Politechnika Gdańska

Wydział Elektrotechniki i Automatyki

Gdańsk 2015

ANALIZA NIEZAWODNOŚCI CZŁOWIEKA Z UWZGLĘDNIENIEM ASPEKTÓW ZARZĄDZANIA ALARMAMI

Emilian PIESIK[1], Marcin ŚLIWIŃSKI[2]

1. Politechnika Gdańska, Wydział Elektrotechniki i Automatyki
   tel: 58 347 14 35 e-mail: emilian.piesik@pg.gda.pl
2. Politechnika Gdańska, Wydział Elektrotechniki i Automatyki
   tel: 58 347 14 35 e-mail: marcin.sliwinski@pg.gda.pl

Streszczenie: W artykule przedstawiono zagadnienie analizy warstwowego systemu zabezpieczeń z uwzględnieniem błędu człowieka-operatora. W analizie bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń istotną kwestią jest dokonanie redukcji ryzyka poprzez warstwy zabezpieczeniowo ochronne. W referacie przeanalizowano system składający się z trzech warstw: podstawowego systemu sterowania BPCS, systemu alarmowego AS oraz systemu automatyki zabezpieczeniowej SIS. W warstwowym systemie zabezpieczeniowym ważną funkcję spełnia system alarmowy, poprzez który człowiek-operator ma istotny wpływ na realizację funkcji bezpieczeństwa. Funkcje te są realizowane poprzez odpowiednie moduły w ramach systemu BPCS, lub SCADA.

Słowa kluczowe: HEP, człowiek-operator, bezpieczeństwo funkcjonalne, system alarmowy.

1. INFORMACJE OGÓLNE

1.1. Wprowadzenie

Bezpieczeństwo funkcjonalne systemów elektrycznych/ elektronicznych i programowalnych elektronicznych E/E/EP może zależeć od czynników ludzkich, które należy rozpoznać i kształtować już na etapie projektowania tak, aby ograniczać wpływ błędów człowieka na ryzyko związane z eksploatacja systemów technicznych. Instalacja podwyższonego ryzyka powinna zostać poddana gruntownej analizie, mającej na celu określenie poziomu nienaruszalności bezpieczeństwa SIL (ang. *safety integrity level*) oraz późniejszą jego weryfikację. W odniesieniu do wyznaczonych miar ryzyka istotne znaczenie mają systemy sterowania i zabezpieczeń. Jeśli poziom ryzyka jest zbyt wysoki, ryzyko to musi zostać zredukowane do poziomu akceptowanego. Określenie wymagań dotyczących niezbędnej redukcji ryzyka (na podstawie analizy ryzyka) z jednej strony i wymagań dotyczących funkcji bezpieczeństwa (redukujących ryzyko) z drugiej, umożliwia dobranie właściwego poziomu SIL systemu E/E/PE (odpowiednia architektura i zasady eksploatacji) dla rozważanych zagrożeń.

System alarmowy przekazuje operatorowi sygnały dźwiękowe i wizualne o zaistniałych zagrożeniach i sytuacjach awaryjnych. Sygnał alarmu wskazuje na zaistnienie problemu wymagającego uwagi operatora [1]. System alarmowy wspomaga operatora w utrzymywaniu instalacji technologicznej w stanie bezpiecznym, operator powinien interweniować w celu skorygowania sytuacji potencjalnie niebezpiecznych przed zadziałaniem systemu awaryjnego wyłączenia ESD (ang. *emergency shutdown system*) lub systemu automatyki zabezpieczeniowej SIS (ang. *safety instrumented system*).

1.2. Metody analizy niezawodności człowieka

Niezawodność człowieka-operatora oszacować można ilościowo przy użyciu jednej z metod HRA (ang. *human reliability analysis*). W literaturze zidentyfikowano ponad 70 metod oceny niezawodności człowieka [1, 2]. Szczególnie przydatną w zastosowaniach praktycznych a zwłaszcza w analizach bezpieczeństwa funkcjonalnego metodą jest SPAR-H (ang. *standardized plant analysis risk - human reliability analysis method*). Metody HRA dają możliwość oszacowania prawdopodobieństw potencjalnych błędów człowieka HEP (ang. *human error probability*) w instalacji procesowej. Ponadto przy użyciu metod HRA można ocenić wpływ potencjalnych błędów człowieka na ryzyko wystąpienia rozpatrywanego scenariusza awaryjnego ze szczególnym uwzględnieniem systemu alarmowego. Metody HRA bazują na opiniach ekspertów oraz danych reprezentowanych w postaci informacji jakościowej i/lub ilościowej. Metoda analizy niezawodności człowieka SPAR -H ma zastosowanie w przypadku obiektów przemysłowych o niedużym stopniu skomplikowania [3].

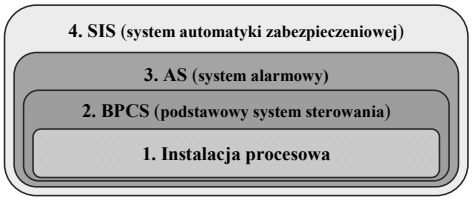
2. SYSTEM ALARMOWY

2.1. Metodyka zarządzania alarmami

Obiekty przemysłowe podwyższonego ryzyka są obecnie projektowane zgodnie z zasadą obrony w głąb z wyróżnieniem kilku warstw zabezpieczeniowo-ochronnych. Projektowanie tych warstw i systemów związanych z bezpieczeństwem bazuje na identyfikacji zagrożeń np. metodą HAZOP (ang. *hazard and operabilit study*) oraz analizie i ocenie ryzyka. Integralność systemów w rozumieniu bezpieczeństwa jest weryfikowana za pomocą metod formalnych na zgodność z wymaganiami i kryteriami, na przykład zawartymi w IEC 61511 [3, 4, 5, 6, 7, 8].

Na rysunku 1 przedstawiono typowe warstwy zabezpieczeniowo-ochronne związane z programowalnymi systemami sterowania, monitorowania i zabezpieczeń

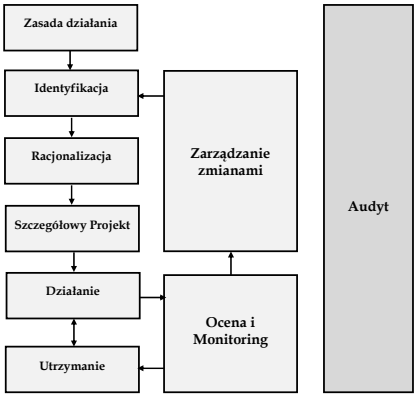
obiektu przemysłowego podwyższonego ryzyka jakim jest instalacja procesowa.



Rys. 1. Warstwy zabezpieczeniowo ochronne wg (IEC 61511) [3, 7, 8]

W warstwowym systemie zabezpieczeniowym ważną funkcję spełnia system alarmowy. Kompletny system alarmowy obejmuje sprzęt i oprogramowanie do odpowiedniego generowania informacji, sygnalizowania i wspomagania decyzji w różnych sytuacjach dynamicznych procesu i obiektu, szczególnie w sytuacjach nienormalnych i awaryjnych. Funkcje te są realizowane przez odpowiednie moduły w ramach systemu BPCS (ang. *basic process control system*) lub SCADA (ang. *supervisory control and data acquisition*).

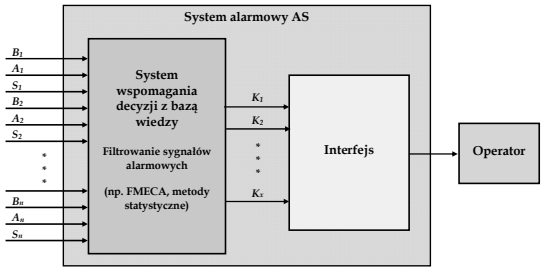
System alarmowy może być projektowany jako odseparowany system niezależny (rys. 1). Na rysunku 2 przedstawiono cykl życia zarządzania alarmami według standardu ISA-18.2 [9, 10].



Rys. 2. Zarządzanie systemem alarmowym w cyklu życia wg (ISA-18.2) [9, 10]

Podstawowym zadaniem w projektowaniu systemu alarmowego jest rozpatrzenie zakresu jego funkcjonalności w nawiązaniu do spodziewanych trudności diagnostycznych sytuacji dynamicznych oraz jego rozwiązania sprzętowego, strukturalnego i oprogramowania. Jednym z ważnych aspektów na etapie projektowania jest odporność systemu alarmowego na tzw. występowanie fałszywych alarmów. Analiza rozwiązań systemów alarmowych w przemyśle wykazała, że są one często niewłaściwie projektowane i użytkowane. Spowodowało to wzrost zainteresowania tym problemem instytucji zrzeszających firmy projektujące i wdrażające w przemyśle nowoczesne rozwiązania systemów sterowania, alarmowych i zabezpieczeń [11, 12, 13]. Podkreśla się w literaturze, że w niektórych instalacjach przemysłowych liczba alarmów przekracza 1400 na dobę, czyli średnio 2 alarmy na minutę, a powinno występować - ze względu na możliwości odbioru i analizy informacji przez operatorów - nie więcej 150 alarmów na dobę, czyli przeciętnie nie więcej niż 1 alarm na 10 min. Wskazuje to skalę wyzwań jakie stoją przed projektantami systemów alarmowych [7, 9, 10].

Zasadniczym problemem w zarządzaniu alarmami jest nadmiar informacji docierających do operatora [5, 7, 9, 13]. W danym przypadku niezbędny jest system pełniący funkcję filtrowania alarmów. Koncepcja takiego rozwiązania wyposażonego w system z bazą wiedzy została przedstawiona na rysunku 3.



Rys. 3. System wspomagania decyzji z bazą wiedzy do filtrowania sygnałów alarmowych

W danym przypadku system alarmowy posiada własne systemy pomiarowe i w sposób niezależny (zgodnie z filozofią przedstawioną na rys. 1) docierają z nich sygnały od A1 do An. Oprócz tego system alarmowy współpracuje z systemami BPCS i SIS. Z systemu BPCS do systemu alarmowego dochodzą sygnały od B1 do Bn (rys. 3), natomiast z systemu SIS sygnały od S1 do S2 (rys. 3). Sygnały od 1 do n pochodzą w danym przypadku od trzech niezależnych systemów: BPCS, podsystemu pomiarowego systemu alarmowego AS oraz systemu SIS. Nieprzetworzona liczba tych sygnałów jest zbyt wielka, żeby trafić bezpośrednio do interfejsu operatorskiego. Zatem przed przesłaniem tych sygnałów do systemu interfejsu operatora, potrzebny jest specjalny system filtrujący. Najlepszym rozwiązaniem jest zastosowanie systemu z bazą wiedzy lub systemu ekspertowego, który odfiltrowywałby sygnały alarmowe z rozmiaru n do rozmiaru x (gdzie $x < n$). Wówczas po odfiltrowaniu do interfejsu operatora w odpowiednich ramach czasowych trafiałyby sygnały alarmowe w skali od K1 do Kx.

Do procesu filtracji sygnałów można wykorzystać metody statystyczne dotyczące występowania fałszywych alarmów dla danej instalacji/procesu. Można także, w trakcie budowy bazy wiedzy wykorzystać analizę rodzajów, skutków i krytyczności uszkodzeń FMECA (ang. *failure mode, effect and criticality analysis*), pozwalającą zidentyfikować i sklasyfikować od najbardziej do najmniej krytycznego, niekorzystne skutki końcowe sprzężone z sygnałami alarmowymi dla danego procesu/instalacji.

Jeżeli w rozpatrywanym systemie alarmowym funkcjonującym w ramach struktury warstw zabezpieczeń przedstawionych na rys. 1, do operatora poprzez system alarmowy docierają informacje o stanie procesu w sposób niezależny z trzech warstw, wówczas tę sytuację można wykorzystać w podejmowaniu decyzji dotyczących eliminacji tzw. fałszywych alarmów. Śledząc jednocześnie trzy trendy (z systemów BPCS, AS i SIS), uzyskuje się tzw. "redundancję" sygnałów docierających do operatora. W oparciu o rejestrowane zmiany można wyeliminować fałszywe alarmy jak i również zredukować liczbę sygnałów alarmowych docierających do operatora. W filtracji alarmów istotną kwestią będzie dynamika procesu oraz czas reakcji operatora na wystąpienie danego sygnału alarmowego

w zależności od stopnia jego krytyczności (zdefiniowanego np. na podstawie FMECA).

W poradniku [13] wyróżnia się kilkanaście rodzajów alarmów, które wymagają odpowiedniego potraktowania. Wymaga się na przykład, aby operator był wspomagany w działaniach polegających na selekcji odpowiednich ekranów graficznych i właściwym reagowaniu na jeden lub więcej alarmów jeśli sytuacja tego wymaga, przy czym intensywność pojawiania się alarmów powinna być zdecydowanie ograniczona. W procesie projektowania systemu alarmowego należy uwzględnić zagadnienia związane z ochroną informacji (ang. *security*) w szczególności w infrastrukturze sieciowej, w której funkcjonuje stacja SCADA [3, 7, 8, 14].

2.2. Niezawodność operatora

System alarmowy nieodpowiednio zaprojektowany może spowodować dezorientację operatora, przyczyniając się do popełnienia błędu z większym prawdopodobieństwem HEP. W publikacji EEMUA [13] podkreślona jest istota funkcji interfejsu człowiek-komputer HCI (ang. *human computer interface*), za podstawową funkcję uważa się dostarczenie operatorowi zwartego (spójnego z procesem) i łatwego w użytkowaniu interfejsu, który zapewni odpowiednią funkcjonalność monitorowania i sterowania we wszystkich możliwych do przewidzenia warunkach procesu technologicznego.

Tablica 1. Wymagania niezawodności systemu alarmowego i człowieka – operatora [13]

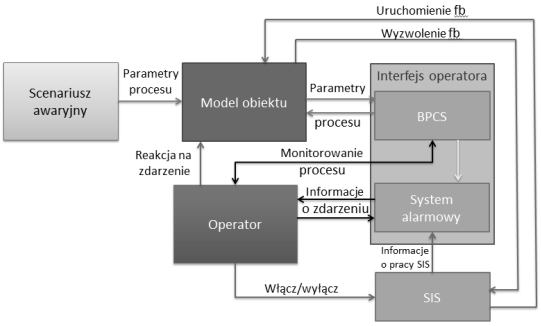
Wymagane PFD_{avg}	Rodzaj systemu alarmowego i wymagania niezawodnościowe	Wymagania związane z rolą i niezawodnością człowieka - OPERATORA
Na poziomie 10^{-1}	System alarmowy bez wymagań - może być zintegrowany z BPCS	Nie ma specjalnych wymagań – systemu alarmowego.
$[10^{-2}, 10^{-1}]$	System alarmowy traktowany, jako system związany z systemem automatyki zabezpieczeniowej SIS - projektowany na poziomie SIL1	Operator powinien być szkolony w zarządzaniu sytuacjami awaryjnymi zgodnie z projektem system alarmowy; dostęp do procedur, dostęp informacji; audyt działań operatora.
$< 10^{-2}$	System alarmowy traktowany, jako system związany z systemem SIS - projektowany na poziomie, od poziomu SIL2	Wymagania na prawdopodobieństwo błędu w reakcji operatora ($PFD_{i;PL2} = HEP_{i;PL2}$) nie powinny być poniżej wartości 0.01.

W celu optymalizowania interfejsu należy przeprowadzić analizę zadań operatora, co umożliwi ocenę pełnego zakresu obowiązków operatora w danej sytuacji. W tablicy 1 zawarto przykładowe wymagania dotyczące kształtowania poziomów probabilistycznych (PFD lub HEP), odpowiednio systemu alarmowego i człowieka - operatora. Z tablicy 1 wynikają podstawowe założenia do projektowania systemu alarmowego, w przypadku obiektów wysokiego ryzyka system alarmowy powinien być odseparowany od BPCS i projektowany, jako system związany z systemem bezpieczeństwa. Zasady projektowania systemów zgodnie z wymaganiami bezpieczeństwa funkcjonalnego podano w normach [3, 15], które rozszerzono w pracy [16] o zagadnienia analizy niezawodności człowieka HRA. Należy zwrócić uwagę na fakt, iż odpowiednio zaprojektowany system alarmowy, przyczyni się do zmniejszenia prawdopodobieństwa błędów człowieka-operatora. Umożliwi to ograniczenie ryzyka do poziomu wyznaczonego w procesie zarządzania bezpieczeństwem.

3. PROPOZYCJA PODEJŚCIA

3.1. Operator w warstwowym systemie zabezpieczeń

Nowa edycja normy IEC 61511 [3] zawiera wskazania na dokumenty dotyczące analizy niezawodności człowieka, jednakże w ich treści nie znajduje się jednoznaczna odpowiedź, co do wyboru metody czy też proponowanego podejścia w rozważaniach związanych z analizą niezawodności człowieka.

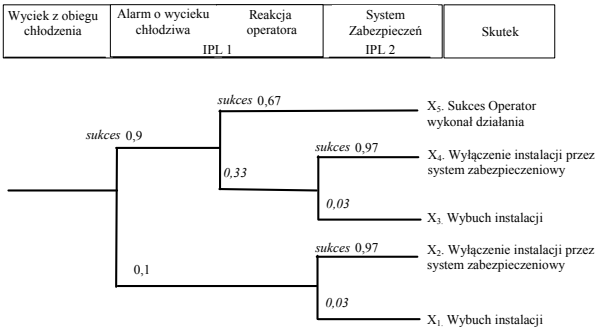


Rys. 4. Schemat roli operatora w warstwowym systemie zabezpieczeń: fb – funkcja bezpieczeństwa

Operator w warstwowym systemie zabezpieczeń wpływa na proces poprzez warstwę BPCS a także reaguje na informacje z systemu alarmowego AS. Relacje pomiędzy człowiekiem-operatorem a instalacją procesową zostały przedstawione na rysunku 4.

3.2. Przykład

Analizie poddano fragment instalacji biogazowni której model przedstawiono szczegółowo w pracy [17]. W skład systemu wchodził odsiarczalnik biogazu. W skutek rozszczelnienia instalacji chłodzenia może dojść do zapłonu metanu. W ramach rozpatrywanego scenariusza awaryjnego przyjmuje się, że instalacja odsiarczania pracuje z 100% wydajnością. Następuje pęknięcie rurociągu obiegu chłodzenia, w skutek czego dochodzi do utraty chłodziwa w następstwie, czego powstaje atmosfera wybuchowa. W przypadku powodzenia działań operatora zostanie usunięte zagrożenie poprzez uruchomienie flary.



Rys. 5. Drzewo zdarzeń z wyróżnieniem błędów operatora dla rozpatrywanej sytuacji

Analiza ryzyka wykazała, iż rozpatrywane zagrożenie stwarza ryzyko na poziomie nieakceptowalnym, ryzyko to musi zostać zredukowane do poziomu tolerowanego. Na podstawie analizy ryzyka określono wymagania SIL1 dla funkcji bezpieczeństwa. Liczba interwencji człowieka – operatora dla tego obiektu powiązana jest z drzewem zdarzeń ET (ang. *event tree*) przedstawionym na rysunku 5. Drzewo zdarzeń prezentuje także niepowodzenie w przypadku: błędnej oceny sytuacji, odizolowania obiegu, redukcji mocy, zamknięcia zaworu odcinającego dopływ biogazu, fałszywych alarmów itp. Operator po otrzymaniu alarmu w formie dźwiękowej oraz pojawieniu się informacji graficznej w oknie systemu alarmowego, powinien rozpocząć wykonywanie działań. Prawdopodobieństwo błędu człowieka wyliczone na podstawie metody SPAR-H dla tego rodzaju scenariusza awaryjnego przy założeniu, że kolejne działania operatora będą oddziaływały na system w sposób niezależny wynosi HEP = 0,33. Czas na podjęcie działań przez operatora T_{max}=10 min, od otrzymania informacji z systemu alarmowego. W przypadku niepowodzenia, po tym czasie powinno nastąpić uruchomienie funkcji bezpieczeństwa wykonywanej przez system automatyki zabezpieczeniowej SIS. System alarmowy zgodnie z wytycznymi zawartymi w tablicy 1 zrealizowany jest wraz z systemem BPCS co nie zapewnia wymaganego poziomu nienaruszalności bezpieczeństwa SIL1.

4. PODSUMOWANIE

W niniejszym artykule przedstawiono podejście metodyczne zarządzania alarmami z uwzględnieniem analizy niezawodności człowieka na przykładzie fragmentu instalacji biogazowni, w nawiązaniu do wymagań norm PN-EN 61508 i PN-EN 61511. Problem analizy niezawodności człowieka z punktu widzenia warstw zabezpieczeń w obiekcie infrastruktury krytycznej jest aktualny i wymaga dalszych prac badawczych, w których uwzględnione zostaną aspekty zarządzania informacjami z systemu alarmowego. Dane te muszą być doprowadzone do operatora w odpowiedniej konfiguracji uzależnionej od ich wagi.

5. BIBLIOGRAFIA

1. Bell J., Holroyd J.: Review of human reliability assessment methods, Health and Safety Laboratory for the Health and Safety Executive (HSE), Buxton, Derbyshire 2009.
2. Carey M.: Proposed framework for addressing human factors in IEC 61508, Amey VECTRA Limited for the Health and Safety Executive (HSE), HSE Books, Sudbury, Suffolk 2001.
3. IEC 61511:2015 Ed.2: Functional safety – Safety instrumented systems for the process industry sector.
4. Missala T. Księga procedur do oceny zgodności bezpieczeństwa funkcjonalnego w przemyśle procesowym, Studium, PIAP, Warszawa 2010.
5. Smith D., Simpson K.: Functional Safety 2nd Edition, A straightforward guide to applying IEC 61508 and related standards, Elsevier, Oxford 2004.
6. Process Safebook1: Functional safety in the process industry, Principles, standards and implementation, Rockwell Automation, 2013.
7. Projekt VI.B.10: Opracowanie metod i narzędzi do wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym i ochroną informacji, WEiA PG, Gdańsk 2013.
8. EMERSON Process Management: Safety Lifecycle Workbook, For The Process Industry Sector, Emerson, 2010.
9. ISA 18.02-2009, Management of Alarm Systems for the Process Industries.
10. EMERSON Process Management: Alarm Management. DeltaV Whitepaper, Emerson, 2010.
11. Carlin A.S., Schurr N., Marecki J.: ALARMS: Alerting and Reasoning Management System for Next Generation Aircraft Hazards, NASA No. NNL08AA20B, 2009.
12. EEMUA Publication 191: Alarm Systems; A Guide to Design, Management and Procurement(Edition 2), The Engineering Equipment and Materials Users' Association, London 2007.
13. EEMUA Publication 201: Process Plant Control Desks Utilising Human-Computer Interfaces. London: The Engineering Equipment and Materials Users' Association, 2002.
14. IEC 62443:2008, Network and system security for industrial-process measurement and control, Parts 1-5.
15. PN-EN 61508:2010, Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1-7, Polski Komitet Normalizacyjny.
16. Kosmowski K.T.: Functional safety analysis including human factors. Proceedings of the Third Summer Safety & Reliability Seminars 2009. ESRA-PSRA, Gdańsk-Sopot, 19-25 July 2009. Vol. 2, pp. 251-263, 2009.
17. Barnert T., Piesik E., Śliwiński M.: Real-time simulator of agricultural biogas plant, Computers and Electronics in Agriculture, Elsavier, 2014.

HUMAN RELIABILITY ANALYSIS WITH THE ALARM MANAGEMENT ASPECTS

The paper presents the problem of layer of protection analysis with safety systems, taking into account human error probability. In the functional safety analysis control and protection systems, the important issue is to reduce risk by independent protection layer. The paper assessment system consisting of three independent protection layers: BPCS control system, alarm system AS and a safety instrumented system SIS. In the systems with protection layers an important function via the alarm system have human-operator who has a significant impact on the implementation of safety functions. The complete alarm systems consist of hardware and software for generating appropriate information, signaling and decision support in different situations dynamic process, especially in abnormal and emergency situations. These functions are carried out by the appropriate modules within the system BPCS, or SCADA. These paper presents the problem of determining the probability of human error probability HEP using the simplified plant analysis risk human reliability assessment method SPAR-H. The probability of human error is the issue related to the stage of verification of certain levels SIL.

Keywords: HEP, human-operator, functional safety, alarm system.