XXVI Seminarium

ZASTOSOWANIE KOMPUTERÓW W NAUCE I TECHNICE 2016

Oddział Gdański PTETiS

ANALIZA NIEZAWODNOŚCI CZŁOWIEKA-OPERATORA W KONTEKŚCIE BEZPIECZEŃSTWA FUNKCJONALNEGO

Emilian PIESIK[1], Kazimierz T. KOSMOWSKI[2]

1. Politechnika Gdańska
   tel: 58 347 14 35 fax: 58 347 24 87 e-mail: emilian.piesik@pg.gda.pl
2. Politechnika Gdańska
   tel: 58 347 24 39 fax: 58 347 24 87 e-mail: kazimierz.kosmowski@pg.gda.pl

Streszczenie: Artykuł przedstawia niektóre kwestie analizy warstwowego systemu zabezpieczeń instalacji podwyższonego ryzyka z uwzględnieniem analizy niezawodności człowieka HRA (*human reliability analysis*). Działania człowieka operatora w odniesieniu do systemu operatorskiego HSI (*human system interface*), w tym systemu alarmowego i potencjalnych błędów człowieka mogą mieć istotny wpływ na wyniki analiz probabilistycznych w procesie weryfikacji poziomów nienaruszalności bezpieczeństwa SIL (*safety integrity level*). Wpływ ten może być analizowany przy użyciu wybranych metod HRA. W pracy przeanalizowano wpływ czynników ludzkich na prawdopodobieństwo błędu człowieka HEP (*human error probability*) korzystając z metod SPAR-H oraz HEART. Uzyskane wyniki HEP są analizowane dla wybranego scenariusza awaryjnego w kontekście rozwiązań bezpieczeństwa funkcjonalnego.

Słowa kluczowe: czynniki ludzkie, bezpieczeństwo funkcjonalne, system alarmowy, analiza niezawodności człowieka-operatora.

1. WPROWADZENIE

1.1. Wstęp

W ostatnim czasie wzrasta zainteresowanie analizami niezawodności człowieka w instalacjach i systemach technicznych, w których człowiek nadzoruje przebieg procesu przemysłowego. Okazuje się, że w sytuacjach nienormalnych, a szczególnie podczas awarii, diagnozowanie i działania człowieka są kluczowe w osiągnięciu określonych celów bezpieczeństwa. Rozwój przemysłu oraz technologii sprawia, że w sektorze przemysłu procesowego pojawia się coraz więcej rozwiązań bezpieczeństwa funkcjonalnego. Istotną rolę odgrywają tutaj warstwy zabezpieczeniowo-ochronne co wiąże się z opublikowaniem szeregu poradników i dokumentów normatywnych.

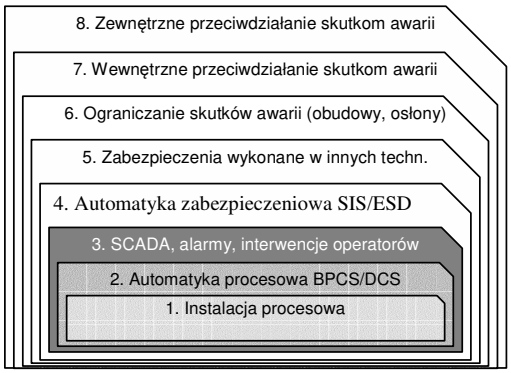
Znaczenie czynników ludzkich w bezpieczeństwie instalacji podkreśla się w nowych edycjach norm: IEC 61511 [1] oraz IEC 61508 [2], dotyczących projektowania i użytkowania systemów związanych z bezpieczeństwem. Jednakże stawiane w nich tylko ogólnie wymagania dotyczące zakresu analizy czynników ludzkich nie dają jednoznacznej odpowiedzi, w jaki sposób wyznaczyć na przykład prawdopodobieństwo błędu człowieka. Istniejące w tych dokumentach odwołania do opublikowanych pozycji literaturowych nie wskazują jak przeprowadzać analizę niezawodności człowieka HRA (*human reliability analysis*) z uwzględnieniem funkcji systemu alarmowego.

W raporcie [3] i opracowaniu [4] zestawiono liczne odwołania i uwagi do problematyki czynników ludzkich w kontekście różnych części norm bezpieczeństwa funkcjonalnego [1, 2]. Jak wiadomo, kategoria czynników ludzkich obejmuje nie tylko operatorów, ale również personel obsługi technicznej. Pełnią oni odpowiedzialne role w bezpiecznej eksploatacji instalacji. W niniejszym artykule skoncentrowano się na operatorach podejmujących decyzje oraz realizujących sterowania w sytuacjach nienormalnych i awaryjnych. W analizie częstości scenariusza awaryjnego danej instalacji przemysłowej należy oszacować m.in. prawdopodobieństwo błędu człowieka Q, oznaczane zwykle w publikacjach anglojęzycznych akronimem HEP (*human error probability*).

1.2. Przykładowy warstwowy system zabezpieczeń

Zadaniem warstw zabezpieczeniowo-ochronnych przedstawionych na rysunku 1 jest ograniczenie wpływu potencjalnych zdarzeń niepożądanych, takich jak np. zakłócenia wewnętrzne i zewnętrzne, a także zredukowanie częstości i skutków (czyli ryzyka) możliwych zdarzeń awaryjnych w rozważanej instalacji procesowej.

Wypełnienie funkcji bezpieczeństwa przewidzianych do zaimplementowania w systemie zabezpieczeń może być nieskuteczne z powodu niezdatności funkcjonalnej systemów występujących w warstwach 2, 3 i 4 na rysunku 1.



Rys. 1. Typowe warstwy zabezpieczeniowo-ochronne w instalacji procesowej

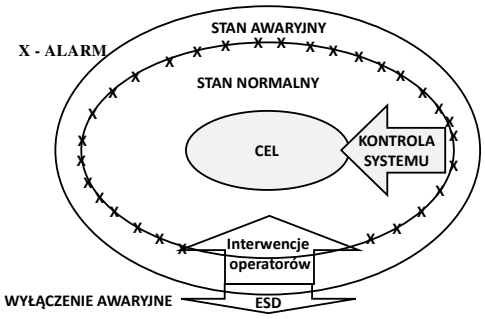
W analizie warstwowego systemu zabezpieczeń korzysta się z metody analizy LOPA (*layer of protection*

analysis) [5], przy czym rozważana funkcja bezpieczeństwa nie będzie w pełni wypełniona, jeśli zawiedzie dana i kolejne warstwy zabezpieczeń. Szczególne znaczenie w systemie zabezpieczeń mają warstwy trzecia i czwarta, co wynika z dużej złożoności systemu (BPCS/DCS) występującego w warstwie drugiej, a zatem większej jego zawodności.

1.3. Wyzwania w projektowaniu systemu alarmowego

Wpływ czynników ludzkich jest uzależniony od specyfiki procesu przemysłowego oraz przyjętych rozwiązań technicznych i organizacyjnych. Istotne znaczenie ma projekt system alarmowego. W procesie eksploatacji instalacji i użytkowania systemów sterowania istotne znaczenie odgrywają interfejsy człowiek-maszyna typu HMI (*human-machine interface*), a w przypadku bardziej złożonych i skomputeryzowanych instalacji, interfejsy typu HSI (human-system interface). Projekt interfejsów HMI/HSI powinien umożliwiać nieskomplikowaną i intuicyjną interakcję pomiędzy człowiekiem i systemem zgodnie z zasadami współczesnej ergonomii. Wymaga to współpracy projektanta i użytkownika od etapu koncepcyjnego [6].

Projektowanie systemu alarmowego AS (*alarm system*) stanowi szczególne wyzwanie. Ogólne zasady projektowania AS zawiera poradnik EEMUA [7]. Należy zwrócić uwagę na fakt, że operatorzy z powodu przeciążenia nieistotnymi alarmami lub "potokiem" alarmów mogą popełnić błędy. System alarmowy może mieć również niedoskonałości funkcjonalne lub ulec uszkodzeniu, uniemożliwiając operatorowi podejmowanie właściwych w danej sytuacji decyzji. Dotyczy to zwłaszcza AS zaprojektowanego w ramach BPCS, gdyż wówczas trudno jest uzyskać nawet najniższy poziom nienaruszalności bezpieczeństwa (*safety integrity level*) SIL1 [7, 8]. Rysunek 2 ilustruje osiągane stany systemu zależne od funkcjonalności systemu, kiedy wyświetlane alarmy są zrozumiałe dla operatorów i mogą oni podjąć właściwe działania.



Rys. 2. Stany systemu w zależności od działania systemu alarmowego [7]

Alarmy takie są oznaczone poprzez X i znajdują się w pobliżu okręgu oznaczającego obszar poprawnej pracy systemu. Niewłaściwe interwencje mogą spowodować na przykład niepotrzebne odstawienie instalacji, a w sytuacji zagrożenia stan awaryjny instalacji.

1.4. Istniejące metody i problematyka ich stosowania

Niezawodność człowieka operatora oszacować można ilościowo przy użyciu jednej z metod HRA. Metody te uwzględniają w modelach zawodności człowieka określone zbiory czynników wpływu PSF (*performance shaping factors*).

Metodą przydatną w zgrubnych analizach rozwiązań bezpieczeństwa funkcjonalnego jest metoda SPAR-H (*Simplified Plant Analysis Risk Human Reliability Assessment*) [9, 10]. W metodzie tej dokonuje się dekompozycji zadań, jakie wykonuje człowiek-operator na dwa podstawowe elementy: działanie (*action*) i/lub diagnozowanie (*diagnosis*).

Prawdopodobieństwo błędu popełnionego przez człowieka Q w danej sytuacji, w przypadku zadań złożonych z diagnozowania i działania, wyznacza się w przybliżeniu jako sumę prawdopodobieństw: błędów diagnozowania i błędów działania. Prawdopodobieństwa te szacuje się na podstawie odrębnych tablic z uwzględnieniem ośmiu czynników kształtujących działanie człowieka (PSF), przy czym każdemu czynnikowi przypisuje się zbiory: określeń słownych i wartości liczbowych.

W metodzie SPAR-H [10] wyróżnia się następujące czynniki wpływu $C_{w,k}$: 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*), przygotowanie do wykonania zadania (*fitness for duty*) i przygotowanie procesów pracy (*work processes*).

Jak widać, w metodzie SPAR-H występuje czynnik wpływu "dostępnego czasu" na wykonanie diagnozowania oraz działania. Ma on koncepcyjny związek z podejściem przyjętym w metodzie ASEP (*Accident Sequence Evaluation Programme*) [11], w której występuje ograniczenie czasowe ("okno czasowe") na przeprowadzenie diagnozowania, podjęcie decyzji i działanie, z powodu możliwej nieodwracalności procesów prowadzących do awarii. Wspomniana metoda ASEP została opracowana, aby zmniejszyć nakłady czasu i środków w przeprowadzaniu analiz HRA.

Wyniki uzyskiwane za pomocą metody ASEP i SPAR-H okazały się bardzo zbliżone do wyników otrzymywanych przy wykorzystaniu metody THERP, traktowanej przez ekspertów jako metoda odniesienia. W opracowaniu [4] zaleca się jednak stosować te pochodne metody w analizach bezpieczeństwa funkcjonalnego w przypadkach rozwiązań systemów E/E/PE lub SIS do poziomu SIL 3.

Metoda HEART [11] (*Human Error Assessment and Reduction Technique*) wymaga określenia zadań człowieka oraz czynników ergonomicznych i środowiskowych, które mogą wpływać negatywnie na wykonywanie tych zadań. W metodzie tej występuje 9 kategorii zadań z przypisanymi nominalnymi wartościami prawdopodobieństwa błędów człowieka, które poddaje się korekcie zależnie od czynników istotnych w danej sytuacji. Metoda HEART może być stosowana w analizie rozwiązań bezpieczeństwa funkcjonalnego. Okazała się ona szczególnie przydatna w kontekście projektowania interfejsów operatorskich.

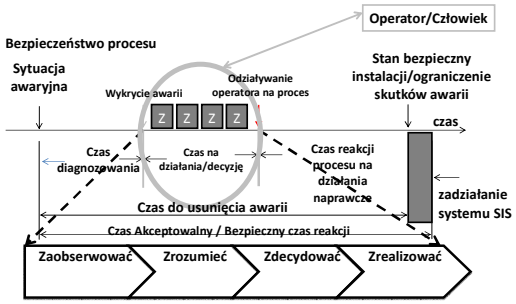
2. PROPOZYCJA PODEJŚCIA

2.1. Funkcje operatora

Istotnym aspektem w analizie niezawodności człowieka-operatora jest uwzględnienie projektu koncepcyjnego systemu alarmowego. Ma to szczególne znaczenie w instalacjach przemysłowych podwyższonego ryzyka, a zwłaszcza kiedy system alarmowy powinien być traktowany jako związany z bezpieczeństwem (*safety-related*) [7]. Wymaga to uwzględnienia interfejsu AS w analizie niezawodności człowieka, z uwzględnieniem czynników ludzkich [6, 7, 8]. Podstawowe znaczenie w tej analizie ma dostępny czas reakcji operatora, w którym przeprowadza on diagnozowanie stanu instalacji i podejmuje

wymagane działania, korzystając z opracowanych uprzednio procedur.

Rysunek 3 ilustruje zależności czasowe pomiędzy wystąpieniem sytuacji awaryjnej i działaniami operatora, mającymi na celu doprowadzenie instalacji do stanu bezpiecznego lub do ograniczenia skutków awarii. Wyróżnić można kilka faz postępowania operatora, czyli czas wymagany na diagnozowanie, podejmowanie decyzji oraz działania korekcyjne lub naprawcze.

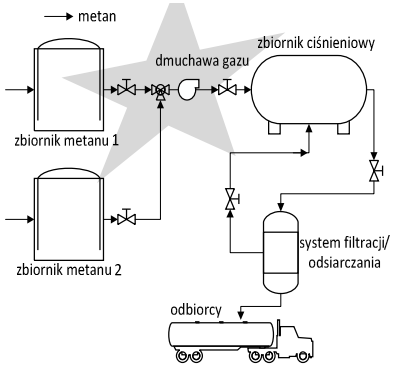


Rys. 3. Zależności czasowe pomiędzy wystąpieniem sytuacji awaryjnej i działaniami operatora

Podejście to nazwano 4Z: Zaobserwować/ Zrozumieć/ Zdecydować/ Zrealizować.

2.2. Analizowana instalacja

Rozpatrywanym systemem jest układ filtracji i odsiarczania biometanu wytwarzanego w biogazowni. Schemat tego układu przedstawiono na rysunku 4.



Rys. 4. Schemat instalacji podlegającej analizie

Wytworzony biometan jest tłoczony za pomocą dmuchawy do zbiornika o podwyższonym ciśnieniu. Ze zbiornika ciśnieniowego metan trafia do systemu filtracji, który ma za zadanie oczyścić biogaz ze szkodliwych substancji, które mogą spowodować korozję w instalacjach odbiorców. Zbiornik ciśnieniowy ze względu na specyfikę obiektu wykonany jest z wielowarstwowego tworzywa podatnego na uszkodzenia mechaniczne.

Instalacja filtracji biogazu wyposażona jest w interfejs operatorski oraz system alarmowy, który został zaprojektowany w ramach systemu BPCS. W sytuacji awaryjnej operator jest informowany o wystąpieniu zdarzenia przez system SCADA, który posiada funkcje alarmowania. Ponadto operator ma możliwość sterowania procesem za pomocą dedykowanego, dotykowego panelu HMI, który jest pozbawiony systemu alarmowego.

2.3. Przykład obliczeniowy

Rozważany scenariusz awaryjny dotyczy sytuacji, w której następuje uszkodzenie elementów instalacji przesyłu biogazu za dmuchawą gazu. W wyniku czego może nastąpić wzrost ciśnienia biogazu w zbiorniku, co może spowodować rozszczelnienie układu a w konsekwencji uwolnienie metanu. Rozpatrywana sytuacja została przedstawiona na rysunku 4. Wymieniony przypadek jest jednym z zagrożeń wynikających z przeprowadzonej analizy ryzyka.

W ramach rozpatrywanego scenariusza przyjęto, że metan może być tłoczony z obu zbiorników. Tłoczenie odbywa się dmuchawą gazu pracującą z maksymalną wydajnością. Jeśli nastąpi pęknięcie rurociągu na łączeniu elementów ze zbiornikiem, dochodzi do uwolnienia chmury metanu. Wymagane jest, aby zamknąć niezwłocznie zawór za dmuchawą gazu i wyłączyć ją wraz z pozostałymi elementami instalacji, związanymi z zagrożoną częścią instalacji.

Realizacja funkcji bezpieczeństwa powinna spełniać wymagania poziomu nienaruszalności bezpieczeństwa SIL 2. Funkcja ta została zaimplementowana w systemie SIS. Wyznaczenie wymaganego poziomu SIL zostało przeprowadzone na podstawie zdefiniowanego grafu ryzyka.

Prawdopodobieństwo błędu człowieka Q (HEP) dla rozpatrywanego scenariusza awaryjnego zostało oszacowane przy wykorzystaniu dwóch metod analizy niezawodności człowieka: SPAR-H oraz HEART.

Analizę metodą HEART wykonano przy uwzględnieniu czynników zestawionych w tablicy 1, a obliczenia wykonano zgodnie z wzorem (1).

$$Q = Q_N \prod_{i=1}^{n} K_i \tag{1}$$

gdzie: Q – prawdopodobieństwo błędu człowieka,
K_i – wartości poszczególnych parametrów;

Tablica 1. Zestawienie parametrów do obliczeń metodą HEART

Czynnik - parametr	Całościowy wpływ HEART	Miara wpływu (0-1)	Uzyskane wartości K_i
Brak doświadczenia – K1	x3	0.4	(3,0 - 1) x 0,4 + 1 = 1,8
Brak procedur – K2	x6	1.0	(6,0 - 1) x 1,0 + 1 = 6,0
Słaba percepcja ryzyka – K3	x4	0,8	(4,0 - 1) x 0,8 + 1 = 3,4
Konflikt celów – K4	x2,5	0,8	(2,5 - 1) x 0,8 + 1 = 2,2
Niskie morale – K5	x1.2	0,6	(1,2 - 1) x 0,6 + 1 = 1,12

Powyższy wzór przedstawia wyliczenia dotyczące prawdopodobieństwa błędu człowieka Q metodą HEART, przy czym Q_N jest wartością nominalną, równą 0,003 dla przyjętej kategorii działania, zgodnie z metodą HEART. Na podstawie przeprowadzonych obliczeń uzyskano wynik $Q = 0{,}27$.

Podobne analizy zostały przeprowadzone przy wykorzystaniu metody SPAR-H przy założeniu, iż kolejne działania operatorów będą niezależne. Obliczenia dotyczące błędu diagnozowania i błędu działania zostały przeprowadzone zgodnie z równaniami (2) i (3)

$$Q_{di} = Q_{Ndi} \prod_{k=1}^{8} C_{wdi,k} \tag{2}$$

gdzie: Q_{di} – wartość prawdopodobieństwa błędu człowieka w procesie diagnozowania, Q_{Ndi} – nominalna wartość

prawdopodobieństwa błędu człowieka podczas diagnozowania (równa 0,01), $C_{wdi,k}$ – wartości przypisane czynnikom wpływu dotyczącym diagnozowania;

$$Q_{dz} = Q_{Ndz} \prod_{k=1}^{8} C_{wdz,k} \tag{3}$$

gdzie: Q_{dz} – wartość prawdopodobieństwa błędu człowieka w procesie działania naprawczego, Q_{Ndz} – nominalna wartość prawdopodobieństwa błędu człowieka podczas działania (równa 0,001), $C_{wdz,k}$ – wartości przypisane czynnikom wpływu dotyczącym działania;

Wartości przypisane czynnikom wpływu $C_{wdi,k}$ oraz $C_{wdz,k}$ zostały określone z uwzględnieniem opinii ekspertów zgodnie z odpowiednimi tablicami SPAR-H. Wyznaczone na podstawie wzorów (2) i (3) wartości prawdopodobieństw wyniosły odpowiednio $Q_{di} = 0{,}28$ oraz $Q_{dz} = 0{,}05$.

Wynikową wartość prawdopodobieństwa Q błędu człowieka w rozważanej sytuacji wyznacza się na podstawie następującego wzoru:

$$Q \cong Q_{di} + Q_{dz} \tag{4}$$

Wykorzystując zależność (4) uzyskano wynikowe prawdopodobieństwo błędu człowieka $Q = 0{,}33$. Wartość ta jest zbliżona do wartości tego prawdopodobieństwa uzyskanej metodą HEART ($Q = 0{,}27$).

Wartości te są relatywnie wysokie w odniesieniu do przedziału kryterialnego dla poziomu SIL1, co potwierdza konieczność zastosowania przyrządowego systemu bezpieczeństwa SIS na poziomie SIL2, aby osiągnąć wymagane zmniejszenie ryzyka.

3. PODSUMOWANIE

W niniejszym artykule przedstawiono w zarysie istotę analizy niezawodności człowieka. Zaprezentowano przykład obliczeniowy którego wyniki, w przeciwieństwie do przykładów z dokumentów normatywnych (gdzie przyjmuje się zwykle $Q = 0{,}1$), są znacząco wyższe. Otrzymane wartości Q dla rozważanego przykładu są zbliżone jednakże wymagana będzie w przyszłych pracach ocena niepewności uzyskanych wyników w odniesieniu do przyjętych założeń. W rozpatrywanym rozwiązaniu proponuje się, aby system SIS realizował funkcję bezpieczeństwa automatycznie ze względu na wysokie prawdopodobieństwo błędu człowieka. Dalsze prace będą zmierzały w kierunku opracowania zaawansowanego modelu dynamiki procesów awaryjnych w instalacji.

4. BIBLIOGRAFIA

1. IEC 61511 (2nd Ed.): Functional safety – Safety instrumented systems for the process industry sector. International Electrotechnical Commission. Geneva 2016.
2. PN-EN 61508 (Ed. 2): Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych syst. związanych z bezpieczeństwem, PKN, Warszawa 2010.
3. Carey M.:"Proposed framework for addressing human factors in IEC 61508. Amey VECTRA Limited for the Health and Safety Executive (HSE), Suffolk, 2001.
4. Kosmowski K.T. i inni: Opracowanie metod i narzędzi do wspomagania oceny wpływu czynników ludzkich na częstość zdarzeń inicjujących i ryzyko scenariuszy awaryjnych w celu zastosowania efektywnych rozwiązań technicznych. Sprawozdanie z I etapu projektu VI.B.10, CIOP-PIB. Gdańsk, 2011.
5. LOPA: Layer of Protection Analysis, Simplified Process Risk Assessment. American Institute of Chemical Engineers, Center for Chemical Process Safety. New York 2001.
6. EN ISO 9241-210: Ergonomics of human-system interaction, Human-centred design for interactive systems, 2010.
7. EEMUA Publication 191 (2nd Ed.): Alarm Systems - A Guide to Design, Management and Procurement. Engineering Equipment and Materials Users' Association. London 2007.
8. Kosmowski K.T.: Functional safety and reliability analysis methodology for hazardous industrial plants. Gdańsk University of Technology Publishers, Gdańsk 2013.
9. Bell J., Holroyd J.: Review of human reliability assessment methods", Health and Safety Laboratory for the Health and Safety Executive (HSE), Buxton, Derbyshire 2009.
10. SPAR-H: Human Reliability Analysis (HRA) Method, NUREG/CR-6883, INL/EXT-05-00509, USNRC, 2005
11. Kirwan B.: The validation of three human reliability quantification techniques, THERP, HEART and JHEDI, Applied Ergonomics, 1997 Feb; 28(1):17-25.

HUMAN-OPERATOR RELIABILITY ANALYSIS IN CONTEXT OF FUNCTIONAL SAFETY

The paper addresses some issues of the layer of protection analysis concerning an industrial hazardous plant taking into account results of the human reliability analysis (HRA). The functional safety analysis includes determining required safety integrity level (SIL) of safety functions proposed for hazards identified, based on the risk analysis results obtained and assessed regarding the risk criteria defined. The next step is to verify whether required SIL level is achieved using appropriate protection layers that include the safety instrumented system (SIS) of configuration considered in design to implement given safety function, using appropriate methods of probabilistic modelling. Human-operator activities in context of the human-system interface - including the alarm system - and potential human errors, may have significant impact on the probabilistic results obtained. This impact is evaluated using appropriate HRA method or methods. In the paper the influence of human factors relevant to two HRA methods selected, i.e. HEART and SPAR-H, are evaluated. The results of the human error probability (HEP) obtained using these methods are discussed for an accident scenario considered.

Keywords: human factors, functional safety, layer of protection analysis, alarm system, human reliability analysis.