XXIV Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE 2014

Oddział Gdański PTETiS

METODA ANALIZY NIEZAWODNOŚCI CZŁOWIEKA SPAR-H W APLIKACJI ProSIL-EAL

Emilian PIESIK[1], Tomasz BARNERT[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: e.piesik@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: m.sliwinski@ely.pg.gda.pl

Streszczenie: W referacie przedstawiono zagadnienie wyznaczania prawdopodobieństwa błędu człowieka HEP za pomocą metody SPAR-H w oprogramowaniu ProSIL-EAL. Oprogramowanie wspomaga proces zarządzania bezpieczeństwem funkcjonalnym w cyklu życia systemów technicznych. Prawdopodobieństwo błędu człowieka jest zagadnieniem związanym z etapem weryfikacji określonych poziomów nienaruszalności bezpieczeństwa SIL dla funkcji bezpieczeństwa. ProSIL-EAL zapewnia wspomaganie w ocenie rozwiązań technicznych i organizacyjnych, jak również ochrony informacji, wpływu błędów systematycznych oprogramowania i błędów człowieka podczas eksploatacji systemów E/E/PE, BPCS i SIS.

Słowa kluczowe: SPAR-H, bezpieczeństwo funkcjonalne, prawdopodobieństwo błędu człowieka HEP

1. WIADOMOŚCI OGÓLNE

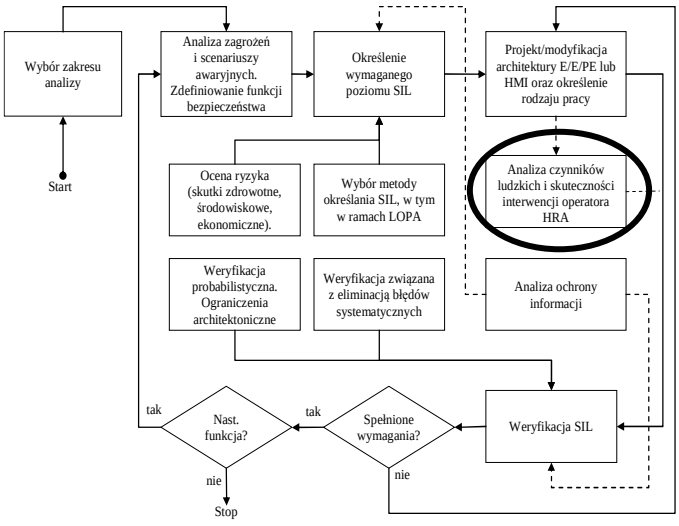
1.1. Wprowadzenie

Pierwsze systematyczne badania niezawodności człowieka były prowadzone, jako próba rozwoju bazy współczynników prawdopodobieństwa błędów personelu. Na początku lat 70. XX wieku pojawiły się pierwsze kompleksowe techniki oceny niezawodności człowieka. Prace badawcze pokazują fakt, iż szeroko rozumiane błędy człowieka uwarunkowane czynnikami ludzkimi i organizacyjnymi są przyczynami aż 70-90% wypadków i awarii przemysłowych [1]. Bezpieczeństwo systemów E/E/EP w ramach sterowania i/lub automatyki zabezpieczeniowej zależy w istotny sposób od czynników ludzkich, które należy rozpoznawać i kształtować tak, aby ograniczać wpływ błędów człowieka na ryzyko związane z eksploatacja systemów technicznych.

W ostatnim czasie zauważalnym jest wzrost znaczenia bezpieczeństwa funkcjonalnego w przemyśle, co wiąże się z opublikowaniem dokumentów normatywnych, w normie IEC 61508 [2] występują wymagania dotyczące analizy czynników ludzkich. W raporcie [3] zestawiono wiele odnośników do szeroko rozumianej problematyki czynników ludzkich, które pojawiają się w różnych częściach tej normy [4]. Tak, więc norma IEC 61508 podkreśla znaczenie czynników ludzkich w analizie bezpieczeństwa funkcjonalnego, jednak nie zawiera jednoznacznych wymagań i wskazań metodycznych dotyczących analizy wpływu czynników ludzkich [4]. Stosowanie niezawodnych rozwiązań bezpieczeństwa funkcjonalnego wpływa bezpośrednio na zmniejszenie poziomu ryzyka związanego z funkcjonowaniem obiektów przemysłowych, wprowadza tym samym szereg wymagań oraz problemów w cyklu życia obiektu.

1.2. Informacje na temat aplikacji ProSIL-EAL

Aplikacja ProSIL-EAL jest rozwinięciem oprogramowania ProSIL służącego do zarzadzania bezpieczeństwem funkcjonalnym w cyklu życia systemów technicznych. W tej wersji aplikacja została rozwinięta o komponenty dotyczące zagadnień ochrony informacji w przemysłowych sieciach internetowych.



Rys. 1. Struktura funkcjonalna aplikacji komputerowej ProSIL-EAL z zaznaczonym modułem analizy czynników ludzkich [4]

Zagadnienia wpływu ochrony informacji na określanie wymaganego poziomu nienaruszalności SIL oraz jego weryfikacja jest zaimplementowana w najnowszej wersji

aplikacji w sposób niezależny od modułów aplikacji ProSIL. Oprogramowanie ProSIL-EAL zapewnia 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] co widać na rysunku 1.

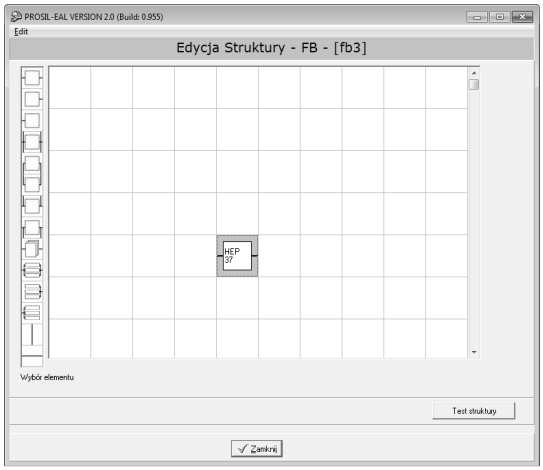
2. ANALIZA NIEZAWODNOŚCI CZŁOWIEKA

2.1. Metody analizy niezawodności człowieka

Niezawodność człowieka-operatora oszacować można ilościowo przy użyciu jednej z metod HRA (Human Reliability Analysis). W literaturze zidentyfikowano aż 72 metody HRA [6]. Szczególnie przydatną metodą w zastosowaniach praktycznych jest metoda SPAR-H. Metody HRA dają możliwość oszacowania prawdopodobieństw potencjalnych błędów człowieka HEP (Human Error Probability) w instalacji procesowej. Ponadto przy użyciu metod HRA można ocenić wpływ potencjalnych błędów człowieka na ryzyko wystąpienia rozpatrywanego scenariusza awaryjnego. Metody HRA bazują na opiniach ekspertów oraz danych reprezentowanych w postaci informacji jakościowej i/lub ilościowej.

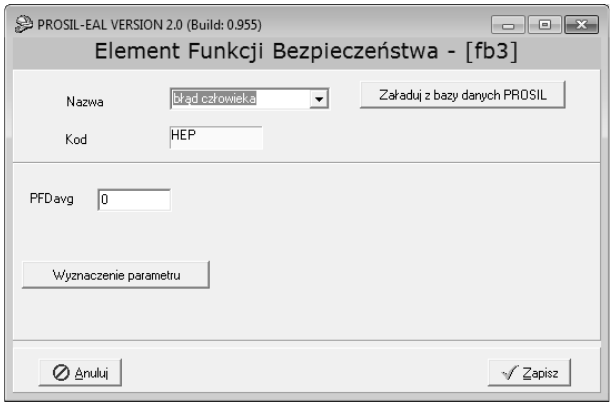
2.2. Metoda SPAR-H w aplikacji ProSIL-EAL

Metoda analizy niezawodności człowieka SPAR - H (Simplified Plant Analysis Risk Human Reliability Assessment) [7] została opracowana przez D. Gertmana i H. Blackmana, J. Marblea, J. Byersa, C. Smitha dla US Nuclear Regulatory Commission. Ma ona zastosowanie w przypadku obiektów przemysłowych o niedużym stopniu skomplikowania. Okno projektowe (przedstawione na rysunku 2) struktury sprzętowej funkcji bezpieczeństwa oprogramowania ProSIL-EAL zawiera element uwzględniający analizę niezawodności człowieka. Funkcja bezpieczeństwa ma postać schematów blokowych.



Rys. 2. Edytor graficzny struktury warstwy sprzętowej SIS z elementem dot. analizy niezawodności człowieka

Na rysunku 3 przedstawiono edytor graficzny pojedynczego elementu funkcji bezpieczeństwa, jakim jest HEP. W tym wypadku można zauważyć wartość PFD_{avg}, która oznacza prawdopodobieństwo niewypełnienia funkcji na przywołanie.



Rys.3. Element funkcji bezpieczeństwa – błąd człowieka

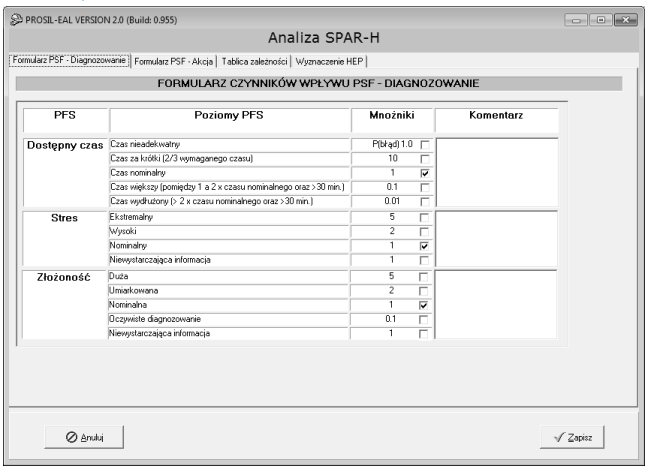
Jest to wartość wynikowa, która wynika z zależności

$$PFD_i = HEP_i \tag{1}$$

Wartość z powyższej zależności dla warstwy Operatora jest możliwa do przyjęcia w przypadku braku zależności z warstwą BPCS warstwowego systemu zabezpieczeń.

W metodzie SPAR - H dokonuje się dekompozycji zadań, jakie wykonuje człowiek - operator na dwa podstawowe elementy: działanie (action) i/lub diagnozowanie (diagnosis). W przypadku diagnozowania operator w celu zrozumienia i poprawnego przenalizowania aktualnej sytuacji musi posiadać odpowiednią wiedzę a także doświadczenie, aby zaplanować i wykonać odpowiednie działania, zapobiegające wystąpieniu poważnych awarii.

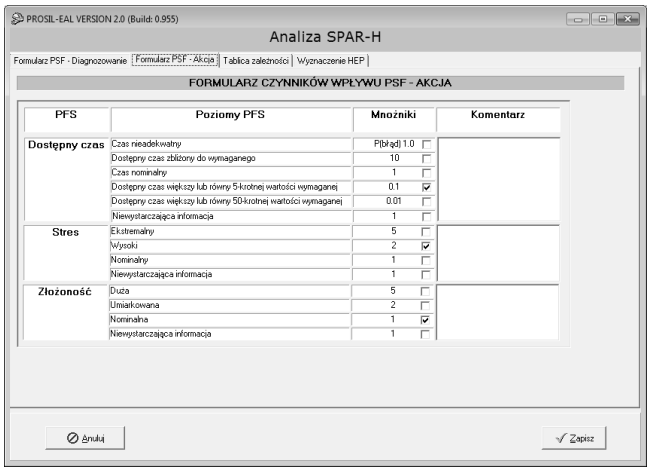
Prawdopodobieństwo błędu człowieka HEP w danej sytuacji w przypadku zadań złożonych z diagnozowania i działania składa się z sumy wartości nominalnych prawdopodobieństw błędów diagnozowania i działania. Prawdopodobieństwo wyliczane jest za pomocą odpowiednio skonstruowanych tablic z uwzględnieniem ośmiu czynników wpływu kształtujących wydajność człowieka PSF (Performance Shaping Factors).



Rys. 4. Tabela czynników wpływu dla „diagnozowania” w aplikacji ProSIL-EAL

Przykładowe czynniki wpływu dla diagnozowania w aplikacji ProSIL-EAL zostały przedstawione na rysunku 4 zauważyć można możliwość wyboru wartości dla poszczególnych czynników jak również skomentować dokonany wybór. Formularze mogą być modyfikowane w zależności od procesu, który podlega analizie. Czynniki w zależności od tego, jaka wartość zostanie im przypisana

mogą być pozytywne lub negatywne. Wybór wartości dla czynników wpływu jest zadaniem częściowo subiektywnym, ponieważ zależy od odczuć osoby wykonującej analizę. Powoduje to sytuacje, gdy analizy wykonywane przez różne zespoły mogą skutkować różnymi wynikami.



Rys. 5. Tabela czynników wpływu dla „działania" w aplikacji ProSIL-EAL

Przykładowe czynniki wpływu dla działania zostały przedstawione na rysunku 5 zauważyć można wartości poszczególnych czynników wpływu dla rozważanego systemu. Czynnik uważany jest za negatywny, jeżeli przypisana mu wartość jest większa od 1. Wartość normalna przyjmowana jest jako 1. Wartość poniżej 1 jest pozytywna i działa na korzyść. W przypadku, gdy w pojedynczym scenariuszu występują trzy lub więcej negatywne czynniki wpływu obliczana jest dodatkowo korekta prawdopodobieństwa wystąpienia błędu człowieka HEP.

W trakcie analizy można wziąć pod uwagę zależność pomiędzy zadaniami (dependency). Należy także zaznaczyć, że w przypadku wystąpienia zależności zdarzeń może ona mieć jedynie negatywny wpływ na końcową wartość HEP [8]. Metoda SPAR-H posiada trzy główne założenia. Pierwszym założeniem jest dekompozycja działań człowieka i prawdopodobieństwa odpowiednich błędów na błędy diagnozowania oraz błędy działania. Parametrem wyznaczającym ilościowo poziom niezawodności człowieka jest prawdopodobieństwo błędu człowieka HEP, uwzględnianie tego parametru jest kluczowe w metodzie.

Pamiętać należy, aby uwzględnić osiem czynników wpływu PSF kształtujących wydajność operatora. Zakłada się także wykorzystywanie określonej dla metody dokumentacji zapewniającej przejrzystość i spójność analizy wraz ze wskazówkami, w jaki sposób przypisywać odpowiednie poziomy dla każdego PSF.

Wyróżnia się następujące czynniki wpływu PSF: dostępny czas (time available), stres (stress), złożoność zadania (complexity), doświadczenie i trening (experience and training), ergonomia włącznie z HMI (ergonomics including HMI), dostępność procedur (procedures), sprawność do wykonania zadania, na którą może wpływać psychiczna i fizyczna kondycja operatora, zmęczenie, choroba, zbytnia pewność siebie, rozproszenie uwagi (fitness for duty), nadzór nad wykonywanymi zadaniami, planowanie zadań i czynniki organizacyjne łącznie rozumiane, jako przygotowanie procesu pracy (work processes).

Tablica 1. Fazy analizy niezawodności człowieka przy użyciu metody SPAR – H

Faza	Opis
1	Wpisanie podstawowych informacji w nagłówku tabeli dotyczących badanej instalacji oraz opisu sekwencji awaryjnej
2	Podjęcie decyzji, czy badane zdarzenie będzie wymagało diagnozowania lub działania czy obu tych elementów
3	Wykonanie obliczeń HEP dla diagnozowania bez uwzględnienia zależności. Jeśli przynajmniej trzem zmiennym PSF przypisano wartości negatywne należy wykonać obliczenie korygujące otrzymaną wartość HEP
4	Jeśli dla badanej sekwencji awaryjnej wymagane jest także działanie, należy powtórzyć punkt 3 dla działania
5	Obliczenie sumy HEP dla diagnozowania oraz działania
6	Dokonanie oceny stopnia zależności, jaki występuje dla danego scenariusza. Jeśli zależność nie występuje należy udokumentować przyczyny takiego stanu w odpowiednim miejscu w tabeli. W takim wypadku ostateczną wartością HEP jest liczba wyliczona w fazie 5
7	Jeśli zależność występuje i została przypisana do jednej z kategorii, wtedy należy obliczyć wartość zależności według zasad modyfikując wartość HEP obliczoną w fazie 5 w celu wyliczenia wartości ostatecznej.

Po wykonaniu kroków 1, 2 należy wykonać krok 3 z tablicy 1, należy obliczyć prawdopodobieństwo błędu dla diagnozowania według poniższych zasad. Jeśli wszystkie PSF mają wartość nominalną to prawdopodobieństwo błędu dla diagnozowania wynosi 0,01. W innym przypadku prawdopodobieństwo błędu dla diagnozowania obliczane jest, jako iloczyn wartości nominalnej 0,01 przez wartości przypisane dla każdego z PSF.

$$HEP_{diag} = 0{,}01 \cdot PSF_{złożon} \tag{2}$$

gdzie: HEP_{diag} –wartość prawdopodobieństwa błędu człowieka dla diagnozowania, $PSF_{złożon}$ - iloczyn wartości przypisanych do każdego PSF.

W przypadku, gdy występują trzy lub więcej negatywnych czynników wpływu PSF należy wykonać obliczenie korygujące otrzymaną wartość HEP. Wartość PSF jest zawsze uważana za negatywną, gdy przypisana mu wartość jest większa od 1. Nominalna wartość HEP (NHEP) dla diagnozowania wynosi 0,01. Wartość HEP z uwzględnieniem korekty jest obliczana według wzoru 3 i jest ostateczną wartością HEP.

$$HEP = \frac{NHEP \cdot PSF_{złożon}}{NHEP \cdot (PSF_{złożon} - 1) + 1} \tag{3}$$

gdzie: *HEP* – ostateczna wartość prawdopodobieństwa błędu człowieka z uwzględnieniem korekty, *NHEP* – wartość nominalna HEP dla diagnozowania, $PSF_{złożon}$ - iloczyn wartości przypisanych do każdego PSF.

W przypadku fazy 4 z tabeli 1 jeśli dla badanej sekwencji awaryjnej wymagane jest także działanie, należy powtórzyć punkt 3 dla działania. Następnie obliczyć prawdopodobieństwo błędu dla działania według poniższych zasad. Jeśli wszystkie PSF mają wartość nominalną to prawdopodobieństwo błędu dla działania wynosi 0,001. W innym przypadku prawdopodobieństwo błędu dla działania obliczane jest, jako iloczyn wartości nominalnej 0,001 i wartości przypisanych dla każdego z PSF

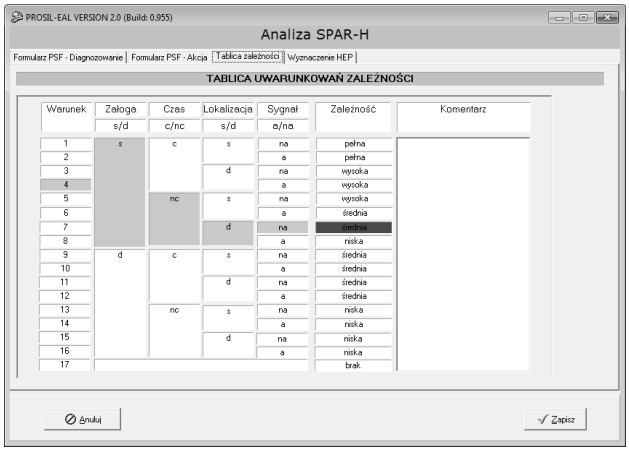
$$HEP_{działał} = 0{,}001 \cdot PSF_{złożon} \tag{4}$$

gdzie: $HEP_{działział}$ – wartość prawdopodobieństwa błędu człowieka dla działania, $PSF_{złożon}$ - iloczyn wartości przypisanych do każdego PSF.

W przypadku konieczności obliczenia współczynnika korekcyjnego jest on obliczany według zasad opisanych w fazie 4 korzystając z wzoru 3 przy założeniu NHEP wynoszącego 0,001. Faza 5 dotyczy obliczenia sumy HEP dla diagnozowania oraz działania bez uwzględnienia zależności ($P_{(B/Z)}$), jeśli obie te czynności wystąpiły według zasad opisanych poniżej.

$$P_{(B/Z)} = HEP_{diag} + HEP_{działział} \quad (5)$$

Dokonanie oceny stopnia zależności, jaki występuje dla danego scenariusza wykonywane jest w fazie 6. W przypadku braku zależności ostateczną wartością HEP jest liczba wyliczona w fazie 5. Jeśli zależność występuje i została przypisana do jednej z kategorii występujących w poniższej tabeli, przedstawionej na rysunku 6 wykonywana jest faza 7. Należy obliczyć wartość zależności modyfikując wartość HEP obliczoną w fazie 5 w celu wyliczenia wartości ostatecznej.



Rys. 6. Tabela zależność między zadaniami aplikacji ProSIL-EAL

Dla wszystkich zadań, z wyjątkiem pierwszego zadania w sekwencji skorzystać należy z tabeli przedstawionej na rysunku 6.

3. PODSUMOWANIE

W niniejszym referacie przedstawiono metodę analizy niezawodności człowieka SPAR-H w oprogramowaniu ProSIL-EAL. Narzędzie, jakim jest ProSIL-EAL posiada moduły i bazy danych do przeprowadzania analiz bezpieczeństwa funkcjonalnego z uwzględnieniem aspektów ochrony informacji dla danej instalacji procesowej. Architektura sprzętu realizującego daną funkcje bezpieczeństwa w tym także analiza niezawodności człowieka jest realizowana za pomocą schematów blokowych. Za pomocą oprogramowania ProSIL-EAL można dokonać analizy niezawodności człowieka jak również dokonać oceny wpływu czynników ludzkich na funkcję bezpieczeństwa.

4. BIBLIOGRAFIA

1. Kosmowski K.T.: Niezawodność człowieka: Zapobieganie stratom w przemyśle (red. A.S. Markowski): część III „Zarządzenie bezpieczeństwem procesowym", rozdz. 5. Wydawnictwo Politechniki Łódzkiej, Łódź 2001, ISBN 7283-001-0
2. PN-EN 61508: Bezpieczeństwo funkcjonalne E/E/EP systemów związanych z bezpieczeństwem. Części 1-7, Polski Komitet Normalizacyjny, 2004
3. Carey M.: Proposed framework for addressing human factors in IEC 61508. Amey VECTRA Limited for the Health and Safety Executive (HSE), Report 373/2001. HSE Books, Sudbury, Suffolk 2001
4. Barnert T., Kacprzak P., Kosmowski K.T., Kozyra M., Porzeziński M., Śliwiński M. Opracowanie metod i narzędzi do wspomagania oceny wpływu czynników ludzkich na częstość zdarzeń inicjujących i ryzyko scenariuszy awaryjnych w celu zastosowania efektywnych rozwiązań technicznych i organizacyjnych sprzyjających redukcji prawdopodobieństwa błędów człowieka i ryzyka wystąpienia strat. Sprawozdanie z I etapu projektu VI.B.10, CIOP-PIB, 2011
5. Barnert T., Kosmowski, K.T., Śliwiński, M.: ProSIL software for functional safety management in life cycle, Journal of KONBiN, Warszawa 2013
6. Bell J. Holroyd J.: Review of human reliability assessment methods - prepared by the Health and Safety Laboratory for the Health and Safety Executive (HSE). Buxton, Derbyshire 2009
7. SPAR-H: Human Reliability Analysis (HRA) Method, NUREG/CR-6883, INL/EXT-05-00509, USNRC, 2005
8. Barnert T., Kacprzak P., Kosmowski K.T., Kozyra M., Porzeziński M., Śliwiński M., Zawalich J.: Opracowanie metod analizy i narzędzi do komputerowo wspomaganego zarządzania bezpieczeństwem funkcjonalnym w ramach systemu warstw zabezpieczeniowo-ochronnych obiektów przemysłowych podwyższonego ryzyka. Sprawozdanie z II etapu projektu 5.R.02, CIOP-PIB. 2009

HUMAN RELIABILITY ANALYSIS METHOD SPAR-H IN SOFTWARE PROSIL-EAL

Key-words: SPAR-H, functional safety, human error probability

The paper presents the problem of determining the probability of human error HEP using the SPAR-H method in ProSIL-EAL software. This software supports the functional safety management in the life cycle of technical systems. The probability of human error is the issue related to the stage of verification of certain levels SIL for safety functions. For the human factors analysis were applied SPAR-H method for the decomposition of tasks, made by operator for two elements: action and/or diagnosis.