Wojas Marta
Urząd Dozoru Technicznego, Centrum Certyfikacji i Oceny Zgodności (UDT-CERT), Warszawa, Polska

Kosmowski Kazimierz T.
Politechnika Gdańska, Gdańsk, Polska

Kościelny Jan M.
Politechnika Warszawska, Warszawa, Polska

Certification system of persons responsible for functional safety
System certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne

Keywords / Słowa kluczowe

certification of persons, functional safety, training programmes, certification process, conformity assessment
certyfikacja osób, bezpieczeństwo funkcjonalne, programy szkoleniowe, proces certyfikacji, ocena zgodności

Abstract

This article describes a certification system of persons responsible for functional safety developed by the Office of Technical Inspection (UDT-CERT) in Poland in cooperation with members of the Programme Committee No. 8 and representatives of two technical universities: in Gdansk and Warsaw. The system is consistent with standard ISO/IEC 17024 concerning the conformity assessment, and includes requirements of EN 61508 and some sector standards. The certification and training programs include two levels of qualification: I – general and II – expert, and four specializations in functional safety: A – hardware and software, B – process industry, C – machinery, and D – nuclear power plants.

1. Wprowadzenie

Koncepcja bezpieczeństwa funkcjonalnego zawarta w normie PN-EN 61508 [10] jest przykładem dobrej praktyki inżynierskiej projektowania i eksploatacji systemów elektrycznych/ elektronicznych/ programowalnych elektronicznych (E/E/PE) związanych z bezpieczeństwem. Systemy takie są obecnie coraz szerzej stosowane w różnych sektorach przemysłu i gospodarki. Dotyczy to również przemysłu procesowego dla którego opracowano normę sektorową PN-EN 61511 [11], przemysłu maszynowego w nawiązaniu do normy PN-EN 62061 [12] i innych sektorów.
Stosowane rozwiązania systemów sterowania i zabezpieczeń są już obecnie i będą coraz szerzej oceniane pod kątem wymagań bezpieczeństwa funkcjonalnego przez organy dozoru technicznego i firmy ubezpieczeniowe. Wymagania zawarte w tych normach są coraz częściej uwzględniane również w specyfikacji technicznej i zamówieniach wyposażenia obiektów i instalacji.
W związku z tym istotne znaczenie ma odpowiednie przygotowanie osób odpowiedzialnych za bezpieczeństwo funkcjonalne. Problem ten podnoszono już w roku 2004 podczas krajowej konferencji naukowo technicznej w Juracie nt. *Zarządzania bezpieczeństwem funkcjonalnym*, a wstępne propozycje szkoleniowe i certyfikacyjne osób zawarto w pracy [1]. Propozycje te następnie rozwinięto w monografii [7].
Niniejszy artykuł poświęcono krajowemu systemowi i programowi certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne [14]. Program ten został wypracowany przez UDT-CERT we współpracy z członkami Komitetu Programowego nr 8, powołanego przez ten UDT, przy pomocy merytorycznej przedstawicieli Politechniki Gdańskiej i Politechniki Warszawskiej.

2. Rola UDT-CERT w krajowym systemie certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne

Wszelkie działania Urzędu Dozoru Technicznego (UDT), wynikające z ustawy o dozorze technicznym [9], mają na celu wspierać państwo, społeczeństwo i podmioty gospodarcze w działaniach służących bezpieczeństwu użytkowania urządzeń technicznych i ochronie środowiska oraz zmierzają do zapewnienia bezpiecznego funkcjonowania urządzeń technicznych. Dotyczy to urządzeń, które mogą stwarzać zagrożenie dla życia lub zdrowia ludzkiego oraz mienia i środowiska, a w szczególności takie, w których może nastąpić:

- rozprężenie cieczy lub gazów znajdujących się pod ciśnieniem różnym od atmosferycznego,
- wyzwolenie energii potencjalnej lub kinetycznej przy przemieszczaniu ludzi i ładunków w ograniczonym zasięgu,
- rozprzestrzenianie się materiałów niebezpiecznych o właściwościach trujących lub żrących oraz ciekłych zapalnych w czasie ich magazynowania.

Urząd Dozoru Technicznego spełnia swoją misję realizując działania jako:

- jednostka inspekcyjna,
- jednostka certyfikująca systemy zarządzania ,
- jednostka certyfikująca wyroby,
- jednostka certyfikująca osoby,
- laboratorium badań oraz wzorcowań.

Kompetencje UDT w tym zakresie zostały potwierdzone certyfikatami akredytacji wydanymi przez Polskie Centrum Akredytacji. Ponadto UDT jest jednostką notyfikowaną nr 1433 do 12 dyrektyw europejskich „nowego podejścia".

Urządzenia techniczne podlegają dozorowi technicznemu podczas wytwarzania i eksploatacji. Jeśli jednak w zakresie wytwarzania obowiązują inne przepisy niż ustawa o dozorze technicznym, np. *dyrektywy nowego podejścia*, wytwarzane urządzenia muszą spełniać takie wymagania. Jednakże urządzenia eksploatowane w kraju, objęte dozorem technicznym, podlegają obowiązkowym rewizjom zewnętrznym i/lub wewnętrznym prowadzonym przez inspektorów UDT. W urządzeniach technicznych stosowane są odpowiednie systemy zabezpieczeń przed niekontrolowanym rozprężeniem się gazów lub cieczy i ich rozprzestrzenianiem się, czy też wyzwoleniem się energii zagrażającym bezpieczeństwu.

Systemy takie muszą zagwarantować odpowiedni poziom redukcji ryzyka. Jeśli są sterowane elektrycznie / elektronicznie, to spełnienie wymagania dotyczy wszystkich działań w cyklu życia bezpieczeństwa systemów zawierających *elektryczne, elektroniczne lub programowalne elektronicznie* (E/E/PE) elementy składowe.

Systemy zabezpieczeń, jako integralne składowe urządzeń technicznych, bez względu na stan techniki, muszą być, podobnie jak urządzenia, których dotyczą, projektowane, wytwarzane i eksploatowane oraz naprawiane lub modernizowane tylko przez kompetentne osoby, to znaczy personel spełniający określone wymagania w zakresie wiedzy, doświadczenia i kwalifikacji. Wymagania takie określają np. normy zharmonizowane z dyrektywami *nowego podejścia*, których stosowanie stanowi domniemanie spełnienia wymagań zasadniczych takich dyrektyw.

Normy zharmonizowane powołują niekiedy wprost wśród normatywnych dokumentów referencyjnych normę EN 61508-1 [2], np. w normie PN-EN 15233:2009 zharmonizowanej z dyrektywą Atex nr 94/9/WE. Norma EN 61508-1 określa wymagania zmierzające do zapewnienia, że osoby odpowiedzialne za wszelkie czynności związane z cyklem życia systemów E/E/PE lub oprogramowania, w tym czynności zarządzania, były odpowiednio wyszkolone, miały wiedzę techniczną, doświadczenia i kwalifikacje do pełnienia konkretnych obowiązków.

Tak sformułowane wymaganie jest zbieżne z definicją kompetencji określoną w normie PN-EN ISO/IEC 17024 (2004) [13] jako *wykazana zdolność do stosowania wiedzy i/lub umiejętności oraz, jeśli to istotne, wykazanych cech osobowych jak to określono w programie certyfikacji.*

UDT z jednej strony jako organ dozoru technicznego, a z drugiej strony posiadający potwierdzone certyfikatem akredytacji PCA kompetencje jako jednostka certyfikująca osoby UDT-CERT, spełniająca wymagania PN-EN ISO/IEC 17024, zaproponowała system potwierdzania kompetencji osób odpowiedzialnych za bezpieczeństwo funkcjonalne spełniający wymagania standardów światowych.

Kompetencje osób odpowiedzialnych za bezpieczeństwo funkcjonalne we wszystkich istotnych branżach przemysłu, np. petrochemicznym, chemicznym czy energetycznym, uznane zostały przez UDT jako podstawowe w zapewnieniu odpowiedniego poziomu bezpieczeństwa wszelkich działań i zastosowanych rozwiązań technicznych w cyklu życia obwodów zabezpieczających, gwarantujących bezpieczną eksploatację wszelkich urządzeń i instalacji, mogących stwarzać zagrożenie dla życia lub zdrowia ludzkiego, mienia lub środowiska.

3. System certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne UDT-CERT

3.1. Założenia systemu certyfikacji

W UDT, przy współpracy krajowych specjalistów i ekspertów w tej dziedzinie i poparciu przedstawicieli firm istotnie zainteresowanych tym obszarem zapewnienia bezpieczeństwa, został opracowany i wdrożony system certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne UDT-CERT w ramach działalności Jednostki Certyfikującej Osoby. Celem takiego działania jest aktywne wspieranie rozwoju i upowszechnianie odpowiedzialności za utrzymywanie odpowiedniego poziomu bezpieczeństwa technicznego.
Wymagania dla osób ubiegających się o certyfikację oraz zasady prowadzenia procesu certyfikacji określa program certyfikacji [14] dostępny na stronie www.udt.gov.pl i na każde życzenie zainteresowanego. W opracowaniu programu certyfikacji aktywną rolę pełni powołany przez UDT Komitet Programowy nr 8, w skład którego zostali powołani przedstawiciele UDT-CERT, krajowego przemysłu i uczelni technicznych: Politechniki Gdańskiej i Politechniki Warszawskiej.
Program przewiduje dwa stopnie certyfikacji (I – ogólny i II – ekspercki) oraz cztery specjalności dla każdego stopnia: A – sprzęt i oprogramowanie (*Safety Hardware Development)*, B – przemysł procesowy (*Process Safety Applications)*, C – maszyny (*Machinery Applications)*, D - elektrownie jądrowe, określone wg wymagań odpowiednich norm, jak podano w *Tabeli 1*.
System UDT-CERT odpowiada certyfikacji międzynarodowej i tak: I stopień (CSBF) - ogólny w systemie UDT-CERT odpowiada CFSP (*Certified Functional Safety Professional*), czyli certyfikowanemu specjaliście bezpieczeństwa funkcjonalnego w systemie międzynarodowym. Stopień II (CEBF) - ekspercki odpowiada międzynarodowemu CFSE (*Certified Functional Safety Expert*), czyli certyfikowanemu ekspertowi bezpieczeństwa funkcjonalnego.

Tabela 1. Zakres certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne

Stopień	Specjalność	Norma
I – ogólny: certyfikowany specjalista bezpieczeństwa funkcjonalnego (CSBF)		PN-EN 61508 PN-EN 61511 PN-EN 62061 IEC 61513
II – ekspercki: certyfikowany ekspert bezpieczeństwa funkcjonalnego (CEBF)	A – sprzęt i oprogramowanie	PN-EN 61508
	B – przemysł procesowy	PN-EN 61511
	C – maszyny*	*PN-EN 62061*
	D - elektrownie jądrowe*	*IEC 61513*

*specjalność będzie uruchomiona w późniejszym terminie.

Certyfikacja I stopnia (ogólna) jest przeznaczona dla tych osób z kadry kierowniczej oraz technicznej, zajmującej się projektowaniem i eksploatacją systemów i urządzeń, których stanowiska nie wymagają dogłębnej wiedzy i praktyki w zakresie bezpieczeństwa funkcjonalnego, ale są odpowiedzialne w firmie za nadzór nad rozwiązaniami organizacyjnymi i technicznymi bezpieczeństwa funkcjonalnego.
Certyfikacja II stopnia (ekspercka) jest przeznaczona dla osób z kadry inżynieryjnej firmy bezpośrednio realizującej prace związane z działaniami na rzecz bezpieczeństwa funkcjonalnego w poszczególnych etapach cyklu życia bezpieczeństwa systemów sterowania i/lub zabezpieczających, z uwzględnieniem określenia poziomów nienaruszalności bezpieczeństwa SIL funkcji związanych z bezpieczeństwem oraz ich weryfikacji.
Propozycja krajowa ma niewątpliwą zaletę, ponieważ certyfikacja na poziomie ogólnym dotyczy nadzorującej kadry menedżerskiej i technicznej, która napotyka w praktyce przemysłowej na problemy decyzyjne dotyczące nie tylko zagadnień ogólnych związanych z bezpieczeństwem funkcjonalnym w nawiązaniu do PN-EN 61508, ale również sektorowych zagadnień i rozwiązań bezpieczeństwa funkcjonalnego, co wymaga wiedzy przekrojowej zawartej m.in. w normach PN-EN 61511 i PN-EN 62061, przewidzianych w Programie Certyfikacji UDT-CERT. Ponadto zakres wiedzy uzyskiwanej i potwierdzonej w krajowym systemie, w obydwu proponowanych stopniach, jest szerszy niż w przypadku odpowiednich stopni w systemie międzynarodowym. Dotyczy to zwłaszcza wiedzy z zakresu zagadnień diagnostyki procesów i systemów technicznych.

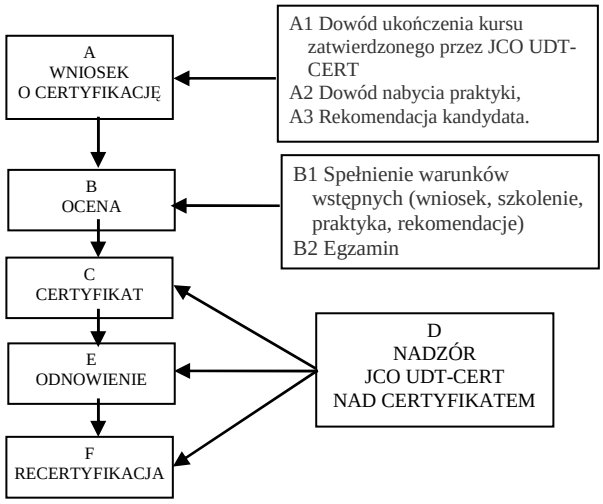
3.2. Uzyskanie i utrzymanie certyfikatu w systemie UDT-CERT

Kandydat w procesie certyfikacji składa wniosek o certyfikację, w którym zawarte są zapisy dotyczące spełnienia wstępnych wymagań certyfikacyjnych, a w szczególności wykształcenia, szkolenia i praktyki, potwierdzone przez pracodawcę, do którego:
a) *kandydat na I stopień* załącza m.in.:

– kopię świadectwa / dyplomu potwierdzającego wykształcenie,
– dwa oświadczenia specjalistów z dziedziny bezpieczeństwa funkcjonalnego rekomendujące kandydata,
– kopię świadectwa ukończenia z pozytywnym wynikiem kursu szkoleniowego zatwierdzonego przez JCO UDT-CERT;

b) *kandydat na II stopień* załącza m.in.:
– kopię świadectwa / dyplomu potwierdzającego wykształcenie,
– trzy oświadczenia specjalistów z dziedziny bezpieczeństwa funkcjonalnego rekomendujące kandydata,
– kopie świadectw ukończenia z pozytywnym wynikiem kursu szkoleniowego zatwierdzonego przez JCO UDT-CERT,
– studium przypadku.

Rysunek 1 przedstawia algorytm procesu certyfikacji.

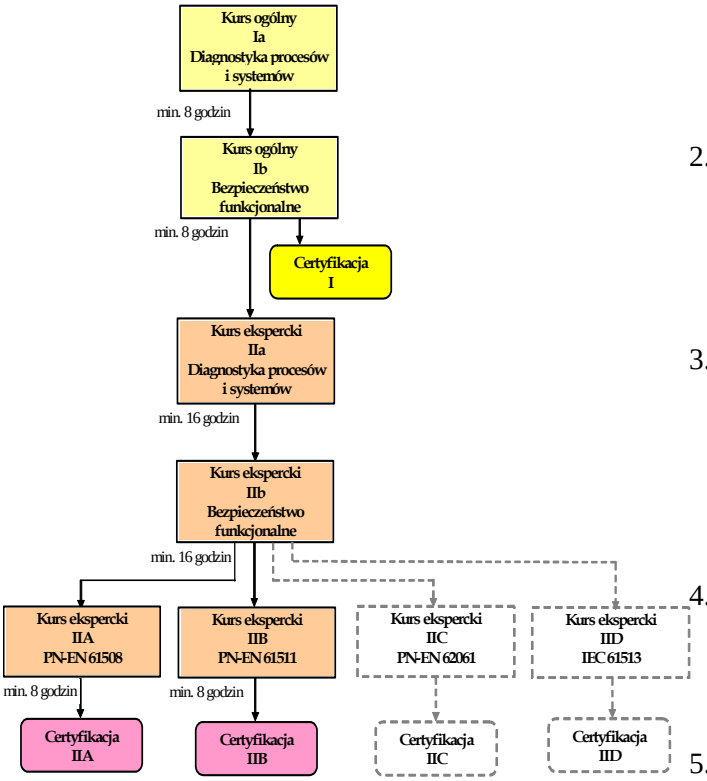


Rysunek 1. Schemat procesu certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne w systemie UDT-CERT

W przypadku spełnienia wymagań wstępnych kandydat może przystąpić do egzaminu kwalifikacyjnego po otrzymaniu zawiadomienia. Egzaminy odbywają się w ośrodkach egzaminacyjnych zatwierdzonych i nadzorowanych przez JCO UDT-CERT.
Egzamin na I jest egzaminem pisemnym i składa się z dwóch części. Część O_1 dotyczy wiedzy ogólnej z zakresu bezpieczeństwa funkcjonalnego oraz diagnostyki procesów i systemów technicznych programu. Część druga „O_2" obejmuje zakres wiedzy dotyczącej systemu UDT-CERT.
W przypadku negatywnego wyniku egzaminu kandydat może przystąpić do egzaminu poprawkowego, nie wcześniej niż po 1 miesiącu od daty egzaminu pierwotnego. Po spełnieniu wszystkich wymagań programu certyfikacji, Jednostka wydaje na swoją odpowiedzialność certyfikat w określonym stopniu i specjalności.
Certyfikat jest ważny 5 lat. Po 5 latach, na wniosek osoby certyfikowanej, następuje odnowienie certyfikatu na następne 5 lat, a po kolejnych 5 latach (łącznie po 10 latach ważności), następuje recertyfikacja. Warunki odnowienia i recertyfikacji opisuje szczegółowo program certyfikacji.
W okresie ważności certyfikatu JCO UDT-CERT sprawuje nadzór nad certyfikacją, który wynika z odpowiedzialności jednostki za działania osoby certyfikowanej przez cały okres ważności certyfikatu, gdyż wydany certyfikat poświadcza, że osoba jest cały czas kompetentna.

3.3. Wymagania dotyczące szkolenia

Kandydat ubiegający o się o certyfikacje w JCO UDT-CERT zobowiązany jest do ukończenia z wynikiem pozytywnym kursu szkoleniowego zatwierdzonego przez tę jednostkę. Kursy takie może prowadzić każda organizacja, która spełni wymagania jednostki. Obecnie zatwierdzone zostały kursy prowadzone przez Politechnikę Gdańską i Politechnikę Warszawską, organizowane odpowiednio przez Polskie Towarzystwo Bezpieczeństwa i Niezawodności (PTBN) z siedzibą w Gdyni (www.ptbn.pl) i EC Training Center Sp. z o.o. z siedzibą w Krakowie.
Na *Rysunku 2* przedstawiono schemat cyklu kursów szkoleniowych. Przystąpienie do certyfikacji na CSBF wymaga ukończenia kursów ogólnych Ia i Ib:
Kurs ogólny Ia – Diagnostyka procesów i systemów prowadzony jest przez Wydział Mechatroniki w Instytucie Automatyki i Robotyki Politechniki Warszawskiej. Informacja o tym kursie znajduje na stronie internetowej http://iair.mchtr.pw.edu.pl.



Rysunek 2. Schemat cyklu kursów szkoleniowych

Kurs ogólny Ib – Bezpieczeństwo Funkcjonalne prowadzony jest przez Wydział Elektrotechniki i Automatyki Politechniki Gdańskiej. Informacja o tym kursie znajduje na stronie internetowej http://www.ely.pg.gda.pl/zs2t/szkolenia/.
Ukończenie z pozytywnym wynikiem kursów Ia i Ib spełnia wymaganie do certyfikacji I stopnia ogólnej (CSBF). Dla stopnia II eksperckiego (CEBF), oprócz kursów Ia i Ib wymagane jest ukończenie kursów: IIa (*Diagnostyka procesów i systemów*) i IIb (*Bezpieczeństwo funkcjonalne*) oraz specjalistycznych IIA, IIB itd., zgodnie z wybraną specjalizacją (tablica 1). Informacja szczegółowa o systemie certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne znajduje się na stronach internetowych http://www.udt.gov.pl (zakładka: *Certyfikacja osób*/ *Bezpieczeństwo funkcjonalne*).

4. Zakres merytoryczny kursów szkoleniowych

4.1. Kursy szkoleniowe w Politechnice Warszawskiej

Kurs Ia. Wiedza ogólna z zakresu podstaw diagnostyki procesów i systemów (część Ia egzaminu na I stopień CSBF):

1. Zagadnienia wstępne: diagnostyka techniczna – podstawowe pojęcia; rola diagnostyki w eksploatacji systemów technicznych, diagnostyka a niezawodność i bezpieczeństwo systemów; rodzaje badań diagnostycznych, fazy diagnozowania, inne klasyfikacje; rodzaje uszkodzeń; pomiary w diagnostyce.
2. Ogólna metodologia diagnostyki procesów i systemów: podstawowe koncepcje diagnostyki procesów i systemów, detekcja, lokalizacja, identyfikacja uszkodzeń, monitorowanie stanu obiektu, prognozowanie uszkodzeń; miary jakości diagnozowania.
3. Detekcja uszkodzeń - charakterystyka podstawowych metod detekcji uszkodzeń: metody kontroli ograniczeń, metody analizy sygnałów (w tym sygnałów wibroakustycznych), metody heurystyczne, metody bazujące na modelach analitycznych, neuronowych i rozmytych procesów.
4. Lokalizacja uszkodzeń: modele opisujące związek: uszkodzenia-symptomy; podstawowe metody lokalizacji uszkodzeń: metody klasyfikacji, metody wnioskowania automatycznego, zakresy ich aplikacji.
5. Systemy diagnostyczne: systemy alarmowe a systemy diagnostyczne, diagnostyka procesów a układy automatyki zabezpieczeniowej, idea budowy systemów tolerujących uszkodzenia
6. Wybrane inne zagadnienia: termowizja, metody diagnostyki sprzętu i oprogramowania systemów komputerowych.

Kurs IIa. Wiedza z zakresu metod diagnostyki procesów i systemów (część IIa egzaminu na II stopień CEBF)

1. Zagadnienia wstępne: cele diagnostyki procesów i systemów, klasyfikacja diagnostyki w układach automatyki: diagnostyka systemu sterującego, diagnostyka inteligentnych urządzeń polowych, diagnostyka procesu, charakterystyka stosowanych metod w tych obszarach, diagnostyka zdalna i lokalna (wbudowana).
2. Modele procesów i modele diagnostyczne: ogólny opis matematyczny obiektu diagnozowania z uwzględnieniem uszkodzeń, modele procesów – do detekcji uszkodzeń, modele diagnostyczne – do lokalizacji uszkodzeń.
3. Schematy diagnozowania: przegląd różnych koncepcji diagnozowania procesów i systemów: diagnostyka na podstawie analizy sygnałów, diagnostyka na podstawie modeli procesów.
4. Detekcja uszkodzeń: metody kontroli ograniczeń, metody analizy sygnałów, metody heurystyczne, metody bazujące na modelach analitycznych, metody bazujące na modelach neuronowych i rozmytych (w tym sieci neuronowe stosowane do detekcji uszkodzeń i modele rozmyte typu TSK).
5. Lokalizacja uszkodzeń: metody pozyskiwania wiedzy o relacji uszkodzenia- symptomy, metody

wnioskowania automatycznego, metody klasyfikacji, zastosowanie logiki rozmytej we wnioskowaniu diagnostycznym.
6. Identyfikacja uszkodzeń: identyfikacja uszkodzeń nagłych, monitorowania uszkodzeń narastających (degradacji obiektu)
7. Projektowanie układów diagnostycznych: analiza obiektu, dobór zbioru testów (algorytmów detekcyjnych), analiza wykrywalności i rozróżnialności uszkodzeń, metody podwyższenia wskaźników jakości diagnozowania, przykład projektowania.
8. Problemy praktyczne: uszkodzenia wielokrotne, opóźnienia symptomów, niepewności w procesie diagnozowania, zmienność struktury obiektu, dekompozycja obiektu diagnozowanie zdecentralizowane.
9. Systemy diagnostyczne: metody i systemy diagnostyki inteligentnych urządzeń obiektowych, systemy diagnostyki procesów przemysłowych, oprogramowanie do nadzoru pętli regulacyjnych.
10. Układy automatyki tolerujące uszkodzenia, redundancja a tolerowanie uszkodzeń, układy regulacji tolerujące uszkodzenia torów pomiarowych i urządzeń wykonawczych.

Dwudniowe kursy Ia prowadzone są okresowo przez zespół prof. J.M. Kościelnego. Opis niektórych zagadnień omawianych podczas tego kursu zawierają prace [4], [5] i [8]. W bieżącym roku zaplanowano prowadzenie kursów IIa (CEBF).

4.2. Kursy szkoleniowe w Politechnice Gdańskiej

Kurs Ib. Wiedza ogólna z zakresu bezpieczeństwa funkcjonalnego systemów (część Ib egzaminu na I stopień CSBF)

Zakres tego kursu obejmuje zagadnienia bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń w nawiązaniu do norm PN-EN 61508 i PN-EN 61511 oraz PN-EN 62061.

1. Ogólne wymagania zawarte w PN-EN 61508 i jej relacje z normami sektorowymi PN-EN 61511 i PN-EN 62061.
2. Ważniejsze pojęcia i definicje związane z niezawodnością i bezpieczeństwem obiektów i systemów; ryzyko indywidualne i grupowe.
3. Koncepcja i cele zarządzania bezpieczeństwem funkcjonalnym w cyklu życia.
4. Wymagania kompetencyjne oraz dotyczące dokumentowania i wprowadzania zmian.
5. Identyfikacja zagrożeń i definiowanie funkcji związanych z bezpieczeństwem.
6. Metoda HAZOP w analizie potencjalnych zdarzeń i scenariuszy awaryjnych.
7. Określanie poziomu nienaruszalności bezpieczeństwa SIL na podstawie analizy i oceny ryzyka; metoda matrycy ryzyka.
8. Metoda ALARP w ocenie rozwiązań sterowania ryzykiem.
9. Potencjalne błędy systematyczne w systemach E/E/PE i ich unikanie; znaczenie jakości oprogramowania i wymagania w cyklu życia.
10. Wymagania dotyczące specyfikacji i bezpieczeństwa oprogramowania; protokoły komunikacyjne i ochrona sieci.
11. Rodzaje uszkodzeń elementów; dane niezawodnościowe i ich uaktualnianie w czasie.
12. Kryteria probabilistyczne dla wyróżnionych rodzajów pracy systemów E/E/PE.
13. Ograniczenia architektoniczne w systemach E/E/PE.
14. Przykładowe rozwiązania systemów E/E/PE do realizacji funkcji związanych z bezpieczeństwem.
15. Weryfikacja poziomu SIL metodą jakościową i charakterystyka metod ilościowych.
16. Problem uszkodzeń zależnych i zasady zmniejszania ich prawdopodobieństwa.
17. Analiza warstw zabezpieczeń LOPA według PN-EN 61511, metoda drzew zdarzeń.
18. Czynniki ludzkie w analizie bezpieczeństwa funkcjonalnego i warstw zabezpieczeń; analiza funkcjonalna, ocena rozwiązań interfejsów i systemu alarmowego.
19. Ogólne wymagania dotyczące bezpieczeństwa maszyn według PN-EN 62061.
20. Uwarunkowania diagnostyki elementów; planowanie obsługi profilaktycznej i testowania systemów E/E/PE.
21. *Metody RCM, RBM i RBI w zarządzaniu bezpieczeństwem.*
22. *Analiza kosztów i efektów (CBA) w ocenie rozwiązań technicznych.*

Zagadnienia 21 i 22 zostały włączone w szerszym wymiarze do kursu IIb.

Kurs IIb. Wiedza z zakresu bezpieczeństwa funkcjonalnego systemów (część IIb egzaminu na II stopień CEBF)

1. Wymagania dotyczące analizy bezpieczeństwa funkcjonalnego według PN-EN 61508 i 61511.
2. Model zarządzania bezpieczeństwem funkcjonalnym w cyklu życia.
3. Metody jakościowe i ilościowe w wyznaczaniu wymaganej redukcji ryzyka i określeniu poziomu SIL funkcji związanych z bezpieczeństwem; metoda matrycy ryzyka z definiowaniem kategorii strat i skutków oraz klas ryzyka.
4. Kalibrowanie grafów ryzyka zorientowanych na: obrażenia/ straty ludzkie, straty w środowisku;

wyznaczanie wynikowego SIL.
5. Kategorie A i B elementów w systemie E/E/PE i ograniczenia architektoniczne podsystemów według PN-EN 61508 i 61511.
6. Błędy systematyczne i ich unikanie, jakość oprogramowania.
7. Projektowanie funkcji i architektury przykładowych systemów E/E/PE i SIS z demonstracją laboratoryjną.
8. Bezpieczeństwo funkcjonalne w systemach rozproszonych i rozwiązania sieciowe; ocena porównawcza protokołów komunikacyjnych.
9. Dane niezawodnościowe elementów systemów E/E/PE i SIS, uaktualnianie danych niezawodnościowych w procesie eksploatacji.
10. Uszkodzenia niebezpieczne i bezpieczne, wykrywalne i niewykrywalne oraz ich szacowanie; wyznaczanie współczynnika pokrycia diagnostycznego DC.
11. Przykład zastosowania metody FMECA w projektowaniu rozwiązań bezpieczeństwa funkcjonalnego.
12. Modelowanie probabilistyczne systemów za pomocą metod RDB, FT i MG, wyznaczanie miar częstości zdarzeń niebezpiecznych PFH oraz prawdopodobieństwa niezadziałania na przywołanie PFD(t) i PFDavg.
13. Ilościowa weryfikacja SIL w warunkach niepewności.
14. Strategie obsługi profilaktycznej i optymalizowanie okresowego testowania wyposażenia dla określonego SIL na podstawie modeli probabilistycznych
15. Wymagania projektowe dotyczące systemów BPCS (SCADA/DCS), SIS/ESD i systemu alarmowego (AS) związane z niezależnością funkcjonalną warstw zabezpieczeń.
16. Uwzględnianie czynników ludzkich w analizie bezpieczeństwa funkcjonalnego, metody analizy niezawodności człowieka (HRA).
17. Charakterystyka metod RCM, RBM i RBI w zarządzaniu bezpieczeństwem.
18. Dokumentowanie analiz bezpieczeństwa funkcjonalnego
19. Analiza kosztów i efektów (CBA) w ocenie rozwiązań technicznych i organizacyjnych bezpieczeństwa funkcjonalnego.

Kurs IIA. Wiedza z zakresu bezpieczeństwa funkcjonalnego systemów według PN-EN 61508 – sprzęt i oprogramowanie(część IIA egzaminu na II stopień CEBF-A)
1. Szczegółowe wymagania i kryteria zawarte w normie PN-EN 61508.
2. Wyznaczanie na przykładach wymaganego poziomu nienaruszalności bezpieczeństwa SIL metodą matrycy i grafu ryzyka.
3. Przykłady projektowania architektury systemu E/E/PE z nadmiarowością strukturalną w podsystemach (1oo2, 2oo3), funkcjonalne i techniczne aspekty ich integrowania.
4. Weryfikacja poziomów bezpieczeństwa SIL w procesie modelowania probabilistycznego przykładowego systemu E/E/PE.
5. Metody modelowania logicznego i probabilistycznego systemu: schematów blokowych niezawodności RBD, drzew stanów niezdatności FT i grafów Markowa MG.
6. Metody uwzględniania uszkodzeń zależnych w modelowaniu probabilistycznym.
7. Metoda analizy rodzajów, skutków i krytyczności uszkodzeń FMECA.
8. Eliminowanie błędów systematycznych sprzętu i oprogramowania.
9. Metody i języki programowania stosowane w programowalnych systemach związanych z bezpieczeństwem.
10. Zastosowanie metod analizy HAZOP i FMECA w ocenie jakości oprogramowania.
11. Rodzaje testów diagnostycznych w systemach E/E/PE i SIS oraz ich realizacja w praktyce.
12. Analiza warstw zabezpieczeń.
13. Projektowanie bazy danych niezawodnościowych z uwzględnieniem kategorii elementów systemu E/E/PE oraz SIS i warunków środowiskowych.
14. Wyznaczanie współczynnika pokrycia diagnostycznego DC elementów.
15. Zasady i metody testowania modułów oprogramowania w procesie jego walidacji.
16. Integracja sprzętu i oprogramowania i całościowa walidacja systemu E/E/PE.
17. Analiza czynników ludzkich i szacowanie prawdopobieństwa potencjalnych błędów obsługi za pomocą metody HEART i THERP.
18. Procedury w zarządzaniu bezpieczeństwem funkcjonalnym; postępowanie w przypadku uszkodzeń częściowych sprzętu.
19. Bezpieczeństwo systemów doradczych.
20. Przykład komputerowo wspomaganego zarządzania bezpieczeństwem funkcjonalnym systemu E/E/PE (zastosowanie aplikacji Pro-SIL).
21. Zarządzanie bezpieczeństwem funkcjonalnym podczas eksploatacji.

Kurs IIB. Wiedza z zakresu bezpieczeństwa funkcjonalnego systemów według PN-EN 61511 – przemysł procesowy (część IIB egzaminu na II stopień CEBF).
1. Szczegółowe wymagania i kryteria zawarte w normie PN-EN 61511; inne krajowe i międzynarodowe normy OSHA, ISA.
2. Procedura identyfikacji zagrożeń i analizy ryzyka
3. Wyznaczanie reprezentatywnych scenariuszy awaryjnych i ich skutków z określeniem częstości

i skutków zdarzeń awaryjnych.
4. Przykłady stosowania metod HAZOP i FMEA/FMECA
5. Metody modelowania logicznego i probabilistycznego systemu: schematów blokowych niezawodności RBD, drzew stanów niezdatności FT i drzew zdarzeń ET.
6. Klasy w matrycy ryzyka i ocena ryzyka.
7. Określenie wymaganej redukcji ryzyka i poziomu nienaruszalności bezpieczeństwa SIL zdefiniowanych funkcji bezpieczeństwa, zastosowanie skalowanej macierzy ryzyka i kalibrowanego modyfikowanego grafu ryzyka
8. Projektowanie architektury sprzętowej systemu SIS realizującego funkcje związanie z bezpieczeństwem (elementy pomiarowe, tory sygnałowe, moduły wejść i wyjść, jednostki centralne, elementy wykonawcze itd.).
9. Problemy uwzględniania zużycia i starzenia elementów.
10. Weryfikacja poziomu nienaruszalności bezpieczeństwa SIL systemu SIS oraz weryfikacja wymaganego poziomu redukcji ryzyka za pomocą warstw zabezpieczeń w warunkach niepewności.
11. Wymagania instalacyjne i nadzoru.
12. Metoda LOPA w analizie i projektowaniu warstw zabezpieczeń z uwzględnieniem systemów BPCS (DCS, SCADA), SIS/ ESD oraz AS.
13. Zdefiniowanie zadań człowieka-operatora w ramach funkcji bezpieczeństwa.
14. Metody analizy niezawodności człowieka HRA: THERP, HEART i SLIM.
15. Ocena wpływu potencjalnych błędów człowieka na wyniki modelowania probabilistycznego warstw zabezpieczeń.
16. Przykład analizy ALARP oraz analizy kosztów i efektów w projektowaniu warstw zabezpieczeń
17. Przykład komputerowo wspomaganej analizy warstw zabezpieczeń (aplikacja Pro-SIL).
18. Zarządzanie bezpieczeństwem funkcjonalnym w procesie eksploatacji i dokumentowanie zmian.

Dwudniowe kursy Ib prowadzone są okresowo przez zespół prof. K.T. Kosmowskiego. Opis niektórych zagadnień omawianych podczas tego kursu zawierają prace [2], [3] i [6]. W bieżącym roku zaplanowano prowadzenie kursów IIb i IIB (CEBF).

5. Uwagi końcowe

W niniejszym artykule opisano krajowy system i program certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne. Program ten został wypracowany przez UDT-CERT we współpracy z członkami Komitetu Programowego nr 8, powołanego przez UDT, przy merytorycznej pomocy przedstawicieli Politechniki Gdańskiej i Politechniki Warszawskiej. Przygotowanie systemu i programu certyfikacji jest zadaniem złożonym, wymagającym uwzględnienia szeregu norm oraz aktualnej wiedzy teoretycznej i praktycznej.

We wspomnianych uczelniach prowadzone są okresowo kursy szkoleniowe Ia i Ib na poziomie ogólnym. W artykule przedstawiono zawartość merytoryczną tych kursów. Przygotowuje się obecnie kursy na poziomie eksperckim IIa, IIb i IIB. Znaczenie i złożoność przedstawionego programu certyfikacji osób wymaga dalszej pogłębionej współpracy UDT-CERT, wyższych uczelni technicznych i zainteresowanych towarzystw naukowych, zajmujących się zagadnieniami niezawodności, diagnostyki i bezpieczeństwa.

Literatura

[1] Dźwiarek, M., Kosmowski, K.T. & Missala, T. (2004). Zintegrowany program szkoleniowy w procesie wdrażania nowoczesnych rozwiązań bezpieczeństwa funkcjonalnego w Polsce. *Materiały konferencji naukowo-technicznej: Zarządzanie Bezpieczeństwem Funkcjonalnym*, Jurata, 16-17 września 2004.

[2] Goble, W.M. & Cheddie, H. (2005). Safety Instrumented Systems Verification. ISA - the Instrumentation, Systems and Automation Society. Research Triangle Park, NC 27709.

[3] Gruhn, P. & Cheddie, H.L. (2006). Safety Instrumented Systems: Design, Analysis and Justification. ISA - the Instrumentation, Systems and Automation Society. Research Triangle Park, NC 27709.

[4] Korbicz, J., Kościelny, J.M., Kowalczuk, Z. & Cholewa, W. (2002). *Diagnostyka procesów. Modele – Metody sztucznej inteligencji – Zastosowania.* Warszawa: WNT.

[5] Korbicz, J., Kościelny, J.M., Kowalczuk, Z. & Cholewa, W. (Ed.) (2004). *Fault Diagnosis. Models, Artificial intelligence, Application.* Springer, Berlin.

[6] Kosmowski, K.T. (2007). *Functional Safety Management in Critical Systems.* Gdansk University of Technology. Wydawnictwo: Fundacja Rozwoju Uniwersytetu Gdańskiego.

[7] Kosmowski, K.T. & Rogala, I. (2007). *Functional safety and managing competence.* W monografii: *Functional Safety Management in Critical Systems*. Wydawnictwo: Fundacja Rozwoju Uniwersytetu Gdańskiego. Gdańsk.

[8] Kościelny, J.M. (2001). *Diagnostyka zautomatyzowanych procesów przemysłowych.* Akademicka Oficyna Wyd. EXIT, Warszawa.

[9] Ustawa z dnia 21 grudnia 2000 r. o dozorze technicznym (Dz. U. Nr 122, poz. 1321, z późn. zm.).
[10] PN-EN 61508-1 (2004). Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem Część 1: Wymagania ogólne.
[11] PN-EN 61511-1 (2007). Bezpieczeństwo funkcjonalne Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego Część 1: Schemat, definicje, wymagania dotyczące systemu, sprzętu i oprogramowania.
[12] PN-EN 62061 (2008). Bezpieczeństwo maszyn – Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem.
[13] PN-EN ISO/IEC 17024 (2004). Ocena zgodności. Ogólne wymagania dotyczące jednostek certyfikujących osoby.
[14] Program Certyfikacji Osób Odpowiedzialnych za Bezpieczeństwo Funkcjonalne, wydanie 2, JCO UDT-CERT Warszawa, 9.12.2010.