczy.
- [2] Barnert, T & Śliwiński, M. (2007). *Methods for verification safety integrity level in control and protection systems, Functional Safety Management in Critical Systems*. Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk, s. 171-185.
- [3] Barnert, T., Kosmowski, K.T. & Śliwiński, M (2008). Determining and verifying the safety integrity level of the control and protection systems under uncertainty. *Materiały konferencji ESREL 2008 European Safety & Reliability Conference*, Walencja.
- [4] IEC 61508. (2010). Functional safety of electrical/electronic/programmable electronic safety – related systems. Parts 1-7. International Electrotechnical Commission (IEC).
- [5] IEC 62061. (2005). Safety of machinery – Functional safety of safety-related electrical/ electronic and programmable electronic control systems (E/E/PE). International Electrotechnical Commission (IEC).
- [6] PN-EN 61508 (2004). Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1-7. Polski Komitet Normalizacyjny.
- [7] PN-EN 61511. (2004). Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1-3. Polski Komitet Normalizacyjny.
- [8] Reliability Data for Safety Instrumented Systems - PDS Data Handbook. (2010). Edition, ISBN 978-82-14-04849-0, SINTEF A13502.
- [9] Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook. (2010). Edition, ISBN 978-82-14-04849-0, SINTEF A13502.

*Barnert Tomasz, Kacprzak Przemysław, Kosmowski Kazimierz, Kozyra Maciej, Porzeziński Michał,
Śliwiński Marcin, Zawalich Jacek*

ProSIL software for computer aided functional safety management

Program komputerowy ProSIL do wspomagania zarządzania bezpieczeństwem funkcjonalnym
