XXIII Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE' 2013
Oddział Gdański PTETiS
Referat nr 34

WSPOMAGANA KOMPUTEROWO WERYFIKACJA POZIOMU NIENARUSZALNOŚCI BEZPIECZEŃSTWA SIL Z WYKORZYSTANIEM AUTORSKIEJ APLIKACJI ProSIL

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

1. 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
2. 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
3. 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

Streszczenie: W referacie przedstawiono oprogramowanie Pro SIL wspomagające zarządzanie bezpieczeństwem funkcjonalnym. Program ProSIL składa się z trzech modułów wspomagających: określanie wymaganego poziomu SIL (moduł ProSILen) weryfikację SIL (moduł ProSILer) oraz przeprowadzenie analizy warstw zabezpieczeń metodą LOPA (moduł ProSIL/LOPA). W aplikacji ProSIL zaimplementowano opracowaną w trakcie badań metodykę analizy bezpieczeństwa funkcjonalnego w projektowaniu i użytkowaniu systemów SIS zgodnie z wymaganiami PN-EN 61508 i PN-EN 61511.

Słowa kluczowe: modelowanie probabilistyczne, weryfikacja poziomu nienaruszalności bezpieczeństwa SIL

1. WIADOMOŚCI OGÓLNE

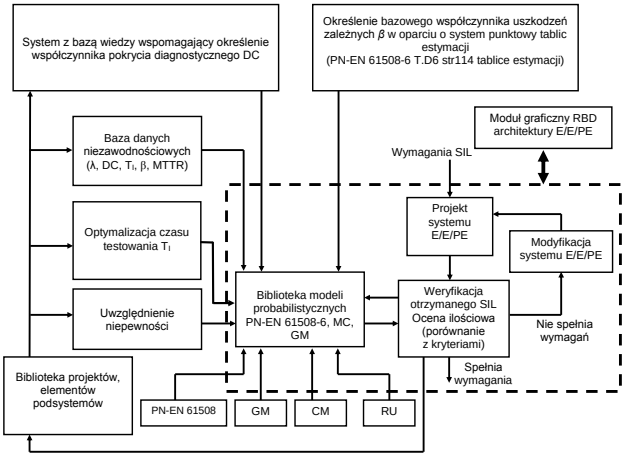
1.1. Wprowadzenie

Referat nawiązuje w swej tematyce do zagadnień związanych z procesem weryfikacji poziomów nienaruszalności bezpieczeństwa SIL (ang. Safety Integrity Level) określonych dla zdefiniowanych funkcji bezpieczeństwa, które realizowane są przez systemy sterowania BPCS (ang. Basic Process Control System) i zabezpieczeń SIS (ang. Safety Instrumented System), zawierające elementy elektryczne, elektroniczne i programowalne elektroniczne E/E/PE (ang. Electrical/Electronic/Programmable Electronic System). Systemy te są jednym ze środków pozwalających na zmniejszenie ryzyka pochodzącego od instalacji technicznej i procesu [1, 2]. Istnieje problem właściwego zaprojektowania systemu E/E/PE [4]. Problematyka dotycząca weryfikacji SIL zawarta jest w części szóstej normy PN-EN 61508 oraz w normach sektorowych PN-EN 61511 (przemysł procesowy) i PN-EN 62061 (przemysł maszynowy) [5, 6].

1.2. Moduł ProSILer w oprogramowaniu ProSIL

Oprogramowanie ProSIL składa się z trzech niezależnych modułów bazowych. Pierwszy moduł służy do wyznaczania poziomu nienaruszalności bezpieczeństwa SIL, drugi pozwala na komputerowo wspomaganą weryfikację tych poziomów. ProSIL zawiera również moduł wspomagający przeprowadzenie analizy warstw zabezpieczeń LOPA. Moduł do weryfikacji SIL w oprogramowaniu ProSIL posiada nazwę ProSILer [3].

Moduł ProSILer zawiera bibliotekę modeli probabilistycznych elementów i podsystemów bazowych wyznaczonych na podstawie: techniki schematów blokowych niezawodności RBD (ang. Reliability Block Diagram); grafów Markowa; analizy drzewa niezdatności (wykorzystanie cięć minimalnych) oraz równań uproszczonych. W bibliotece znajdują się również modele gotowych typowych struktur elementów i podsystemów E/E/PE (SIS i BPCS) zaadoptowanych z PN-EN 61508-6 i PN-EN 61511 [1, 3, 5, 6, 8]. Strukturę modułu weryfikacji SIL ProSILer przedstawiono na rysunku 1.



Rys.1. Struktura modułu weryfikacji SIL w aplikacji ProSIL

Modelowanie probabilistyczne systemów E/E/PE i SIS z wykorzystaniem modułu ProSILer przeprowadzane jest na podstawie modeli probabilistycznych podsystemów, które traktowane są ogólnie jako nadmiarowości *k z n*. Moduł weryfikacji SIL zawiera bazę danych niezawodnościowych ogólnych wraz z innymi parametrami modeli

probabilistycznych podstawowych elementów, istnieje możliwość ich aktualizacji dla wyróżnionych kategorii i podkategorii projektowanych systemów.

W module weryfikacji przewidziano możliwość wprowadzania przez użytkownika własnych danych niezawodnościowych na podstawie innych bibliotek i istniejących baz danych niezawodnościowych z udokumentowaniem źródła danych, które musi się znaleźć w raporcie wynikowym weryfikacji warstwy sprzętowej realizującej daną funkcję bezpieczeństwa. Biblioteka projektów i elementów podsystemów w module ProSILer jest na bieżąco aktualizowana [3, 7].

Prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez system zabezpieczeniowy realizujący funkcje związane z bezpieczeństwem można określić na podstawie zależności:

$$PFD(t) \cong (1 - e^{-\lambda_D t}) \approx \lambda_D t \qquad (1)$$

gdzie: λ_D – intensywność uszkodzeń niebezpiecznych; t – czas.

Wykorzystując zależność (1), można obliczyć przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie, zakładając, że poszczególne podsystemy są testowane z czasem między testami okresowymi T_I, mającymi na celu wykrycie uszkodzeń niebezpiecznych:

$$PFD_{avg} = \frac{1}{T_I} \int_0^{T_I} PFD(t)dt \qquad (2)$$

gdzie: T_I – interwał przeprowadzania testów okresowych.

Prawdopodobieństwo uszkodzenia niebezpiecznego na godzinę PFH może być oszacowane na podstawie wzoru przedstawionego poniżej:

$$PFH \approx \frac{1 - R(T)}{T} = \frac{1 - \exp(-\lambda_{avg} \cdot T)}{T}$$
$$gdy \quad \lambda_{avg} \cdot T << 1 \qquad (3)$$
$$PFH \approx \frac{\lambda_{avg} \cdot T}{T} = \lambda_{avg}$$

gdzie: R(T) – niezawodność podsystemu/elementu systemu E/E/PE w chwili T; λ_{avg} – przeciętna intensywność uszkodzeń podsystemu/elementu systemu E/E/PE.

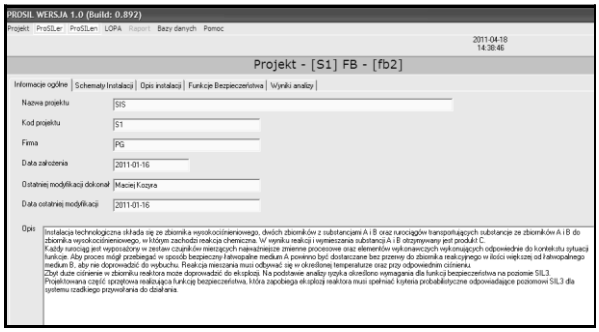
Moduł weryfikacji SIL zapewnia możliwość optymalizowania czasów testowania oraz opcjonalnie w wersji rozszerzonej uwzględnienia niepewności i wpływu błędów systematycznych na wartości końcowe prawdopodobieństw PFD_{avg} i PFH. Określanie współczynnika pokrycia diagnostycznego DC w module weryfikacji SIL w aplikacji ProSIL jest wspomagane przez system z bazą wiedzy. Uwzględnienie uszkodzeń o wspólnej przyczynie w modelowaniu probabilistycznym systemów E/E/PE i SIS w module weryfikacji SIL jest realizowane poprzez zastosowanie współczynnika uszkodzeń zależnych β. Współczynnik β jest wyznaczany na podstawie tablic estymacji dla struktury bazowej tzn. równoległej (1 z 2), dla pozostałych konfiguracji nadmiarowych współczynnik ten jest modyfikowany przez mnożnik korekcyjny [1, 5, 8].

W module weryfikacji przebiegi prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa PFD(t) dla systemu SIS, jego podsystemów i elementów przedstawiane są w module graficznym wraz z naniesionymi odpowiednio wartościami przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na żądanie PFD_{avg}. Architektura warstwy sprzętowej realizującej funkcję bezpieczeństwa w module ProSILer jest przedstawiana w postaci schematów blokowych z wyróżnieniem elementów, podsystemów i modułów systemu E/E/PE lub SIS w specjalnym module graficznym (oknie projektowym).

2. WERYFIKACJA POZIOMÓW SIL

2.1. Okno główne oprogramowania ProSIL

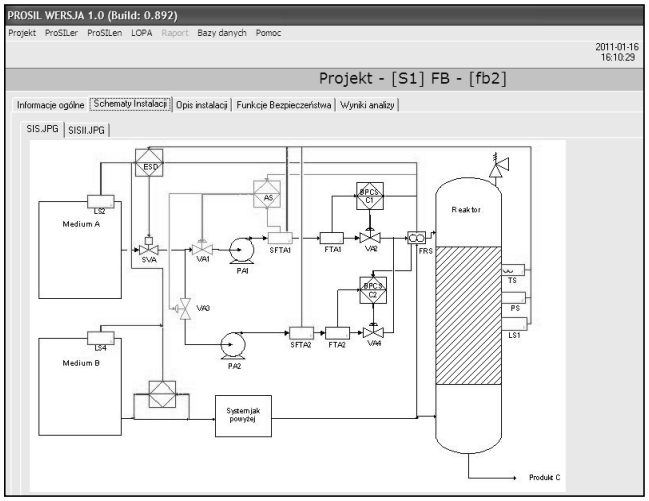
Na rysunku 2 znajduje się główne okno projektu w oprogramowaniu ProSIL.



Rys. 2. Okno główne projektu

Na górnym pasku okna użytkownik ma do wyboru bezpośrednie przejście do modułów określania, weryfikacji i analizy LOPA. Każdy nowowprowadzony projekt posiada szczegółowy opis, który jest przechowywany w bazie danych aplikacji ProSIL.

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



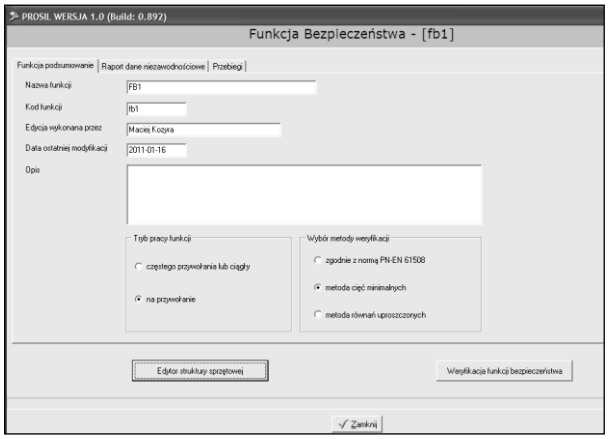
Rys. 3. Schemat instalacji procesowej

Oprogramowanie ProSIL umożliwia wprowadzenie zbioru funkcji bezpieczeństwa zidentyfikowanych wcześniej na etapie analizy zagrożeń. Metody pozwalające na identyfikację zagrożeń, takie jak np. HAZOP nie zostały jednak zaimplementowane z uwagi na utrzymanie prostoty i przejrzystości interfejsu. Ta możliwość brana jest pod uwagę w kolejnej, rozbudowanej wersji programu. 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.

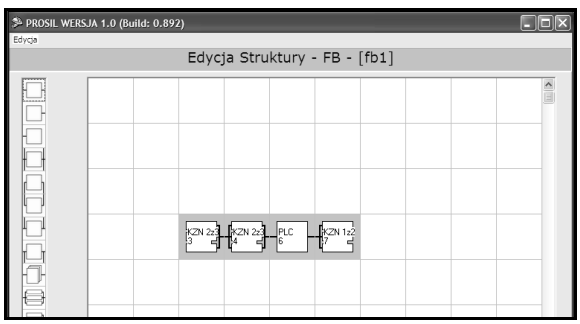
2.2. Moduł wspomagający weryfikację SIL

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 4 przedstawiono okno główne modułu weryfikacji SIL (ProSILer).



Rys. 4. Okno główne modułu wspomagającego weryfikację SIL

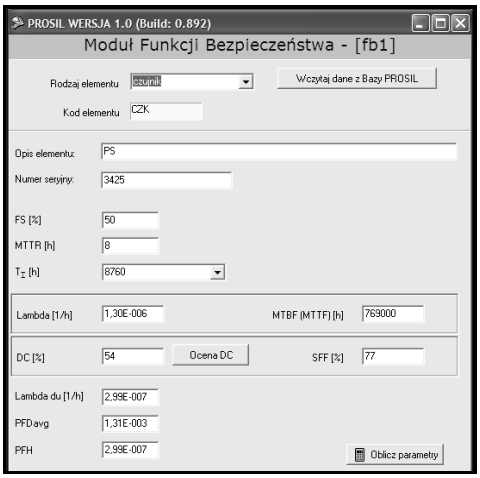
W oknie głównym modułu weryfikacji SIL aplikacji ProSIL należy wprowadzić nazwę funkcji bezpieczeństwa realizowanej przez warstwę SIS, kod funkcji, dane osoby odpowiedzialnej za wprowadzenie modelu struktury sprzętowej funkcji bezpieczeństwa oraz datę ostatniej modyfikacji. Można dodatkowo zamieścić 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 [1, 5, 6]. 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 (przedstawionego na rysunku 5) struktury sprzętowej funkcji bezpieczeństwa, wybierając przycisk „Edytor struktury sprzętowej".



Rys. 5. Edytor graficzny struktury warstwy sprzętowej SIS

Projektowana funkcja bezpieczeństwa ma postać 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 ich zamieszczeniu należy dokonać testu połączeń bloków, wybierając przycisk „Test struktury".

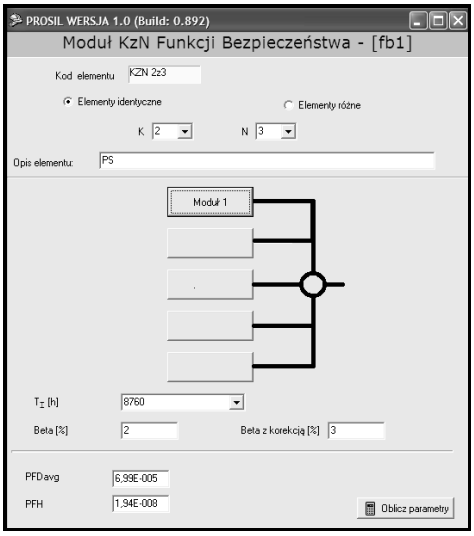
Na rysunku 6 przedstawiono edytor graficzny pojedynczego elementu funkcji bezpieczeństwa.



Rys. 6. Dane niezawodnościowe pojedynczego elementu systemu SIS

Dane niezawodnościowe dla pojedynczego elementu funkcji bezpieczeństwa np. czujnika temperatury, mogą być wprowadzone do systemu ręcznie przez projektanta lub automatycznie z bazy danych ProSILcdb. Użytkownik posiadający dokładne dane odnośnie wartości pokrycia diagnostycznego ma możliwość bezpośredniego wpisania ich w odpowiednie pole oznaczone symbolem „DC [%]". W przypadku, gdy nie ma takich danych można uruchomić moduł wspomagający dobór tego współczynnika.

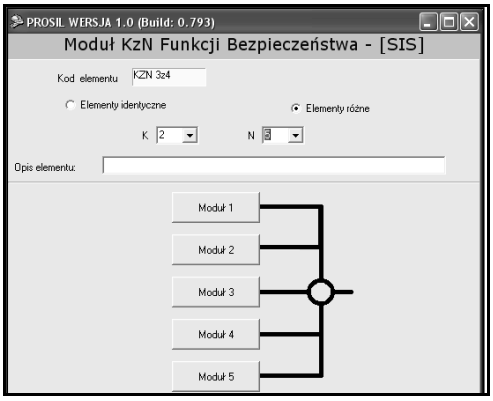
W oknie dialogowym zastosowano podział całego podsystemu realizującego funkcje bezpieczeństwa, na elementy pomiarowe, logiczne i wykonawcze (rys. 5). Po kliknięciu prawym klawiszem myszy na symbol graficzny struktury k z n pojawia się okno przedstawione na rysunku 7.



Rys. 7. Struktura k z n dla identycznych elementów

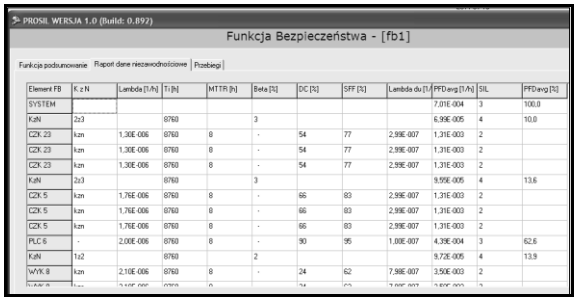
Struktura k z n ma wyższy poziom w hierarchii od pojedynczego elementu, zawiera bowiem pojedyncze elementy o określonym modelu probabilistycznym. Struktura k z n może

składać się z jednakowych bądź różnych elementów, co przedstawiono na rysunku 8.



Rys. 8. Struktura k z n - różne elementy

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" (rys. 4). Po uruchomieniu weryfikacji pojawia się tablica raportu z weryfikacji SIL w aplikacji ProSIL co przedstawiono na rysunku 9 (osobno dla trybu pracy „ciągłej" lub „na przywołanie").



Rys. 9. Okno raportu weryfikacji SIL

Po dokonaniu weryfikacji wyznaczone zostają wartości PFD_{avg}, PFH dla rozpatrywanego systemu E/E/PE, oraz jego podsystemów i elementów. Wartości te przedstawione są w postaci raportu (zawierającego dane wynikowe oraz schemat analizowanej struktury).

3. PODSUMOWANIE

W niniejszym referacie przedstawiono komputerowy proces wspomagania zarządzania bezpieczeństwem funkcjonalnym z wykorzystaniem oprogramowania ProSIL. Narzędzie to zawiera odpowiednie moduły i bazy danych do prowadzenia projektów analizy bezpieczeństwa funkcjonalnego dla danego obiektu złożonego lub instalacji procesowej. Aplikacja ProSIL pozwala na definiowanie zbioru funkcji bezpieczeństwa w ramach danego projektu (konkretny obiekt złożony lub instalacja w projektowaniu lub eksploatacji). W procesie weryfikacji architektura sprzętu realizującego funkcję bezpieczeństwa jest przedstawiana za pomocą schematów blokowych z wyróżnieniem podsystemów i elementów. W aplikacji ProSIL dostępna jest baza danych niezawodnościowych i innych parametrów modeli probabilistycznych wyróżnionych kategorii elementów (lub podsystemów) z możliwością jej aktualizacji. Oprogramowanie ProSIL umożliwia także optymalizowanie czasów testowania elementów (lub podsystemów) w systemie E/E/PE lub SIS. Moduł weryfikacji SIL pozwala także na wyznaczenie i graficzną reprezentację przebiegu prawdopodobieństwa PFD(t) co jest bardzo przydatne w procesie optymalizowania czasów testowania elementów (lub podsystemów) i ich wpływu na wartości prawdopodobieństw PFD_{avg} oraz PFH.

4. BIBLIOGRAFIA

1. Barnert T., Śliwiński M.: Methods for verification safety integrity level in control and protection systems. Functional Safety Management in Critical Systems. Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk 2007 s. 171-185, ISBN 978-83-7531-006-1.
2. Barnert T., Kosmowski K.T., Śliwiński M.: Determining and verifying the safety integrity level of the control and protection systems under uncertainty. ESREL 2008 European Safety & Reliability Conference, Valencia, 2008
3. Barnert T., Kosmowski K.T., Śliwiński M.: A knowledge-based approach for functional safety management. Taylor & Francis Group, European Safety & Reliability Conference ESREL, Praga, Czechy, 2009.
4. Barnert T., Kosmowski K.T., Śliwiński M.: Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issues. PSAM, Seattle, USA, 2010.
5. PN-EN 61508. Functional safety of electrical/electronic/programmable electronic safety – related systems. Parts 1-7. International Electrotechnical Commission (IEC), 2010.
6. PN-EN 61511. Functional safety: Safety instrumented systems for the process industry sector. Parts 1-3. International Electrotechnical Commission (IEC), 2000.
7. Reliability Data for Safety Instrumented Systems - PDS Data Handbook. SINTEF 2010 Edition, ISBN 978-82-14-04849-0, SINTEF A13502.
8. Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook. SINTEF 2010. Edition, ISBN 978-82-14-04849-0, SINTEF A13502.

ProSIL SOFTWARE SYSTEM FOR COMPUTER AIDED SAFETY INTEGRITY LEVEL VERIFICATION

Key-words: probabilistic modelling, safety integrity level (SIL) verification

In this article a prototype ProSIL software system for computer-aided functional safety management is discribed. The software consists of three modules for: determination of the required SIL level (ProSILen), verification of the SIL level (ProSILer), 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.