MARCIN ŚLIWIŃSKI

BEZPIECZEŃSTWO FUNKCJONALNE I OCHRONA INFORMACJI W OBIEKTACH I SYSTEMACH INFRASTRUKTURY KRYTYCZNEJ

POLITECHNIKA GDAŃSKA

monografie
171

PRZEWODNICZĄCY KOMITETU REDAKCYJNEGO
WYDAWNICTWA POLITECHNIKI GDAŃSKIEJ
Janusz T. Cieśliński

REDAKTOR PUBLIKACJI NAUKOWYCH
Michał Szydłowski

REDAKTOR SERII
Zbigniew Krzemiński

RECENZENCI
Marek Dźwiarek
Kazimierz Lebecki

REDAKCJA JĘZYKOWA
Agnieszka Frankiewicz

PROJEKT OKŁADKI
Jolanta Cieślawska

Wydano za zgodą
Rektora Politechniki Gdańskiej

Oferta wydawnicza Politechniki Gdańskiej jest dostępna pod adresem
www.pg.edu.pl/wydawnictwo/katalog
zamówienia prosimy kierować na adres wydaw@pg.edu.pl

ISBN 978-83-7348-743-7

WYDAWNICTWO POLITECHNIKI GDAŃSKIEJ

Wydanie I. Ark. wyd. 14,9, ark. druku 13,75, 171/1010

Druk i oprawa: Volumina.pl Daniel Krzanowski
ul. Księcia Witolda 7-9, 71-063 Szczecin, tel. 91 812 09 08

SPIS TREŚCI

Wykaz ważniejszych oznaczeń i akronimów

Oznaczenia

α – współczynnik rodzaju uszkodzenia
β – udział uszkodzeń niewykrytych, które mają wspólną przyczynę
β_F – prawdopodobieństwo warunkowe wystąpienia wyróżnionego skutku końcowego zdarzenia krytycznego
β_{kzn} – udział uszkodzeń niewykrytych o wspólnej przyczynie dla architektury nadmiarowej (k z n)
C – krytyczność skutków
C_{bf} – krytyczność skutków związanych z bezpieczeństwem funkcjonalnym
C_{cf} – krytyczność skutków związanych z cyberzagrożeniami
C_{kzn} – współczynnik korekcyjny w modelu uszkodzeń β_{kzn}
C_m – liczba krytyczności rodzaju uszkodzenia
C_r – liczba krytyczności jednostki
$f_{i,j}$ – funkcja dwuparametrowa
$F(T)$ – prawdopodobieństwo niesprawności podsystemu/ elementu systemu E/E/PE w chwili T
F_{cs} – częstość występowania cyberataku
F_{np} – częstość zdarzenia awaryjnego bez uwzględnienia systemu zabezpieczeniowego
F_t – częstość zdarzenia awaryjnego zredukowana do poziomu ryzyka akceptowalnego
$I^B(i|t)$ – miara ważności Birnbauma
$I^C(i|t)$ – miara krytyczności
$I^{VF}(i|t)$ – miara ważności Vesely'ego–Fussella
λ – intensywność uszkodzeń [h^{-1}]
λ_{avg} – przeciętna intensywność uszkodzeń [h^{-1}]
λ_D – intensywność uszkodzeń niebezpiecznych [h^{-1}]
λ_{DD} – intensywność uszkodzeń niebezpiecznych wykrywalnych przez testy diagnostyczne [h^{-1}]
λ_{DU} – intensywność uszkodzeń niebezpiecznych niewykrywalnych przez testy diagnostyczne [h^{-1}]
λ_S – intensywność uszkodzeń bezpiecznych [h^{-1}]
λ_{SD} – intensywność uszkodzeń bezpiecznych wykrywalnych przez testy diagnostyczne [h^{-1}]
λ_{SU} – intensywność uszkodzeń bezpiecznych niewykrywalnych przez testy diagnostyczne [h^{-1}]
μ – współczynnik częstości napraw [h^{-1}]
π_i – współczynnik korekcyjny uwzględniający wpływ warunków środowiskowych
R – ryzyko
$R(T)$ – niezawodność podsystemu/ elementu systemu E/E/PE w chwili T
r^F – względna redukcja częstości rozważanego scenariusza awaryjnego
R_{np} – ryzyko bez zastosowania systemu zabezpieczeniowego
R_t – ryzyko tolerowane
t_{CE} – średni czas przestoju wyposażenia kanału [h]
t_{GE} – średni czas przestoju wyposażenia grupy głosowania [h]
T_I – interwał przeprowadzania testów okresowych [h]
w_R – wskaźnik różnicowy
w_R^d – wskaźnik różnicowy dolny
w_R^g – wskaźnik różnicowy górny

Akronimy

AI (*analog input*) – wejście analogowe
ALARP (*as low as reasonably practicable*) – zasada, zgodnie z którą każde ryzyko powinno zostać zmniejszone w takim stopniu, w jakim jest to racjonalnie uzasadnione
AO (*analog output*) – wyjście analogowe
BPCS (*basic process control system*) – podstawowy system sterowania procesem
CBA (*cost benefit analysis*) – analiza kosztów i efektów
CC (*common criteria*) – wspólne kryteria wg ISO/IEC 15408
CCF (*common cause failure*) – uszkodzenie o wspólnej przyczynie
CPU (*central processor unit*) – jednostka centralna procesora
DC (*diagnostics coverage*) – pokrycie diagnostyczne
DCS (*distributed control system*) – rozproszony system sterowania
DI (*digital input*) – wejście dyskretne
DMZ (*demilitarized zone*) – strefa zdemilitaryzowana
DNS (*domain name system*) – system nazw domenowych
DO (*digital output*) – wyjście dyskretne
DoS (*denial of service*) – blokada usług (atak na system komputerowy lub usługę sieciową)
E/E/PE (*electrical/ electronic/ programmable electronic*) – elektryczny/ elektroniczny/ programowalny elektroniczny
E/E/PES (*electrical/ electronic/ programmable electronic system*) – system elektryczny/ elektroniczny/ programowalny elektroniczny
EAL (*evaluation assurance level*) – poziom uzasadnionego zaufania
ESD (*emergency shutdown*) – wyłączanie awaryjne
ETA (*event tree analysis*) – analiza drzewa zdarzeń
EUC (*equipment under control*) – wyposażenie sterowane
FAT (*factory acceptance test*) – test wykonywany przed dostawą do miejsca docelowego
FMEA (*failure modes and effect analysis*) – analiza rodzajów i skutków uszkodzeń
FMECA (*failure modes, effects and criticality analysis*) – analiza rodzajów, skutków i krytyczności uszkodzeń
FMEDA (*failure mode effect and diagnostic analysis*) – analiza rodzajów, skutków i diagnostyki uszkodzeń
EMC (*electromagnetic compatibility*) – kompatybilność elektromagnetyczna
FPL (*fixed program language*) – język o stałym programie
FSA (*functional safety assesment*) – ocena bezpieczeństwa funkcjonalnego
FTA (*fault tree analysis*) – analiza drzewa niezdatności
FVL (*full variability language*) – język o pełnej zmienności
HAZID (*hazard identification*) – identyfikacja zagrożeń
HAZOP (*hazard and operability study*) – analiza zagrożeń i zdolności działania
HFT (*hardware fault tolerance*) – odporność sprzętu na uszkodzenia
HW (*hardware*) – sprzęt
IACS (*industrial automation and control system*) – system sterowania i automatyki przemysłowej
ICS (*industrial control system*) – przemysłowy system sterowania
IEC (*international electrotechnical commision*) – międzynarodowa komisja elektrotechniczna
ISO (*International Standarization Organization*) – Międzynarodowa Organizacja Normalizacyjna
IT (*information technology*) – technologie informacyjne
LAN (*local area network*) – sieć lokalna
LCC (*life cycle cost*) – analiza kosztów w cyklu życia
LOPA (*layer of protection analysis*) – analiza warstw zabezpieczeń
LVL (*limited variability language*) – język o ograniczonej zmienności
MDT (*mean down time*) – średni czas przestoju
MTBF (*mean time between failures*) – średni czas między uszkodzeniami

MTDF (*mean time to detect failure*) – średni czas do wykrycia uszkodzenia
MTTF (*mean time to failure*) – średni czas do uszkodzenia
MTTR (*mean time to repair*)– średni czas do naprawy
NIST (*National Institute of Standard and Technology*) – Narodowy Instytut Standaryzacji i Technologii
NP (*non-programmable*) – nieprogramowalny
OT (*operational technology*) – sprzęt i oprogramowanie przemysłowych systemów sterowania ICS
P&ID (*piping & instrumentation diagram*) – schemat instalacji i oprzyrządowania
PES (*programmable electronic system*) – programowalny system elektroniczny
PFD_{avg} (*probability of failure on demand average*) – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na żądanie
PFH (*average frequency of a dangerous failure per hour*) – średnia częstość występowania uszkodzenia niebezpiecznego na godzinę
PHA (*preliminary hazard analysis*) – wstępna analiza zagrożeń
PL (*performance level*) – poziom zapewnienia bezpieczeństwa
PLC (*programmable logic controller*) – sterownik programowalny
PSV (*pressure shutdown valve*) – ciśnieniowy zawór bezpieczeństwa
RBD (*reliability block diagram*) – schemat blokowy niezawodności
RRF (*risk reduction factor*) – wskaźnik redukcji ryzyka
SAL (*security assurance level*) – poziom uzasadnionej ochrony
SAT (*site acceptance test*) – test systemu w miejscu docelowym, instalacja i rozruch systemu
SCADA (*supervisory control and data aquisition*) – system monitoringu i akwizycji danych
SFF (*safe failure fraction*) – wskaźnik uszkodzeń bezpiecznych
SIF (*safety instrumented function*) – przyrządowa funkcja bezpieczeństwa
SIL (*safety integrity level*) – poziom nienaruszalności bezpieczeństwa
SIS (*safety instrumented system*) – przyrządowy system bezpieczeństwa
SIT (*site integration test*) – test integralności systemów BPCS i SIS
SRCF (*safety-related control function*) – funkcja sterowania związana z bezpieczeństwem
SRECS (*safety-related electrical control system*) – elektryczny system sterowania związany z bezpieczeństwem
SRS (*safety-related system*) – system związany z bezpieczeństwem wg PN-EN 61508
SRS (*safety requirements specification*) – specyfikacja wymagań bezpieczeństwa wg PN-EN 61511
SW (*software*) – oprogramowanie
SZBI system zarządzania bezpieczeństwem informacji
THR (*torelable hazard rate*) – wskaźnik zagrożenia tolerowanego wg PN-EN 50129
TOE (*target of evaluation*) – cel oceny
VPN (*virtual private network*) – prywatna sieć wydzielona
WLAN (*wireless local area network*) – lokalna sieć bezprzewodowa

Rozdział 1

WSTĘP

Na bezpieczeństwo systemu technicznego infrastruktury krytycznej składa się wiele różnych aspektów. Wśród nich znajdują się dwa bardzo ważne ogniwa, które mogą bezpośrednio wpływać na stopień ryzyka występującego w badanym obiekcie czy systemie. Są to bezpieczeństwo funkcjonalne, które należy traktować jako jeden z czynników zmniejszających ryzyko związane z działaniem systemu technicznego, oraz ochrona informacji. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym [208] definiuje infrastrukturę krytyczną jako systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje oraz usługi kluczowe dla bezpieczeństwa państwa i jego obywateli. Infrastruktura krytyczna obejmuje m.in. systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, składowania i stosowania substancji chemicznych, w tym rurociągi ropy naftowej i gazu ziemnego [208].

W zarządzaniu bezpieczeństwem funkcjonalnym podkreśla się ostatnio znaczenie ochrony informacji systemów komputerowych, szczególnie tych, które pełnią odpowiedzialne funkcje monitorowania, sterowania i zabezpieczeń. Zagadnienie to dotyczy ochrony informacji (w postaci ochrony danych, dokumentacji, dostępu do systemów informatycznych, sieci przewodowych i bezprzewodowych, zarówno firmowych, jak i przemysłowych, itp.). Wymaga ono również przeprowadzenia odpowiedniej analizy, która będzie miała za zadanie zidentyfikowanie potencjalnych zagrożeń występujących w analizowanym systemie bądź obiekcie, ocenę tego typu zagrożeń oraz zaproponowanie potencjalnych rozwiązań im przeciwdziałających. Ogólne wymagania dotyczące zagadnień ochrony informacji w takich systemach są zawarte w normie międzynarodowej ISO/IEC 15408 [93]. Podstawowe zasady związane z zapewnieniem bezpieczeństwa i ochrony informacji zawierają normy PN-ISO/IEC 17779 [171] oraz PN-ISO/IEC 27001 [95]. Normy te dotyczą więc różnych aspektów bezpieczeństwa systemów komputerowych i ochrony informacji.

W praktyce istnieje potrzeba integrowania zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji. Znana jest metodyka SeSa (*SecureSafety*) norweskiej organizacji badawczej SINTEF, opracowana dla systemów sterowania i automatyki zabezpieczeniowej stosowanych w przemyśle wydobywczym na morskich platformach wiertniczych, monitorowanych i zarządzanych zdalnie z lądu, poprzez ogólnie dostępne środki komunikacyjne. Rozwijana jest też metodyka integracji zagadnień bezpieczeństwa funkcjonalnego z zagadnieniami ochrony informacji poprzez uwzględnianie problematyki cyberzagrożeń w postaci poziomów uzasadnionego zaufania EAL w ramach określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL oraz jego późniejszej weryfikacji dla analizowanych funkcji bezpieczeństwa.

W niniejszej monografii zakłada się, że bezpieczeństwo funkcjonalne obiektu technicznego infrastruktury krytycznej powinno być traktowane w sposób nadrzędny, tzn. wyniki oceny ochrony informacji, a także cyberzagrożenia dla tego typu systemu będą brane pod uwagę przy oszacowywaniu aktualnego poziomu redukcji ryzyka z punktu widzenia analiz bezpieczeństwa funkcjonalnego oraz będą miały wpływ na wynikową wartość poziomu nienaruszalności bezpieczeństwa SIL, uzyskaną w procesie weryfikacji.

Zagadnienia związane z zarządzaniem bezpieczeństwem funkcjonalnym systemów sterowania i automatyki zabezpieczeniowej są zawarte w normie PN-EN 61508 [161] o charakterze ogólnym (dotyczącej różnych zastosowań) oraz normach sektorowych, np. PN-EN 61511 [162] opracowanej dla potrzeb przemysłu procesowego i wydobywczego. Natomiast zagadnienia związane z przemysłowymi sieciami komunikacyjnymi oraz z ich bezpieczeństwem i ochroną przekazywanych poprzez nie informacji zawarte są w normach PN-EN 61784, ISO/IEC 15408, PN-EN 61158 oraz IEC 62443 [89, 93, 160, 163, 164, 165]. Interesująca jest zwłaszcza ta ostatnia pozycja, wprowadzająca do oceny przemysłowych systemów sterowania ICS poziomy uzasadnionej ochrony SAL, które swoją konstrukcją nawiązują do poziomów nienaruszalności bezpieczeństwa SIL.

W monografii omówiono aktualne zagadnienia związane z integracją analizy i oceny bezpieczeństwa funkcjonalnego rozproszonych systemów sterowania, monitorowania i zabezpieczeń w obiektach i systemach infrastruktury krytycznej, w nawiązaniu do wymagań norm PN-EN 61508 [161] i PN-EN 61511 [162] z uwzględnieniem zasad ochrony informacji według ISO/IEC 15408 [93], PN-ISO/IEC 17779 [171], metodyki SeSa oraz ISO/IEC 62443 [58, 89]. Przedstawiona koncepcja integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji uwzględnia klasyfikację systemów rozproszonych. Mimo że aspekty związane z analizami bezpieczeństwa funkcjonalnego i ochrony informacji zasadniczo się różnią i dotyczą odrębnych zagadnień (bezpieczeństwo funkcjonalne – automatyka, ochrona informacji – technologie informacyjne), uwzględnienie zagadnień ochrony informacji w analizach bezpieczeństwa funkcjonalnego jest możliwe.

Zaproponowana w monografii metodyka bazuje na odpowiednim integrowaniu kryteriów bezpieczeństwa funkcjonalnego z uwzględnieniem poziomów nienaruszalności bezpieczeństwa SIL i poziomów ochrony informacji (uzasadnionego zaufania EAL oraz uzasadnionej ochrony SAL), w ramach rozszerzonej analizy i oceny ryzyka, a następnie weryfikowaniu tych poziomów dla rozważanych architektur sprzętowych i zastosowanych środków ochrony. Otwarte pozostaje pytanie, czy taka integracja jest właściwa. Z punktu widzenia analiz bezpieczeństwa funkcjonalnego można zastosować zbliżone ideowo do SIL poziomy uzasadnionego zaufania EAL. Jednak ich praktyczna implementacja oraz występujące trudności w ich interpretacji i zrozumieniu sprawiają, że można zauważyć tendencję do niewykorzystywania ich w próbach integracji z bezpieczeństwem funkcjonalnym. Dotyczą one bowiem w zdecydowanej większości pojedynczych rozwiązań technicznych (urządzeń, aplikacji komputerowych itp.), a nie podsystemów czy całych systemów. W związku z tym należy poważnie rozważyć stosowność korzystania z miar EAL na rzecz wartości bardziej ogólnych, będących urzeczywistnieniem realnego poziomu bezpieczeństwa związanego z ochroną informacji, a w istocie poziomu związanego z nią ryzyka. Być może zatem dobrą praktyką w integracji tych zagadnień będzie stosowanie poziomów uzasadnionej ochrony SAL, które w naturalny sposób (choćby przez tę samą liczbę poziomów – 1–4) nawiązują do znanych poziomów nienaruszalności bezpieczeństwa SIL.

W obiektach infrastruktury krytycznej systemy sterowania i automatyki zabezpieczeniowej są najczęściej projektowane jako systemy rozproszone, których nieprawidłowe działanie może doprowadzić do poważnych skutków, np.: skażenia środowiska, pożaru, wybuchu, utraty zdrowia i życia osób, spadku lub załamania produkcji, a w konsekwencji – znacznych strat ekonomicznych. Zagadnienia bezpieczeństwa funkcjonalnego i ochrony informacji powinny być zatem rozpatrywane w sposób zintegrowany, w zależności od rodzaju kanałów komunikacji stosowanych do transmisji danych pomiędzy elementami systemu. Ważną kwestią w integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji jest opracowanie skutecznych metod pozwalających uwzględnić wpływ cyber-

zagrożeń w modelowaniu probabilistycznym systemów automatyki zabezpieczeniowej. Tych aspektów nie można pominąć, gdyż uzyskane wyniki mogą być zbyt optymistyczne w stosunku do rzeczywistej sytuacji.

Rozdział 2

ZAGADNIENIA OCHRONY INFORMACJI W ANALIZACH BEZPIECZEŃSTWA FUNKCJONALNEGO

2.1. Wprowadzenie

Niniejsza monografia jest poświęcona zagadnieniom zarządzania bezpieczeństwem funkcjonalnym w cyklu życia z uwzględnieniem norm międzynarodowych PN-EN 61508 [161] i PN-EN 61511 [162] oraz zarządzania bezpieczeństwem informacji w systemach i sieciach komputerowych w nawiązaniu do wytycznych OECD [145] i wymagań normy ISO/IEC 27001 [95]. Autor rozważa przykłady skupionych i rozproszonych sieci komputerowych pełniących funkcje monitorowania, sterowania i zabezpieczeń, w tym systemu SCADA w obiektach i systemach infrastruktury krytycznej. Zarysowano całościowe podejście do formułowania wymagań i kryteriów z uwzględnieniem aspektów *safety* i *security* w analizie zagrożeń i ocenie ryzyka. Przedstawiono również wymagania dotyczące oprogramowania realizującego funkcje związane z bezpieczeństwem oraz kanałów komunikacyjnych uczestniczących w realizacji tych funkcji w przemysłowych sieciach komputerowych.

Dynamiczny rozwój przyczynił się istotnie do cywilizacyjnego i gospodarczego rozwoju wielu krajów. Z drugiej jednak strony narastają obecnie trudności i problemy, które wpływają niekorzystnie na jakość życia i poczucie bezpieczeństwa poszczególnych ludzi i całych społeczności. Społeczeństwa wykorzystujące szeroko osiągnięcia współczesnej cywilizacji i techniki – w tym nowoczesne środki informatyczne oraz sieci komputerowe i telekomunikacyjne – w komunikowaniu się i pozyskiwaniu użytecznej wiedzy napotykają jednocześnie znaczne trudności w nadążaniu za szybkimi zmianami technologii do stosowania w praktyce, zarówno w życiu prywatnym, jak i zawodowym. Dotyczy to zwłaszcza aktywności indywidualnej i zespołowej w szeroko rozumianej gospodarce w różnych specjalizacjach zawodowych, a szczególnie w transporcie i przemyśle, gdzie nadal występuje wiele wypadków, awarii i katastrof powodujących jeszcze zbyt często duże straty ludzkie, środowiskowe, materialne i ekonomiczne.

Coraz dobitniej uzmysławiamy sobie, że z licznymi dziedzinami aktywności człowieka związane jest ryzyko indywidualne i grupowe, a nawet społeczne. Pojawiają się nowe zagrożenia, które wymagają badań i wdrożenia na czas przeciwdziałania, po to by ograniczyć ich możliwe skutki w przyszłości. Ryzyka wypadków i awarii nie można niestety w pełni wyeliminować. Dlatego ważne jest podejmowanie działań mających na celu identyfikację zagrożeń, analizę i oszacowanie poziomu ryzyka oraz podejmowanie racjonalnych decyzji i wdrażanie działań opartych na ocenach ryzyka [113]. Będzie to sprzyjać rozwojowi społecznemu i gospodarczemu przy zaakceptowanych poziomach ryzyka, które powinny być systematycznie analizowane i oceniane.

Problematyka niezawodności i bezpieczeństwa instalacji przemysłowych podwyższonego ryzyka oraz obiektów i systemów infrastruktury krytycznej znajduje się ostatnio w centrum uwagi organów dozoru technicznego, inspekcji środowiska i różnych instytucji państwa zarządzających bezpieczeństwem. Istotne znaczenie w projektowaniu i wdrażaniu nowych rozwiązań systemów sterowania i zabezpieczeń mają obecnie technologie progra-

mowalne, znane jako rozwiązania bezpieczeństwa funkcjonalnego i stosowane w różnych sektorach przemysłu oraz gospodarki [106, 109, 110, 113, 137].

Systemy takie są postrzegane przez specjalistów jako środki redukcji ryzyka związanego z występującymi obiektywnie zagrożeniami i potencjalnymi zdarzeniami awaryjnymi. Ryzyko oszacowane po zastosowaniu odpowiednich rozwiązań programowalnych systemów E/E/PE (elektrycznych, elektronicznych, programowalnych elektronicznych) powinno być utrzymywane w cyklu życia na określonym akceptowanym poziomie, np. zgodnie z ogólnymi wymaganiami i kryteriami zawartymi w normie bezpieczeństwa funkcjonalnego PN-EN 61508 [161].

W obiektach i systemach infrastruktury krytycznej mogą wystąpić zdarzenia nienormalne i zdarzenia awaryjne, a nawet stany krytyczne powodujące poważne straty. Zdarzenia takie są powodowane zakłóceniami zarówno wewnątrz obiektu, jak i w obiektach współpracujących. Wynikają one z nieuniknionych w praktyce uszkodzeń wyposażenia i błędów człowieka, stymulowanych przez warunki środowiskowe, a więc mają związek ze stosowaną technologią i występującymi obiektywnie zagrożeniami. Mówi się wówczas o zagadnieniach bezpieczeństwa w sensie *safety*, w odróżnieniu od zagadnień bezpieczeństwa w sensie *security*, kiedy to zagrożenia są związane z nieprzyjaznymi działaniami człowieka o charakterze intencyjnym [99, 108, 116, 120]. Przykładami takich działań mogą być ataki hakerskie na komputerowe systemy sterowania i zabezpieczeń infrastruktury krytycznej poprzez sieć komputerową albo bezpośrednie działanie stanowiące atak terrorystyczny w celu pokonania barier elektronicznych i fizycznych, po to by spowodować jak największe straty.

Zagadnienia bezpieczeństwa znajdują się coraz częściej w centrum uwagi różnych instytucji Unii Europejskiej. Po określeniu zasad polityki bezpieczeństwa w skali makro kluczowym zagadnieniem staje się efektywne realizowanie różnych jej aspektów poprzez odpowiednie instytucje międzynarodowe, np. Organizację Współpracy Gospodarczej i Rozwoju [149], a także rządy i instytucje w krajach członkowskich. Celem jest systematyczne i efektywne wdrażanie technicznych i organizacyjnych rozwiązań bezpieczeństwa, głównie w obiektach i systemach infrastruktury krytycznej oraz w przemyśle i transporcie.

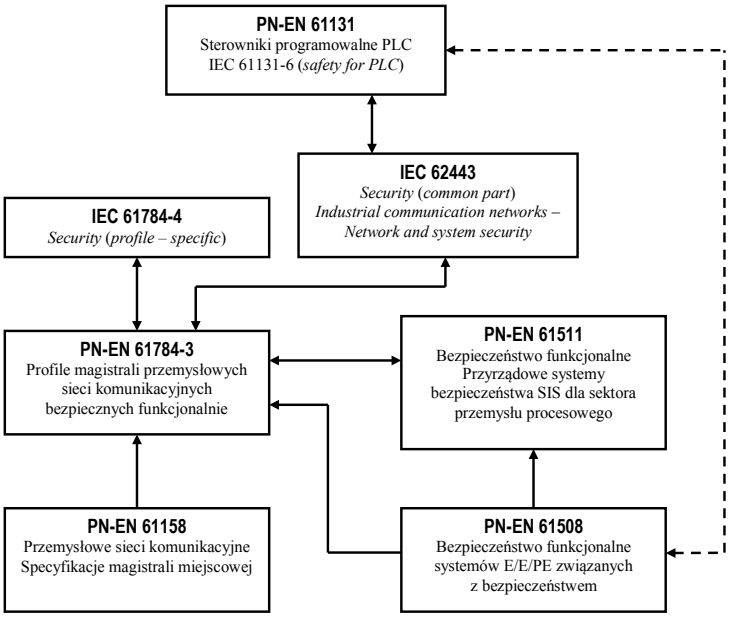
W niniejszej monografii przedstawiono wybrane zagadnienia dotyczące bezpieczeństwa w sensie *safety* i *security*, przy czym nacisk położono na zarządzanie bezpieczeństwem funkcjonalnym, które jest ważną częścią bezpieczeństwa traktowanego całościowo [113]. Zarządzanie to dotyczy systemów monitorowania i sterowania oraz systemów alarmowych i zabezpieczających, opartych na technologiach programowalnych i działających w sieciach komputerowych.

Zarządzanie bezpieczeństwem funkcjonalnym opiera się na analizach i ocenach ryzyka przeprowadzanych w cyklu życia analizowanego obiektu złożonego lub systemu rozproszonego w odniesieniu do wymagań związanych z unikaniem błędów i uszkodzeń systematycznych oraz błędów i uszkodzeń o charakterze losowym w systemach programowalnych pełniących funkcje związane z bezpieczeństwem [161].

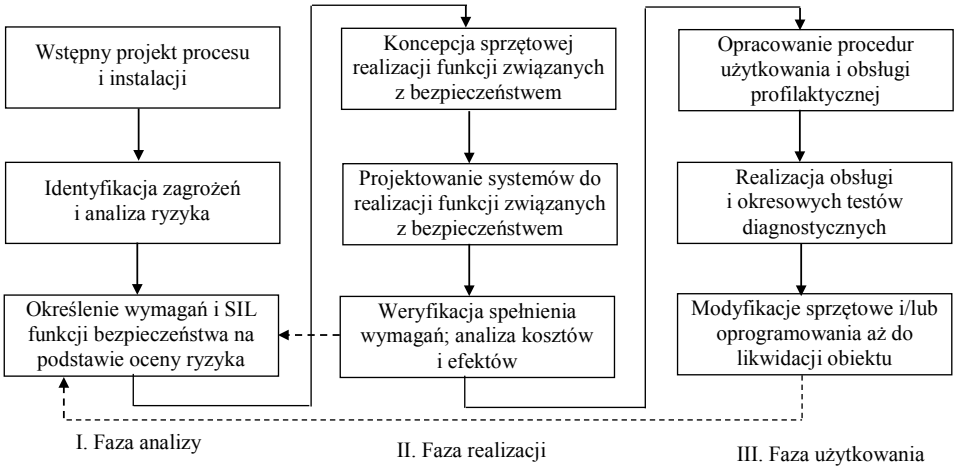
Część 3 normy PN-EN 61784, dotyczącej przemysłowych sieci komunikacyjnych, obejmuje zagadnienia związane z magistralami miejscowymi bezpiecznymi funkcjonalnie [165]. Pomiędzy normami, które wymieniono wcześniej, istnieją pewne relacje, których częścią integrująca jest norma PN-EN 61784-3 (rys. 2.1) [165]. Warto zwrócić uwagę, że wymagania dla sterowników programowalnych *safety PLC*, stanowiących znaczny odsetek jednostek logicznych w systemach BPCS, DCS i SIS, reguluje norma IEC 61131-6.

Zarządzanie bezpieczeństwem funkcjonalnym w cyklu życia musi dotyczyć wszystkich etapów związanych z projektowaniem, wdrożeniem i eksploatacją obiektu techniczne-

go. W procesie projektowania i eksploatacji/ użytkowania rozwiązań bezpieczeństwa funkcjonalnego wyróżnia się trzy fazy (rys. 2.2): I – fazę analizy, II – fazę realizacji, III – fazę użytkowania.



Rys. 2.1. Relacje między normami bezpieczeństwa funkcjonalnego i przemysłowych sieci komunikacyjnych wg PN-EN 61784-3



Rys. 2.2. Fazy i zadania w procesie projektowania i użytkowania rozwiązań bezpieczeństwa funkcjonalnego [50, 54, 122]

Faza analizy ma na celu zdefiniowanie funkcji związanych z bezpieczeństwem i określenie ich poziomów nienaruszalności bezpieczeństwa SIL na podstawie oceny ryzyka.

Faza realizacji obejmuje projektowanie systemów, które będą realizowały funkcje związane z bezpieczeństwem oraz weryfikację wymagań. Zawiera ona również analizę kosztów i efektów CBA rozważanych rozwiązań lub analizę w cyklu życia LCC. Wskazuje się do zaimplementowania najkorzystniejszą opcję systemu E/E/PE lub SIS, spełniającą określone kryteria i wymagania oraz uzasadnioną (optymalną lub racjonalną) z punktu widzenia kosztów i efektów [28, 54].

Faza użytkowania obejmuje przeprowadzanie obsługi profilaktycznej i okresowych testów diagnostycznych mających na celu wykrycie uszkodzeń niebezpiecznych w urządzeniach i podsystemach, niewykrywalnych w testach automatycznych. Jeśli okaże się to celowe, przeprowadza się modyfikacje sprzętowe i/lub oprogramowania.

Zagadnienia związane ściśle z zarządzaniem ochroną informacji są przedstawione w odpowiednich dokumentach normatywnych, m.in. ISO/IEC 15408 [93], PN-ISO/IEC 17779 [171] PN-ISO/IEC 27000 [172] oraz ISO/IEC 27001 [95]. Zarządzanie bezpieczeństwem informacji zostało opisane w ostatniej z wymienionych norm; zgodnie z jej wymaganiami organizacja zainteresowana systemem zarządzania bezpieczeństwem informacji (SZBI) podejmuje działania w następujących etapach:

1) ustanawianie SZBI;
2) wdrażanie i korzystanie z SZBI;
3) monitorowanie i przegląd SZBI;
4) utrzymywanie i doskonalenie SZBI.

Ustanawianie SZBI obejmuje następujące zagadnienia:

a) zdefiniowanie zakresu i granic SZBI;
b) zdefiniowanie polityki SZBI;
c) zdefiniowanie podejścia do szacowania ryzyka w organizacji;
d) określenie ryzyka;
e) analizowanie i ocenianie ryzyka;
f) zdefiniowanie i ocenę wariantów postępowania z ryzykiem;
g) wybranie celów stosowania zabezpieczeń i konkretnych zabezpieczeń jako środków postępowania z ryzykiem;
h) uzyskanie akceptacji kierownictwa dla proponowanych ryzyk szczątkowych;
i) uzyskanie autoryzacji kierownictwa do wdrażania i korzystania z SZBI;
j) przygotowanie deklaracji stosowania.

Oprócz dokumentów normatywnych regulujących kwestie zarządzania bezpieczeństwem informacji istnieją również różnego rodzaju opracowania, które proponują odpowiednio dobrane wytyczne dla obiektów krytycznych, m.in. elektrowni jądrowych. Przykładem mogą być wytyczne MAEA (Międzynarodowej Agencji Energii Atomowej) [86] dotyczące bezpieczeństwa komputerów (*computer security*). W obiektach energetyki jądrowej *bezpieczeństwo komputerów* definiuje się jako *część bezpieczeństwa informacji.* Zaznacza się, że termin „komputery" lub „system komputerowy" obejmuje sprzęt z oprogramowaniem do wykonywania obliczeń, komunikacji, a także oprzyrządowanie i urządzenia sterujące w obiekcie jądrowym. W wytycznych MAEA *bezpieczeństwo informacji* (*information security*) zdefiniowano krócej niż w normie ISO/IEC 27001 [95], to jest jako *utrzymywanie poufności, integralności i dostępności informacji.* Zaznaczono jednak, że definicja ta może uwzględniać również inne właściwości systemu, jak podaje się w normach.

Przeciwdziałanie (*countermeasure*) jest działaniem podjętym przeciw zagrożeniu (*threat*), w celu jego wyeliminowania lub zmniejszenia *podatności* (*vulnerabilities*) syste-

mu. Podatność (*vulnerability*) wiąże się z możliwością narażenia i osłabienia szeroko rozumianych aktywów, w tym oprogramowania do sterowania i zabezpieczenia, co może być wykorzystane przez uaktywnione zagrożenie (*threat*). Zagrożenie (*threat*) stanowi potencjalną przyczynę niechcianego incydentu, który może spowodować szkodę (*harm*) w systemie lub organizacji. Warto podkreślić, że w publikacjach MAEA zagrożenie (*threat*) jest zwykle definiowane jako osoba lub grupa osób z motywacją, intencją i zdolnością popełnienia nieprzyjaznego działania.

Ryzyko (*risk*) w wytycznych MAEA definiuje się jako potencjał, że określone zagrożenie wykorzysta podatność (*vulnerability*) określonych aktywów lub zbioru aktywów, co doprowadzi do szkody w organizacji. Miarą ryzyka jest kombinacja prawdopodobieństwa zdarzenia i krytyczności jego konsekwencji.

Jak można zauważyć, miara ryzyka w wytycznych MAEA została zdefiniowana podobnie jak w normie bezpieczeństwa funkcjonalnego PN-EN 61508, chociaż dotyczy innego rodzaju zagrożeń, to jest działań nieprzyjaznych o charakterze intencyjnym lub ataków, których zamiarem jest spowodowanie zdarzenia awaryjnego o możliwie dużych konsekwencjach, ze stratami ludzkimi, środowiskowymi, materialnymi i ekonomicznymi. Ryzyko tych strat można redukować, zmniejszając prawdopodobieństwo działań intencyjnych i ataków (w rozważanym czasie, np. w okresie rocznym) oraz zmniejszając podatność systemu na te działania i ataki, np. przez wzmacnianie pierścieni zabezpieczeniowo-ochronnych.

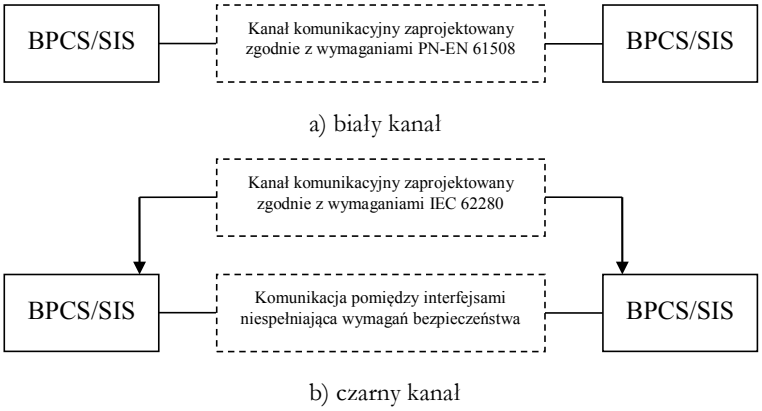
Przykładem innego interesującego podejścia w określaniu wymagań dla rozwiązań informatycznych pełniących odpowiedzialne funkcje monitorowania i sterowania jest propozycja amerykańska [43]. Wskazuje się na nią w wytycznych MAEA [86]. W szczegółowych analizach dotyczących bezpieczeństwa informacji można uwzględniać modele ochrony informacji zestawione w pracach [32, 127, 128].

W niniejszej monografii dokonano przeglądu rozwiązań bezpieczeństwa w sieciach komputerowych typu LAN i WAN (przewodowych i bezprzewodowych) z uwzględnieniem problematyki ochrony informacji. Biorąc pod uwagę fakt, że w złożonych obiektach technicznych wykorzystywane są różnego rodzaju sieci, w tym sieci korporacyjne, inaczej zwane sieciami administracyjnymi, oraz sieci typowo przemysłowe, należy uzmysłowić sobie pewne zagrożenia, jakie niesie ze sobą ich wspólne funkcjonowanie. Oczywiście zadania, jakie stawia się obu rodzajom sieci, są diametralnie różne, zarówno pod względem funkcjonalnym, jak i infrastrukturalnym. Dodatkowo, każda z tych sieci może być zbudowana przy wykorzystaniu innych rozwiązań technicznych i strukturalnych, co dodatkowo komplikuje ewentualne dalsze analizy tych systemów. Coraz częściej spotykane rozwiązania z komunikacją zdalną, bezprzewodową dają realne oszczędności instalacyjne, natomiast wprowadzają do systemu nowe zagrożenia, o czym należy pamiętać.

Biorąc pod uwagę przegląd istniejących rozwiązań sieciowych, zaproponowano klasyfikację występujących w obiektach przemysłowych stref sieciowych na cztery główne architektury rozproszonych systemów technicznych oraz sklasyfikowano rodzaje zagrożeń, jakie mogą występować w takich konfiguracjach sieciowych. Następnie poprzez prezentację przykładowych rozwiązań niezawodności i bezpieczeństwa transmisji danych stosowanych w sieciach komunikacyjnych rozproszonych systemów automatyki sformułowano wymagania stawiane kanałom komunikacyjnym.

W normie PN-EN 61508 zawarto uwagi dotyczące kanałów komunikacji (rys. 2.3). Wyróżniono tu dwie architektury do transmisji danych w ramach realizowanej funkcji związanej z bezpieczeństwem, zawierające: a) biały kanał i b) czarny kanał. W przypadku a) kanał komunikacji powinien spełniać wymagania normy PN-EN 61508, natomiast

w przypadku b) przyjmuje się, że interfejsy spełniają wymagania normy IEC 62280 [88]. Uwzględnienie kanałów komunikacji cyfrowej, szczególnie w sieci komputerowej o złożonej topologii, jest nowym wyzwaniem w analizie i ocenie bezpieczeństwa funkcjonalnego.



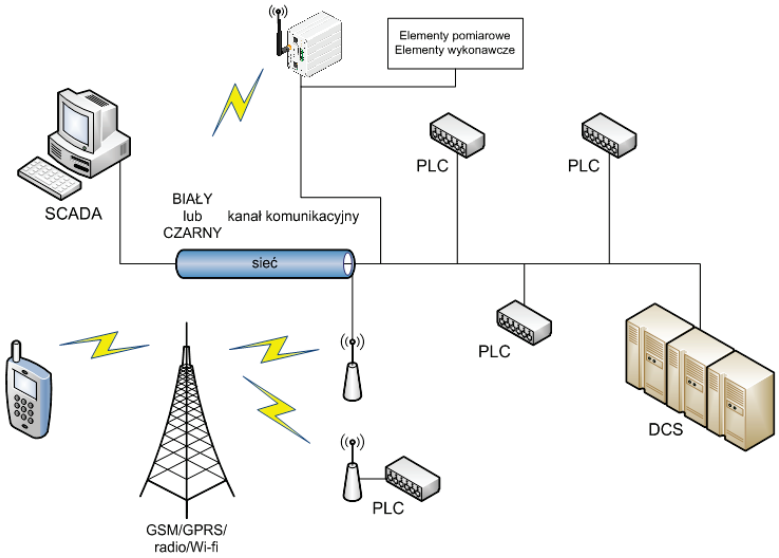
Rys. 2.3. Kanały do transmisji danych w systemach E/E/PE (BPCS lub SIS) (PN-EN 61508)

Przy projektowaniu rozproszonych skomputeryzowanych systemów sterowania, zabezpieczeń, ochrony i monitorowania muszą zostać uwzględnione wszystkie potencjalne zagrożenia wynikające z zastosowania różnych kanałów transmisji danych. W rozproszonych systemach sterowania i automatyki zabezpieczeniowej nie można nie uwzględnić wpływu sieci komputerowej na poziom nienaruszalności bezpieczeństwa SIL. Kanał komunikacyjny pomiędzy dwoma sterownikami należy traktować jako blok sprzętowy z przypisanym mu poziomem SIL, który trzeba określić na podstawie analizy ryzyka, a następnie zweryfikować i ustalić architekturę sieci, która spełni postawione wymagania. Można tego dokonać, stosując metody jakościowe lub ilościowe. Metody ilościowe są bardziej wiarygodne, jeśli dysponuje się zestawem danych niezawodnościowych dotyczących poszczególnych elementów składowych. Przy braku danych niezawodnościowych można stosować podejście jakościowe, które ma jedynie charakter szacunkowy.

W przypadku przemysłowej sieci komputerowej bardzo ważnymi wymaganiami są również zapewnienie odpowiednio wysokiej niezawodności przesyłania danych, skuteczne wykrywanie błędów transmisji oraz możliwość szybkiej lokalizacji potencjalnych uszkodzeń. W celu spełnienia powyższych wymagań przy projektowaniu elementów sieci stosuje się wiele specyficznych rozwiązań na poziomie zarówno sprzętu, jak i oprogramowania.

Jeśli zatem weźmie się pod uwagę aspekt techniczny funkcjonowania obiektów wykorzystujących rozproszone systemy sterowania, jakość oraz bezpieczeństwo przesyłu danych/ informacji mają kluczowe znaczenie dla ich poprawnego działania, a co za tym idzie – realizacji zadań, jakie im wyznaczono. Obiekt techniczny może się składać z różnego rodzaju systemów, wpływających bezpośrednio na jego działanie. Najczęściej jako główne systemy tego typu wymienia się systemy sterowania, monitorowania oraz zabezpieczeń, które wykorzystują w swojej pracy wszelkiego rodzaju kanały przesyłu danych, wykonane w różnych technikach: przewodowych i bezprzewodowych. Przesył danych analogowych, a w szczególności cyfrowych na większe odległości nie stanowi już w dzisiejszych czasach bariery technologicznej, dlatego coraz częściej wykorzystuje się strukturę rozproszonego systemu sterowania i monitorowania, tzw. DCS. Rozwiązanie to pozwala na ograniczenie kosztów budowy systemu i jednocześnie zwiększa jego elastyczność działania. Niesie jed-

nak ze sobą nowe wyzwania i problemy, związane m.in. z zapewnieniem niezawodnego i bezpiecznego przesyłu danych pomiędzy elementami takiego systemu. Ideowy przykład systemu rozproszonego zaprezentowano na rys. 2.4.



Rys. 2.4. Przykład rozproszonego systemu sterowania wykorzystującego różne rozwiązania komunikacyjne

Na rys. 2.5 przedstawiono przykładowy sterownik programowalny PLC, mający zastosowanie w warstwie sterowania, którego interfejs komunikacyjny należy zakwalifikować do czarnego kanału komunikacyjnego.

Rys. 2.5. Sterownik PLC PCD3 WAC z wbudowanym serwerem web i kilkoma alternatywnymi możliwościami transferu danych: Ethernet przemysłowy, Internet, GSM/GPRS (PLC + IT + Web)

Sterownik PCD3 WAC pozwala na wymianę danych z innymi sterownikami oraz modułami rozproszonymi przy wykorzystaniu sieci Internet bezpośrednio bądź przez zastosowanie technologii VPN w Intranecie. Możliwa jest również jednoczesna komunikacja z tymi urządzeniami poprzez wykorzystanie technologii bezprzewodowej GSM/GPRS. W obydwu przypadkach przedstawiony system wykorzystuje zewnętrzne kanały transmisji danych (Internet oraz GSM/GPRS); może on stanowić część większego systemu, który według klasyfikacji zaproponowanej w podrozdziale 6.5.1 (s. 123) będzie się zaliczał do II lub III kategorii.

W tego typu systemach duży nacisk należy położyć na zagadnienie ochrony informacji, które w szerokim rozumieniu dotyczy:
— *poufności danych/ informacji*, czyli zapewnienia dostępu do zasobów tylko autoryzowanym jednostkom;
— *integralności danych/ informacji*, czyli zapewnienia poprawności i kompletności przetwarzanych i gromadzonych danych;
— *dostępności danych/ informacji*, czyli zapewnienia dostępu do zasobów, zawsze gdy zajdzie taka potrzeba.

Mając na uwadze powyższe definicje, można wywnioskować, że zagadnienie ochrony informacji oraz jej analiza i ocena bardzo dobrze oddają w tym przypadku istotę prawidłowego funkcjonowania rozproszonego systemu sterowania, monitorowania i zabezpieczeń.

Zarówno dla bezpieczeństwa funkcjonalnego, jak i ochrony informacji kluczowe staje się rozpatrzenie zagrożeń, które mogą występować w analizowanych systemach technicznych. Identyfikacji zagrożeń można dokonać przy użyciu jednej spośród kilku dostępnych i opisanych w literaturze metod (np. C-Hazop – od *cyber HAZOP*). We wszystkich przypadkach otrzyma się wynikową listę zagrożeń, na które narażony jest obiekt techniczny i które niosą ze sobą zbyt duży poziom ryzyka dla ludzi, środowiska oraz mienia – poziom, który trzeba będzie zredukować przynajmniej do wartości tolerowanej, wykorzystując różne rozwiązania techniczne i organizacyjne.

Proces analizy zagrożeń pozwala zatem na uzyskanie odpowiedzi na wiele interesujących pytań, dotyczących funkcjonowania (bezpiecznego) obiektu, systemu technicznego infrastruktury krytycznej:
— jakie zagrożenia, z punktu widzenia bezpieczeństwa funkcjonalnego oraz ochrony informacji, mogą wystąpić w systemie (bądź występują, w przypadku systemu już działającego);
— jakie są przyczyny powstania tych zagrożeń (rozpatruje się tutaj najczęściej poszczególne scenariusze awaryjne);
— jakie jest prawdopodobieństwo wystąpienia tych zagrożeń (lub ich częstość występowania);
— jakie konsekwencje wiążą się z wystąpieniem poszczególnych zagrożeń;
— jakie środki zaradcze zostały już zastosowane/ zaprojektowane;
— jakie środki zaradcze muszą zostać uwzględnione.

Do identyfikacji i oceny zagrożeń w systemach technicznych można wykorzystać m.in. takie metody, jak [51, 73, 126, 135, 139]:
— przegląd cech bezpieczeństwa SR (*safety review*);
— analiza list kontrolnych CA (*checklist analysis*);
— klasyfikacja względna RR (*relative ranking*);
— wstępna analiza zagrożeń PHA (*preliminary hazard analysis*);
— analiza „co-jeżeli” (*what-if analysis*);
— analiza zagrożeń i zdolności działania HAZOP (*hazard and operability study*);
— analiza rodzajów i skutków uszkodzeń FMEA (*failure modes and effects analysis*) lub analiza rodzajów, skutków i krytyczności uszkodzeń FMECA (*failure modes, effects & criticality analysis*);
— analiza drzewa uszkodzeń FTA (*fault tree analysis*);
— analiza drzewa zdarzeń ETA (*event tree analysis*);
— analiza przyczyn i skutków CCA (*cause-consequence analysis*);

— analiza niezawodności człowieka HRA (*human reliability analysis*);
— identyfikacja zagrożeń HAZID (*hazard identification*).

Przy określaniu stopnia ochrony informacji skupiono się na wykorzystaniu metody HAZOP. Domyślnie została ona stworzona do oceny systemów procesowych chemicznych, jednak jej zalety dostrzeżono również w innych branżach przemysłu i zaczęto ją stosować zarówno w innych złożonych systemach, jak i – w nieco zmodyfikowanej wersji – w analizie oprogramowania komputerowego. Metoda ta polega na ocenie poszczególnych elementów analizowanego systemu dokonywanej przez grupę ekspertów przy użyciu pewnych wytycznych i słów kluczowych. Jest to metoda zespołowa, którą można wykorzystać na każdym etapie życia systemu, zalecane jest jednak, aby zostałą zastosowana najwcześniej, jak to możliwe, tak by miała wpływ na późniejszy projekt końcowy systemu. Dzięki temu możliwe są systematyczna i w pełni udokumentowana ocena oraz wykrycie potencjalnych zagrożeń występujących w analizowanym systemie. Poprawne wykonanie analizy HAZOP wymaga posiadania szczegółowego schematu technologicznego rozważanego systemu, jak również bardzo dokładnej wiedzy o zachodzących w nim procesach. W przypadku braku takich informacji (najczęściej w pierwszej fazie projektowania systemu) można się posłużyć analizą HAZID (*hazard identification*), która także pozwala na zgrubną ocenę zagrożeń występujących bądź mogących wystąpić w systemie i nie wymaga dysponowania aż tak szczegółowymi danymi.

Analiza HAZOP może być przeprowadzona w różnych fazach życia systemu, a mianowicie [87]:
— w fazie wstępnego projektu systemu;
— gdy dostępne są końcowe diagramy instalacji i połączeń elementów systemu (*piping and instrumentation diagrams*, P&ID);
— podczas budowy i instalacji systemu w celu upewnienia się, czy spełnione zostały wszystkie założenia projektowe;
— podczas uruchamiania systemu;
— w fazie działania systemu, w celu upewnienia się, czy procedury awaryjne oraz operacyjne są przeprowadzane i modyfikowane zgodnie z wytycznymi zawartymi w projekcie.

W przypadku procesu określania wymagań dotyczących nienaruszalności bezpieczeństwa wzięto pod uwagę metody grafów ryzyka oraz analizy warstw zabezpieczeń (*layers of protection analysis*, LOPA). Przeanalizowano możliwość dostosowania ich do zintegrowanej analizy bezpieczeństwa funkcjonalnego oraz ochrony informacji, biorąc pod uwagę ich charakter: jakościowy, półilościowy lub ilościowy.

Najczęściej wykorzystywaną metodą jakościową jest graf ryzyka. Metoda ta bazuje na pewnej liczbie parametrów ryzyka, opisujących charakter sytuacji niebezpiecznej, mogącej spowodować poważne skutki dla zdrowia i życia jednostki ludzkiej lub grupy ludzi, dla środowiska lub mogącej wywołać poważne straty finansowe przy niezadziałaniu lub nieistnieniu systemu zabezpieczającego. Parametry te posiadają zdefiniowane zbiory przedziałów (czynników) opisujące ich wartości jakościowe. Dzięki wykorzystaniu tych parametrów można dokonać oceny oraz stopniowania ryzyka. Wyszczególniono cztery parametry ryzyka, które są wystarczająco ogólne, aby mogły być wykorzystane w szerokim spektrum zastosowań. Z kolei kalibrowany graf ryzyka został przedstawiony w dokumencie PN-EN 61511 jako próba dostosowania metody grafu ryzyka do potrzeb przemysłu procesowego. Jest to metoda typu półjakościowego, tzn. graf ryzyka jest częściowo kalibrowany jakościowo. Założono, że w grafie tym będą wykorzystywane te same parametry ryzyka co

w metodzie przedstawionej w dokumencie PN-EN 61508, z tym że zmodyfikowano ich opis i znaczenie.

Poszczególnym poziomom SIL projektowanego systemu E/E/PE odpowiadają ilościowe kryteria probabilistyczne. W analizie bezpieczeństwa funkcjonalnego kluczowe znaczenie ma określenie poziomu nienaruszalności bezpieczeństwa SIL dla obiektu (instalacji) podwyższonego ryzyka, a następnie zaprojektowanie takiego systemu zabezpieczeniowego, który spełni te wymagania. Dowód spełnienia przez system zabezpieczeniowy wymagań dotyczących określonego poziomu SIL nazywa się weryfikacją.

Model probabilistyczny dowolnego systemu sterowania lub zabezpieczeń można przedstawić za pomocą schematów blokowych niezawodności RBD (*reliability block diagram*), grafów Markowa, równań uproszczonych oraz drzew niezdatności FTA (*fault tree analysis*). W sytuacji, gdy system rozpatrywany jest z punktu widzenia jego uszkadzalności, wygodnym podejściem jest skorzystanie z metody cięć minimalnych. W przypadku weryfikacji SIL pogłębionych badań wymaga problematyka integrowania koncepcji bezpieczeństwa funkcjonalnego z ochroną (*security*) rozproszonych i skomputeryzowanych systemów sterowania i automatyki zabezpieczeniowej przed możliwymi nieprzyjaznymi działaniami z zewnątrz poprzez sieć lokalną i/lub zewnętrzną.

W modelowaniu probabilistycznym rozproszonych systemów sterowania DCS lub automatyki zabezpieczeniowej SIS należy uwzględnić infrastrukturę przemysłowej sieci komputerowej w modelach probabilistycznych tych systemów. Budując taki model, można wykorzystać technikę ścieżek lub cięć minimalnych. Po uwzględnieniu struktury fizycznej sieci komputerowej w rozproszonym systemie sterowania BPCS lub zabezpieczeń SIS można obliczyć prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa.

W przypadku weryfikacji SIL powstaje zasadnicze pytanie, czy uwzględnienie zagadnienia ochrony informacji musi się odbywać poprzez integrację SIL i EAL, czy też w inny sposób, np. przy przeprowadzaniu dla każdego prototypowego rozproszonego systemu E/E/PE (BPCS lub SIS) szczegółowej analizy rodzajów, skutków i krytyczności uszkodzeń FMECA (*failure mode effect and criticality analysis*). Umożliwia ona zbadanie wpływu infrastruktury sieciowej na brak realizacji funkcji bezpieczeństwa.

Przy weryfikacji SIL zaproponowano dwa podejścia do uwzględnienia zagadnień ochrony informacji. Pierwsze podejście bazuje na tablicy porównawczej poziomów SIL i EAL. Drugie rozwiązanie uwzględnia także znaczenie zagadnień niepewności, analizy wrażliwości modelu probabilistycznego oraz wykorzystania wskaźników różnicowych w modelu regułowym uwzględniającym wpływ stopnia ochrony informacji (np. EAL) na weryfikowany poziom SIL.

Innym rozwiązaniem integrowania zagadnień bezpieczeństwa funkcjonalnego z zagadnieniami ochrony informacji jest opracowana przez SINTEF metodyka SeSa (*SecureSafety*). Została ona opracowana z myślą o systemach sterowania i automatyki zabezpieczeniowej stosowanych w przemyśle wydobywczym na morskich platformach wiertniczych, monitorowanych i zarządzanych zdalnie z lądu, poprzez ogólnie dostępne środki komunikacyjne. Podejście to wykorzystuje uwzględnienie pierścieni zabezpieczeniowo-ochronnych w przemysłowych sieciach komputerowych ze szczególnym zwróceniem uwagi na programowalne systemy sterowania i zabezpieczeń.

2.2. Kryteria probabilistyczne dla wyróżnionych rodzajów pracy systemów E/E/PE

W analizie bezpieczeństwa funkcjonalnego uwzględnia się dwa rodzaje pracy systemu E/E/PE w odniesieniu do częstości jego przywołań do działania i zasad okresowego przeprowadzania testów sprawności funkcjonalnej [161]:

— *rodzaj pracy na rzadkie przywołanie*, gdy częstość przywołań do działania systemu związanego z bezpieczeństwem nie przekracza jednego na rok lub nie przekracza dwukrotnej częstości testów okresowych;

— *rodzaj pracy na częste przywołanie lub ciągły*, gdy częstość przywołań do działania systemu związanego z bezpieczeństwem jest większa od jednego na rok lub większa niż dwukrotna częstość testów okresowych.

Klasyfikacja ta ma istotne znaczenie w modelowaniu probabilistycznym systemu w odniesieniu do przedstawionych poniżej kryteriów probabilistycznych.

W normie PN-EN 61508 *nienaruszalność bezpieczeństwa* definiuje się jako prawdopodobieństwo, że system związany z bezpieczeństwem wykona właściwie wymagane funkcje bezpieczeństwa w określonych warunkach i w określonym przedziale czasu. Ważne znaczenie praktyczne ma poziom nienaruszalności bezpieczeństwa SIL, traktowany jako poziom dyskretny (jeden z czterech możliwych) do wyszczególnienia wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które mają być alokowane w systemach E/E/PE związanych z bezpieczeństwem. Poszczególnym poziomom nienaruszalności bezpieczeństwa SIL projektowanego systemu E/E/PE odpowiadają ilościowe kryteria probabilistyczne, które zestawiono w tablicy 2.1.

Tablica 2.1

Poziomy nienaruszalności bezpieczeństwa i kryteria probabilistyczne dla systemów związanych z bezpieczeństwem [161]

Poziom nienaruszalności bezpieczeństwa SIL	Przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie PFD_{avg} (rodzaj pracy na rzadkie przywołanie do działania)	Średnia częstość występowania uszkodzenia niebezpiecznego na godzinę *PFH* (rodzaj pracy na częste przywoływanie do działania lub ciągłej)
4	$[10^{-5}, 10^{-4})$	$[10^{-9}, 10^{-8})$
3	$[10^{-4}, 10^{-3})$	$[10^{-8}, 10^{-7})$
2	$[10^{-3}, 10^{-2})$	$[10^{-7}, 10^{-6})$
1	$[10^{-2}, 10^{-1})$	$[-10^{-6}, 10^{-5})$

Uzyskanie poziomu nienaruszalności bezpieczeństwa SIL3 dla rodzaju pracy rzadkiego przywołania do działania może się okazać niemożliwe bez zastosowania nadmiarowości strukturalnej w systemie E/E/PE. Do spełnienia wymagań dotyczących SIL3, a zwłaszcza SIL4, niezbędne jest zwykle zastosowanie rozbudowanych struktur nadmiarowych i stanowi to zazwyczaj duże wyzwanie projektowe i techniczne z powodu konieczności eliminowania potencjalnych uszkodzeń zależnych w podsystemach nadmiarowych, a niekiedy nawet problem organizacyjny podczas użytkowania systemu (przeprowadzanie testów

funkcjonalności podsystemów z uwzględnieniem danych statystycznych przebiegu użytkowania systemu i zaistniałych uszkodzeń).

2.3. Wybrane aspekty zarządzania bezpieczeństwem w obiektach i systemach infrastruktury krytycznej

Problematyka niezawodności i bezpieczeństwa złożonych obiektów podwyższonego ryzyka znajduje się ostatnio w centrum uwagi nie tylko projektantów, inwestorów, organów dozoru technicznego, kadry technicznej i operatorów tych obiektów, ale również – po wystąpieniu licznych katastrof transportowych i awarii obiektów przemysłowych – społeczności lokalnych i polityków. Dla specjalistów zainteresowanych tą problematyką staje się oczywiste, że niezbędne jest opracowanie i możliwie niezwłoczne wdrożenie w różnych sektorach krajowego przemysłu i w transporcie nowych, bardziej skutecznych systemów zarządzania bezpieczeństwem.

W związku z istotną rolą, jaką w złożonych obiektach i instalacjach technicznych zaczynają odgrywać programowalne systemy monitorowania, sterowania i automatyki zabezpieczeniowej, szczególne znaczenie w praktyce eksploatacji instalacji i obiektów podwyższonego ryzyka ma zarządzanie bezpieczeństwem funkcjonalnym [109, 113, 115, 116, 136]. Systemy sterowania i automatyki zabezpieczeniowej są coraz częściej postrzegane jako środki do zmniejszenia ryzyka związanego z możliwymi w każdym systemie technicznym zdarzeniami awaryjnymi, a następnie utrzymywania tego ryzyka na odpowiednio niskim poziomie w procesie eksploatacji [114]. Powinny one oczywiście spełniać określone wymagania i kryteria, w tym te zawarte w normach bezpieczeństwa funkcjonalnego – zarówno międzynarodowych, jak i ich krajowych odpowiednikach [93, 157–159].

Doświadczenia eksploatacyjne obiektów różnych kategorii i instalacji podwyższonego ryzyka dobitnie wskazują, że występują w nich stany nienormalne i awaryjne oraz zdarzenia zagrażające, które mogą spowodować poważne straty ludzkie, środowiskowe, majątkowe i ekonomiczne [111, 113]. Zdarzenia takie mogą wystąpić z powodu poważnych zakłóceń zarówno w obrębie obiektu, jak i jego otoczenia, w tym w obiektach i instalacjach współpracujących. Mogą być one powodowane zawodnością wyposażenia technicznego, niekorzystnym wpływem środowiska przyrodniczego, błędami człowieka, a więc mają związek z zastosowaną technologią i obiektywnie występującymi zagrożeniami, których nie można całkowicie wyeliminować [90, 114].

Wyróżnia się czynniki wpływające na bezpieczeństwo w sensie *safety* i w sensie *security*, kiedy to zdarzenia zagrażające i ich skutki są powodowane nieprzyjaznymi działaniami intencyjnymi. Tego typu zdarzenia zagrażające mogą być spowodowane działaniami takimi jak sabotaż lub atak terrorystyczny. Ocena możliwości wystąpienia takich sytuacji ma szczególne znaczenie w obiektach i systemach tzw. infrastruktury krytycznej, która powinna zapewnić ciągłość realizacji ważniejszych funkcji państwa i gospodarki [116, 122, 208]. Do takich obiektów i systemów zalicza się m.in. obiekty i sieci energetyki i elektroenergetyki, rafinerie, zakłady chemiczne, elektrownie, sieci komputerowe, telekomunikację itd. [208]. We wszystkich tych obiektach, sieciach i systemach zaleca się stosować szerzej programowalne systemy monitorowania, sterowania i zabezpieczeń [113, 166].

Wspomniane nieprzyjazne działania intencyjne mogą być zainicjowane wewnątrz obiektu lub z zewnątrz. Obejmują one ataki hakerskie na zbiory danych gromadzone w systemach komputerowych w przemyśle dla celów zarządzania procesem produkcji i eksploatacji wyposażenia oraz szeroko rozumianego zarządzania bezpieczeństwem. Mogą

być one skierowane na rozproszone systemy monitorowania i sterowania typu DCS, zwłaszcza na warstwę funkcjonalną SCADA, a także na programowalne systemy sterowania i zabezpieczeń, projektowane i użytkowane zgodnie z wymaganiami bezpieczeństwa funkcjonalnego [56–58, 122, 156, 173, 205].

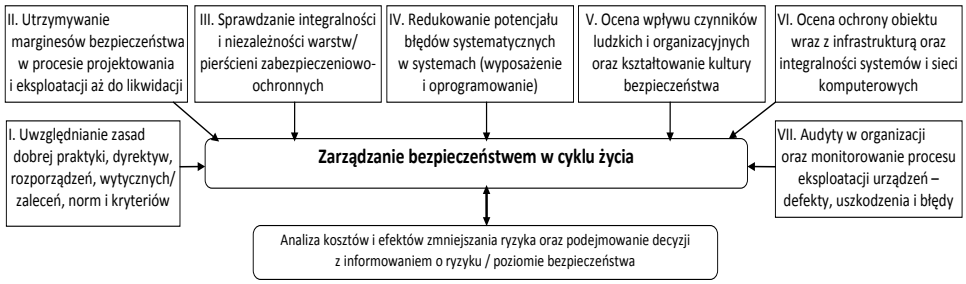
Ostatnio wiele uwagi poświęca się problemom związanym z atakami na rozproszone przemysłowe sieci i systemy komputerowe w zakresie możliwego rozprzestrzeniania się złośliwego oprogramowania. Zagadnienia ochrony systemów programowalnych z uwzględnieniem aspektów *security* są obecnie w fazie intensywnych badań [29, 32, 58, 62, 86, 110, 116, 127, 128] i powstają normy techniczne dotyczące tych zagadnień [89, 94, 95, 163–165].

Istotnym zagadnieniem w systemach technicznych podwyższonego ryzyka jest potencjalny wpływ czynników ludzkich [27, 53, 80, 81, 102, 103], przy czym korzysta się z prac badawczych i raportów dotyczących energetyki jądrowej i przemysłu procesowego [61, 62, 177, 178, 186, 194, 211]. Zwraca się ostatnio uwagę na potrzebę szerszego uwzględniania tych czynników w całościowych rozwiązaniach bezpieczeństwa funkcjonalnego [33, 61, 105, 107, 123, 132, 210] oraz projektowania interfejsów człowiek–maszyna w systemach interaktywnych, również w kontekście projektowania systemu alarmowego [2, 47, 48, 91, 129, 154, 167, 168, 191].

Zarządzanie bezpieczeństwem funkcjonalnym bazuje na ocenach ryzyka przeprowadzanych w cyklu życia w odniesieniu do wymagań i kryteriów zawartych w normie o charakterze ogólnym PN-EN 61508 [161] i normach sektorowych, np. normy sektorowej opracowanej dla przemysłu procesowego PN-EN 61511 [162]. Jeśli nie opracowano jeszcze normy dla danego sektora przemysłowego, podstawę zarządzania bezpieczeństwem funkcjonalnym stanowi norma o charakterze ogólnym PN-EN 61508.

Najbardziej skutecznym sposobem przeciwdziałania poważnym awariom przemysłowym byłoby wyeliminowanie zagrożeń, a ponieważ jest to zwykle niewykonalne, podstawowe znaczenie ma ograniczenie częstości zdarzeń inicjujących i ryzyka zdarzeń zagrażających, szczególnie tych powodujących znaczne straty ludzkie, środowiskowe oraz materialne, a szerzej ekonomiczne. Interesujące są wyniki analiz poważnych awarii odnotowanych w Unii Europejskiej (UE). Okazało się, że główną przyczyną większości z nich były niedociągnięcia w zarządzaniu i/lub niedociągnięcia organizacyjne; niespójność systemu zarządzania przyczyniła się do powstania aż ponad 85% awarii. Skalę problemu uzmysławia fakt, że w ostatnim dwudziestopięcioleciu w państwach UE doszło do niemal tysiąca poważnych awarii [133, 134].

Szczególną uwagę należy zwrócić na wnioski wynikające z wcześniejszych incydentów i awarii, zarówno wewnątrz, jak i na zewnątrz danej organizacji, jak również z doświadczeń eksploatacyjnych danej instalacji lub podobnych oraz z wcześniejszych inspekcji i audytów bezpieczeństwa [38, 45, 62]. Kluczowe zagadnienia do uwzględnienia w zarządzaniu bezpieczeństwem obiektów technicznych/ instalacji przemysłowych/ zakładów podwyższonego ryzyka przedstawiono na rys. 2.6.



Rys. 2.6. Całościowe zarządzanie bezpieczeństwem obiektów podwyższonego ryzyka (w tym infrastruktury krytycznej) w cyklu życia [16, 107]

Na powyższym rysunku wyróżniono następujące grupy zagadnień:

— uwzględnianie zasad dobrej praktyki, dyrektyw, rozporządzeń, wytycznych/ zaleceń, norm i kryteriów;
— utrzymywanie marginesów bezpieczeństwa w procesie projektowania i eksploatacji aż do likwidacji;
— sprawdzanie integralności i niezależności warstw/ pierścieni zabezpieczeniowo-ochronnych;
— redukowanie potencjału błędów systematycznych w systemach (wyposażenie i oprogramowanie);
— ocena wpływu czynników ludzkich i organizacyjnych oraz kształtowanie kultury bezpieczeństwa;
— ocena ochrony obiektu wraz z infrastrukturą oraz integralności systemów i sieci komputerowych;
— audyty w organizacji oraz monitorowanie procesu eksploatacji urządzeń – defekty, uszkodzenia i błędy.

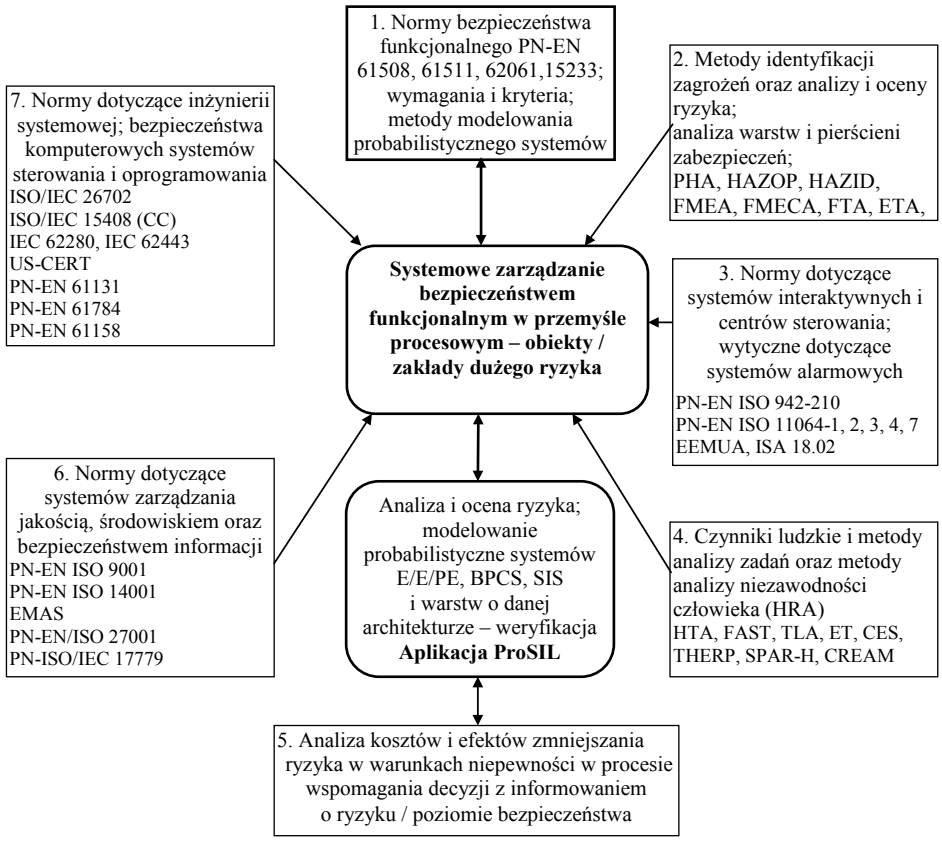
Zalecenia metodyczne dotyczące tych zagadnień opisano bardziej szczegółowo w pracach [41–43, 84, 107, 113, 115, 122, 145–149, 207]. Podczas podejmowania decyzji o przyjęciu określonych rozwiązań istotne znaczenie w praktyce przemysłowej ma analiza kosztów i efektów zmniejszania ryzyka w nawiązaniu do zasady ALARP i/lub LCC [107, 114, 206]; decyzje powinny być też podejmowane z informowaniem o ryzyku/ poziomie bezpieczeństwa [16, 60, 82, 85, 141].

Zaleca się, aby w procesie zarządzania bezpieczeństwem przeprowadzać analizę kosztów i efektów zmniejszania ryzyka, a przy podejmowaniu ostatecznych decyzji projektowych lub modernizacyjnych dotyczących systemu sterowania i zabezpieczeń informować o poziomach ryzyka/ bezpieczeństwa, jakie zostały osiągnięte [16, 107, 114–116, 197]. Aby zarządzanie bezpieczeństwem w obiektach przemysłowych – w szczególności bezpieczeństwem funkcjonalnym – było skuteczne, zaleca się, aby miało ono charakter systemowy [16, 114].

2.4. Systemowe zarządzanie bezpieczeństwem funkcjonalnym w przemyśle procesowym

Elementy składowe systemowego podejścia do zarządzania bezpieczeństwem funkcjonalnym w systemach technicznych, ze szczególnym uwzględnieniem przemysłu proce-

sowego, głównie zakładów dużego ryzyka (ZDR) i zakładów zwiększonego ryzyka (ZZR), przedstawiono na rys. 2.7 [107, 118].



Rys. 2.7. Propozycja systemowego zarządzania bezpieczeństwem funkcjonalnym w obiektach przemysłowych podwyższonego ryzyka (na podstawie [107, 118])

Trzon tego algorytmu stanowią bloki znajdujące się w środkowej części rysunku od góry do dołu, które dotyczą:

— norm bezpieczeństwa funkcjonalnego (blok 1) wraz z odpowiednimi wymaganiami i kryteriami oraz propozycjami metodycznymi dotyczącymi wyznaczania poziomów nienaruszalności bezpieczeństwa SIL i ich weryfikacji przy wykorzystaniu metod modelowania probabilistycznego systemów i warstw zabezpieczeniowo-ochronnych;
— metod analizy i oceny ryzyka oraz modelowania probabilistycznego systemów E/E/PE, BPCS i SIS oraz warstw zabezpieczeniowo-ochronnych o rozważanych na etapie projektu architekturach; możliwe jest analizowanie tych systemów przy wykorzystaniu prototypowej aplikacji komputerowej ProSIL lub jej wersji ProSIL-EAL rozszerzonej o aspekty związane z ochroną informacji;
— metodyki analizy kosztów i efektów zmniejszania ryzyka w warunkach niepewności w procesie wspomagania decyzji z informowaniem o ryzyku/ poziomie bezpieczeństwa (blok 5).

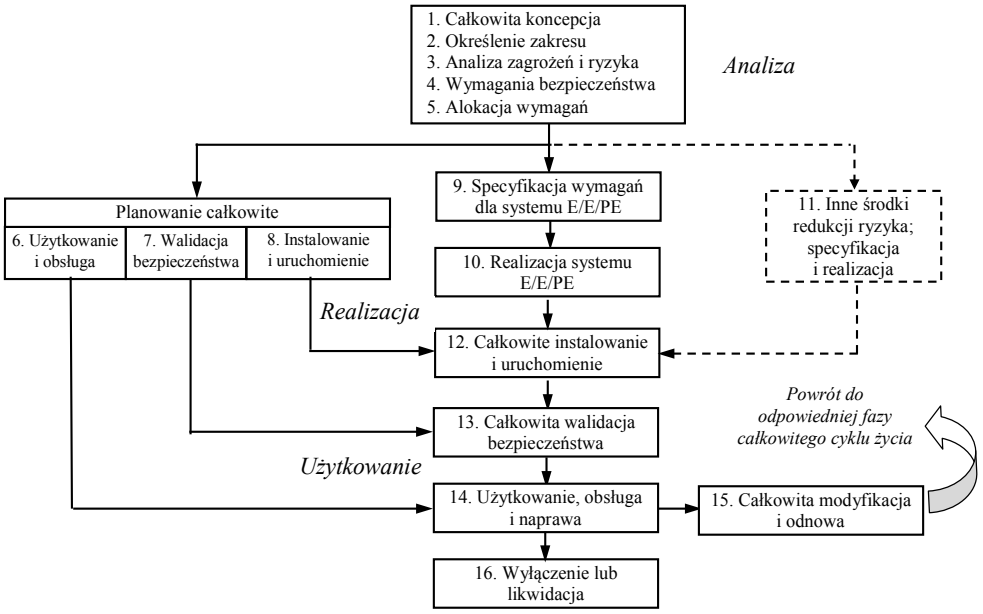
Warto zaznaczyć, że modele probabilistyczne przedstawione w normie PN-EN 61508 mają pewne ograniczenia dotyczące architektur systemów, jakie mogą być modelowane. W związku z tym zaproponowano modele uwalniające od tych ograniczeń. Bazują one na wyznaczonych zbiorach cięć minimalnych podsystemów systemu E/E/PE lub SIS [197].

2.5. Normy bezpieczeństwa funkcjonalnego

Norma PN-EN 61508 obejmuje zagadnienia, które należy rozpatrzyć, gdy systemy elektryczne/ elektroniczne/ programowalne elektroniczne (E/E/PE) są stosowane do wypełniania funkcji bezpieczeństwa. Ma ona zastosowanie do systemów związanych z bezpieczeństwem, gdy jeden lub kilka z tych systemów zawiera rozwiązania w postaci układów E/E/PE.

Norma PN-EN 61508 [161] jest normą o charakterze ogólnym i może być stosowana do wszystkich systemów E/E/PE związanych z bezpieczeństwem, niezależnie od zastosowania. Obejmuje ona możliwe zagrożenia spowodowane przez uszkodzenie funkcji bezpieczeństwa, które są realizowane przez systemy E/E/PE. Norma ta dotyczy tych systemów E/E/PE związanych z bezpieczeństwem, których uszkodzenie może mieć wpływ na bezpieczeństwo osób i/lub środowiska. Jest oczywiste, że skutki zdarzeń awaryjnych mogą spowodować utratę majątku, a szerzej mogą mieć również poważne konsekwencje ekonomiczne dla zakładu z powodu zaprzestania produkcji.

W celu usystematyzowania postępowania przy czynnościach koniecznych do osiągnięcia wymaganego poziomu nienaruszalności bezpieczeństwa systemów E/E/PE związanych z bezpieczeństwem w normie PN-EN 61508 [161] przyjęto cykl całkowity życia bezpieczeństwa zgodnie ze schematem przedstawionym na rys. 2.8.



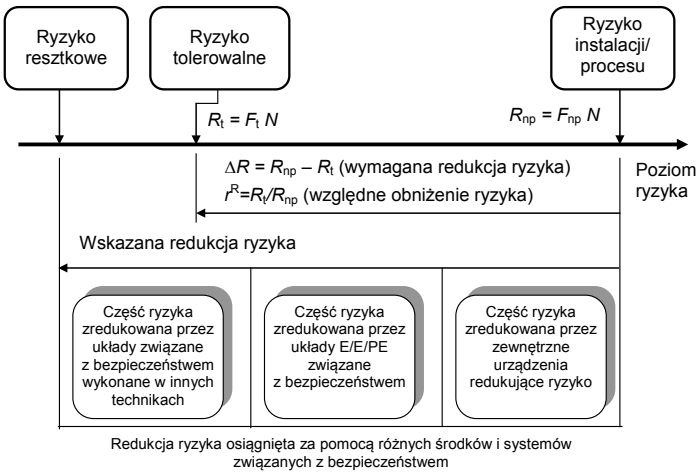
Rys. 2.8. Cykl całkowity życia bezpieczeństwa wg PN-EN 61508 [161]

Głównym celem zarządzania bezpieczeństwem funkcjonalnym jest wyszczególnienie czynności technicznych w kolejnych fazach cyklu życia bezpieczeństwa całkowitego, systemu E/E/PE i oprogramowania, koniecznych do osiągnięcia wymaganego bezpieczeństwa funkcjonalnego systemów E/E/PE związanych z bezpieczeństwem. Ponadto ważnym celem jest wyszczególnienie zakresu obowiązków osób, działów i organizacji odpowiedzialnych za każdą fazę cyklu życia bezpieczeństwa całkowitego, systemu E/E/PE i oprogramowania. Podjęte procedury organizacyjne powinny umożliwić skuteczne wdrożenie wymagań technicznych; do ich głównych zadań należą osiągnięcie i utrzymanie bezpieczeństwa funkcjonalnego systemów E/E/PE. Wymagania techniczne konieczne do utrzymania bezpieczeństwa funkcjonalnego są zwykle zamieszczone jako część informacji dostarczanych przez dostawcę systemu E/E/PE związanego z bezpieczeństwem [161].

Zaleca się, aby cykl całkowity życia bezpieczeństwa był podstawą do wykazania zgodności z tą normą, zezwala się jednak na użycie cyklu całkowitego życia bezpieczeństwa odmiennego od przedstawionego na rysunku, ale zapewniającego utrzymanie zgodności z celami i wymaganiami kolejnych rozdziałów normy PN-EN 61508 [161].

Wymagania dotyczące zarządzania bezpieczeństwem funkcjonalnym powinny być formułowane równolegle do faz cyklu całkowitego życia bezpieczeństwa. O ile nie uzasadniono inaczej, każda faza cyklu całkowitego życia bezpieczeństwa powinna zostać wprowadzona. W omawianej normie opisuje się szczegółowo poszczególne fazy cyklu życia z podaniem informacji wejściowej, odniesień do określonych części normy z opisem wymaganego zakresu działania oraz informacji wyjściowej [136, 161].

Zastosowanie określonego rozwiązania bezpieczeństwa funkcjonalnego (programowalnego systemu zabezpieczeń) E/E/PE lub SIS z zaimplementowanymi funkcjami bezpieczeństw ma na celu zmniejszanie ryzyka (rys. 2.9) od poziomu R_{np} (np – *no protection*), to jest bez zastosowania programowalnych zabezpieczeń w obiekcie podwyższonego ryzyka, do poziomu tolerowanego R_t. Wyróżniono dwie miary zmniejszenia ryzyka: bezwzględne ΔR i względne r^R. Na osi ryzyka wskazano również ryzyko resztkowe, to jest takie, jakie nadal występuje, mimo zastosowania środków zabezpieczeniowych [114].



Rys. 2.9. Sposoby zmniejszania ryzyka w obiekcie podwyższonego ryzyka [114, 117, 161]

Przy założeniu, że redukcję ryzyka do poziomu tolerowanego można osiągnąć dzięki zastosowaniu funkcji bezpieczeństwa realizowanej za pomocą systemu zabezpieczeniowe-

go E/E/PE lub SIS, zakładając pesymistycznie ten sam poziom strat $N = const$, otrzymuje się zależność na względne zmniejszenie poziomu ryzyka w postaci:

$$r^{\mathrm{R}} = R_{\mathrm{t}} / R_{\mathrm{np}} = F_{\mathrm{t}} / F_{\mathrm{np}} = r^{\mathrm{F}} \tag{2.1}$$

gdzie: R_{np} – ryzyko bez zastosowania systemu zabezpieczeniowego E/E/PE lub SIS; F_{np} – częstość zdarzenia awaryjnego bez uwzględnienia tego systemu; R_{t} – ryzyko tolerowane; F_{t} – częstość zdarzenia awaryjnego zredukowana do poziomu ryzyka tolerowanego R_{t} po wprowadzeniu środka zabezpieczeniowego; r^{F} – względna redukcja częstości rozważanego scenariusza awaryjnego.

Jeśli redukcja ryzyka ma być realizowana przez system E/E/PE lub SIS, wówczas ze wzoru (2.1) wynika zależność na przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa dla rodzaju rzadkiego przywołania do działania PFD_{avg} [114]:

$$PFD_{\mathrm{avg}} = r^{\mathrm{F}} = F_{\mathrm{t}} \Big/ F_{\mathrm{np}} \tag{2.2}$$

W normie PN-EN 61508 [161] wyróżniono dwie kategorie podsystemów: typu A i typu B. Podsystem można przyporządkować do kategorii A, jeśli spełnione są następujące warunki:

(a) jego wszystkie rodzaje uszkodzeń są dobrze zdefiniowane;
(b) jego zachowanie w danych warunkach można w pełni określić oraz
(c) dostępne są wystarczające dane empiryczne, na podstawie których można oszacować intensywność uszkodzeń niebezpiecznych wykrywalnych i niewykrywalnych.

Jeśli dany podsystem nie spełnia tych wymagań, musi być traktowany jako podsystem kategorii B. Sposób uwzględnienia w analizie ograniczeń architektonicznych dla podsystemów i najwyższe poziomy SIL, jakie można przypisać funkcji bezpieczeństwa realizowanej przez podsystemy typu A oraz typu B, zestawiono na podstawie PN-EN 61508 w tablicy 2.2 [107, 113, 161].

Tablica 2.2

Ograniczenia architektoniczne dla podsystemów i najwyższe poziomy SIL, jakie można przypisać funkcji bezpieczeństwa realizowanej przez podsystemy typu A i typu B [161]

Udział uszkodzeń bezpiecznych S_{FF}	Tolerancja sprzętu na defekty N		
	0	1	2
<60%	SIL1 (niedozwolone)	SIL2 (SIL1)	SIL3 (SIL2)
od 60% do <90%	SIL2 (SIL1)	SIL3 (SIL2)	SIL4 (SIL3)
od 90% do <99%	SIL3 (SIL2)	SIL4 (SIL3)	SIL4 (SIL4)
≥99%	SIL3 (SIL3)	SIL4 (SIL4)	SIL4 (SIL4)
Tolerowane uszkodzenie sprzętu N oznacza, że $N + 1$ uszkodzeń spowoduje utratę funkcji bezpieczeństwa.			

Jak widać, ograniczenia te zależą istotnie od udziału uszkodzeń bezpiecznych S_{FF}. Poziom SIL, jaki można przypisać funkcji bezpieczeństwa realizowanej przez podsystemy

typu B, jest mniejszy lub równy niż w przypadku podsystemów typu A. Wynika to z większej złożoności podsystemów typu B oraz mniejszego zaufania do nich, ponieważ zawierają one moduły programowalne, w których mogą wystąpić m.in. błędy systematyczne.

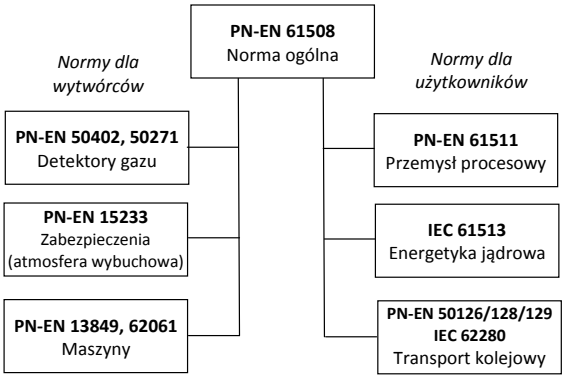
W tablicy 2.2 występuje parametr S_{FF} definiowany jako udział intensywności uszkodzeń bezpiecznych S (*safe*) i intensywności uszkodzeń niebezpiecznych wykrywalnych DD (*danger detected*) w całkowitej intensywności uszkodzeń (bezpiecznych i niebezpiecznych) w rozpatrywanym podsystemie, który wyznacza się następująco:

$$S_{FF} = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \tag{2.3}$$

gdzie: λ_S – sumaryczna intensywność uszkodzeń bezpiecznych (*safe*) [h^{-1}]; λ_{DD} – intensywność uszkodzeń niebezpiecznych wykrywalnych (*danger detected*) [h^{-1}]; λ_{DU} – sumaryczna intensywność uszkodzeń niebezpiecznych niewykrywalnych (danger undetected) [h^{-1}].

W tablicy 2.2 wyróżnia się cztery przedziały procentowych wartości S_{FF}, co jest wspólną cechą wszystkich sektorowych norm bezpieczeństwa funkcjonalnego. Największym zaufaniem obdarza się oczywiście rozwiązania, dla których wartość $S_{FF} \geq 99\%$.

Na rys. 2.10 przedstawiono relacje ogólnej normy bezpieczeństwa funkcjonalnego z wybranymi normami sektorowymi. Uwzględnione na tym rysunku normy sektorowe dotyczą programowalnych systemów sterowania i/lub systemów zabezpieczeń. W poszczególnych blokach podano skrótowo obszar ich zastosowań [114, 176].



Rys. 2.10. Relacje ogólnej normy bezpieczeństwa funkcjonalnego z wybranymi normami sektorowymi

Wyzwaniem jest zaprojektowanie systemu E/E/PE lub jego odpowiedników zdefiniowanych w normach sektorowych w taki sposób, aby zapobiec potencjalnym uszkodzeniom niebezpiecznym lub skutecznie je kontrolować, jeśli się pojawią [161]. Istnieje wiele przyczyn potencjalnych defektów, błędów i uszkodzeń w systemach E/E/PE, które mogą wynikać z [114]:

1. niekompletnej lub miejscami niedopracowanej specyfikacji dotyczącej systemów E/E/PE, sprzętu lub oprogramowania;
2. pominięcia w specyfikacji wymagań bezpieczeństwa (np. błąd w określeniu wszystkich niezbędnych funkcji bezpieczeństwa podczas różnych rodzajów pracy);
3. różnych mechanizmów przypadkowych uszkodzeń sprzętu, nie w pełni rozpoznanych;

4. różnorodnych mechanizmów systematycznych uszkodzeń sprzętu;
5. błędów systematycznych w oprogramowaniu i niepełnego przetestowania programów;
6. grupowych uszkodzeń zależnych od wspólnej przyczyny CCF (*common cause failures*);
7. błędów szeroko rozumianego człowieka-operatora, niekompletnych procedur i błędów popełnianych w organizacji z powodu nie w pełni ukształtowanej kultury bezpieczeństwa;
8. niekorzystnego wpływu środowiska (zjawiska elektromagnetyczne, zmienne temperatury, wibracje itp.);
9. znacznych zakłóceń w układach zasilania elektrycznego (np. utrata zasilania, zbytnio obniżone napięcie lub wielokrotne jego zaniki z ponownym załączaniem zasilania);
10. braku właściwej ochrony informacji w sieci komputerowej, której podsystemy pełnią funkcje związane z bezpieczeństwem.

Norma PN-EN 61508 zawiera usystematyzowane wymagania w celu minimalizowania wpływu potencjalnych defektów, błędów i uszkodzeń wyposażenia. Nie zostały w niej jednak uwzględnione niektóre istotne kwestie, szczególnie zagadnienia 7–10 spośród wymienionych powyżej. Zaleca się ujęcie tych zagadnień w analizach i ocenach rozwiązań bezpieczeństwa funkcjonalnego. Mogą być one również przydatne w analizie i ocenie bezpieczeństwa funkcjonalnego według norm (rys. 2.10): PN-EN 61511 [162], PN-EN 62061 [166], PN-EN 15233 [157] i PN-EN 50402 [158]. Propozycje i zalecenia dotyczące innych spośród wymienionych wyżej aspektów bezpieczeństwa funkcjonalnego zostały zawarte w monografiach [107, 113, 114].

2.6. Niezawodność i bezpieczeństwo obiektów technicznych

Parametrami modelu probabilistycznego systemu, np. jego *nieuszkadzalności* lub *niegotowości*, są m.in. funkcje intensywności uszkodzeń różnych kategorii elementów lub podsystemów, które pozyskuje się w praktyce z różnych źródeł danych niezawodnościowych.

W wyznaczaniu funkcji intensywności uszkodzeń określonych kategorii elementów (podsystemów) wskazane jest korzystanie z danych statystycznych dotyczących przebiegu eksploatacji i uszkodzeń obiektów identycznych lub podobnych, eksploatowanych przez dłuższy czas w zbliżonych warunkach środowiskowych. Nie jest to jednak możliwe w przypadku obiektów nowo projektowanych i w początkowej fazie ich eksploatacji. Wówczas korzysta się z dostępnych baz danych niezawodnościowych o charakterze ogólnym, dokonując odpowiedniej korekty funkcji intensywności uszkodzeń dla przewidywanych warunków środowiskowych.

W przypadku niektórych kategorii obiektów lub podsystemów uzasadnione jest założenie o stałej w czasie funkcji intensywności uszkodzeń $\lambda(t) = \lambda = const$, co znacznie ułatwia modelowanie probabilistyczne systemu. Założenie to jest uzasadnione zwłaszcza w przypadkach niewystępowania procesów zużycia i starzenia materiałów. Również inne parametry modelu probabilistycznego podsystemów i systemu – jak np.: intensywność odnowy, pokrycie diagnostyczne czy też czas pomiędzy przeprowadzaniem testów sprawności funkcjonalnej elementów wyposażenia – wyznacza się często, ze względu na brak danych z przebiegu eksploatacji, korzystając z różnych źródeł danych. W oszacowaniach tych parametrów uwzględnia się często opinie ekspertów [114, 176].

Zarządzanie bezpieczeństwem opiera się na analizie i ocenie ryzyka. Analiza ryzyka obejmuje wyznaczenie miary prawdopodobieństwa lub częstości rozważanych scenariuszy awaryjnych. Kolejnemu zdefiniowanemu scenariuszowi awaryjnemu przypisuje się określone straty, które szacuje się na podstawie odpowiednich metod modelowania procesów (tzw. modelowanie deterministyczne procesów fizycznych i/lub chemicznych), przy czym często korzysta się również z opinii ekspertów. Rzetelność tych opinii wpływa zwykle w istotny sposób na założenia dotyczące modelu ryzyka i jego parametrów, a zatem jego wiarygodność i przydatność uzyskanych wyników w podejmowaniu decyzji.

Każdy współczesny złożony obiekt techniczny wyposaża się w systemy sterowania i zabezpieczeń, które wpływają istotnie na niezawodność i bezpieczeństwo całego systemu. Zarządzanie bezpieczeństwem złożonego obiektu lub instalacji przeprowadza się w cyklu życia. Decyzje natury technicznej, organizacyjnej i ekonomicznej w cyklu życia danego obiektu złożonego podejmuje się na podstawie uzyskanych oszacowań ryzyka oraz analizy kosztów i efektów rozważanych opcji sterowania ryzykiem [12, 111, 113].

Problematyka niezawodności i bezpieczeństwa ma coraz większe znaczenie w eksploatacji systemów technicznych. Zagadnienia te ujmują niektóre dyrektywy europejskie i krajowe akty prawne w postaci ustaw i rozporządzeń w kontekście wymagań dotyczących szeroko rozumianej jakości (projekt, wyrób, usługa itd.), ochrony środowiska przyrodniczego i bezpieczeństwa (pracy, systemu, działalności gospodarczej, informacji itd.) [37, 44–46]. W coraz większej liczbie przedsiębiorstw wprowadza się zintegrowane systemy zarządzania jakością, środowiskiem i bezpieczeństwem. W takim szerokim ujęciu należy również spojrzeć na system zarządzania procesem eksploatacji w przedsiębiorstwie, który powinien obejmować ocenę ryzyka i diagnostykę techniczną oraz analizę i kształtowanie niezawodności [96, 167].

W normach technicznych dotyczących zagadnień niezawodności i bezpieczeństwa formułuje się m.in. kryteria probabilistyczne, jakie powinny spełniać proponowane rozwiązania. Do takich norm można zaliczyć normy bezpieczeństwa funkcjonalnego PN-EN 61508 oraz normy sektorowe, np. opracowane dla przemysłu procesowego, lub normy dotyczące bezpieczeństwa funkcjonalnego maszyn w nawiązaniu do wymagań dyrektywy maszynowej [161].

W większości sytuacji odpowiedni poziom bezpieczeństwa uzyskuje się za pomocą pewnej liczby systemów zabezpieczeń, które wykorzystują różne techniki (np. mechaniczną, hydrauliczną, pneumatyczną, elektryczną, elektroniczną, programowalną elektroniczną). Dlatego też każda strategia bezpieczeństwa oparta na zarządzaniu ryzykiem musi rozpatrywać nie tylko elementy wchodzące w skład danego systemu (np. czujniki, urządzenia sterujące i urządzenia wykonawcze), lecz także inne systemy związane z bezpieczeństwem, tworzące całościowy zestaw systemów wiążących się z bezpieczeństwem [6, 79, 170].

Nieuszkadzalność (*reliability*) definiuje się jako zdolność obiektu do wypełnienia wymaganych funkcji w danych warunkach i w określonym przedziale czasu. Natomiast gotowość, dyspozycyjność (*availability*) to zdolność obiektu do utrzymywania się w stanie umożliwiającym wypełnianie wymaganych funkcji w danych warunkach i określonej chwili lub w rozważanym przedziale czasu, przy założeniu, że zapewniono odpowiednie warunki zewnętrzne (zdolność ta zależy łącznie od nieuszkadzalności, obsługiwalności i zapewnienia środków obsługi obiektu) [6, 79, 170].

Nieuszkadzalność jest zdolnością obiektu (wyrobu) do wypełnienia wymaganych funkcji w danych warunkach (zadany poziom maksymalnych obciążeń i narażeń w określonych warunkach środowiskowych) w danym przedziale czasu. Miarę tej zdolności wyraża się liczbowo, np. jako prawdopodobieństwo poprawnego wypełniania wymaganej funk-

cji $P(t)$ w rozważanym przedziale czasu [0, t]. Prawdopodobieństwo to jest funkcją czasu i przy założeniu, że obiekt jest nienaprawialny w tym umownym przedziale czasu, wyraża się za pomocą wzoru [79, 111, 113]:

$$R(t) = \exp[-\int_0^t \lambda(\tau) d\tau] \tag{2.4}$$

gdzie: $\lambda(t)$ – funkcja intensywności uszkodzeń, definiowana jako częstość uszkodzeń obiektów w przedziale czasu Δt od chwili t, przy warunku, że obiekt był sprawny do chwili t:

$$\lambda(t) = \lim_{\Delta t \to 0} \frac{P\{t < T \le t + \Delta t \mid T > t\}}{\Delta t} \tag{2.5}$$

gdzie: T – zmienna losowa trwałości typu ciągłego, określająca czas przebywania obiektu w stanie zdatności funkcjonalnej.

W badaniach niezawodności duże znaczenie ma rozkład Weibulla zmiennej losowej T. Funkcję intensywności uszkodzeń dla takiego rozkładu określa wzór [6, 79, 111, 113, 175]:

$$\lambda(t) = (\nu / b)\,(t / b)^{\nu - 1} \tag{2.6}$$

gdzie: b – współczynnik skali, wyrażany w jednostkach czasu, np. w godz.; ν – bezwymiarowy współczynnik kształtu.

Dla współczynnika kształtu o wartości $\nu = 1$ funkcja intensywności uszkodzeń jest stała w czasie $\lambda(t) = \lambda = const$, identycznie jak w przypadku rozkładu wykładniczego. Rozkład wykładniczy stanowi więc szczególny przypadek rozkładu Weibulla. Rozkład wykładniczy ma duże znaczenie w analizie niezawodności, zwłaszcza w przypadku elementów elektronicznych i elektrycznych, w których nie występują procesy zużycia. Jeśli będą występować w nich od pewnego czasu procesy starzenia materiałów, wówczas wskazane jest zastosowanie w analizie trwałości innych rozkładów probabilistycznych [79, 111].

Jeżeli oszacowania parametru intensywności uszkodzeń dla rozkładu wykładniczego dokonuje się na podstawie badania losowej próbki obiektów pracujących w określonych warunkach środowiskowych, o liczności n, do chwili t_b, przed którą wystąpiło m-te uszkodzenie, wówczas, korzystając z metody największej wiarygodności, otrzymuje się następujące oszacowanie nieznanej wartości parametru λ_b^* [111, 175]:

$$\lambda_b^* = \frac{m}{Z(t_b)} \tag{2.7}$$

przy czym wartość $Z(t_b)$ określa wzór:

$$Z(t_b) = \sum_{i=1}^{m} t_{(i)} + (n - m) \cdot t_b \tag{2.8}$$

Wyznaczona w ten sposób wartość $Z(t_b)$ jest zaobserwowaną sumą czasów poprawnej pracy badanych obiektów w przedziale czasu [0, t_b]. W takim przypadku granice dwustronnego przedziału – dolną (dd) i górną (dg) – [λ_{dd}, λ_{dg}] na poziomie ufności β oblicza się z wzorów:

$$\lambda_{dd} = \frac{\chi^2_{2m,(1-\beta)/2}}{2 \cdot Z(t_b)} \tag{2.9}$$

$$\lambda_{\mathrm{dg}} = \frac{\chi^2_{2(m+1),\ (1+\beta)/2}}{2 \cdot Z(t_{\mathrm{b}})} \tag{2.10}$$

W licznikach wzorów (2.9) i (2.10) występują, odpowiednio, kwantyle $(1 - \beta)/2$ i $(1 + \beta)/2$ rozkładu chi-kwadrat przy stopniach swobody $2m$ i $2(m + 1)$.

Należy podkreślić, że zarysowane powyżej badania niezawodności dotyczą określonych warunków zewnętrznych (obciążenie, udary) i czynników środowiskowych (np. temperatura, wibracje, wilgotność). W praktyce analiz niezawodności nie dysponuje się wynikami badań niezawodności dla różnych warunków i posiadane wyniki (dotyczące danej kategorii elementów) trzeba dostosować do innych warunków zewnętrznych i środowiskowych. Korzysta się wówczas z zaawansowanych metod szacowania parametrów rozkładu probabilistycznego lub ich stosownej korekty z uwzględnieniem odpowiednich czynników. Są one opisane w poradnikach specjalistycznych i normach.

Opracowany model probabilistyczny obiektu należy uwiarygodniać w czasie, wykorzystując m.in. dane o przebiegu eksploatacji i zaistniałych uszkodzeniach w zbiorze obserwowanych obiektów danej kategorii. W tym celu stosuje się zwykle Beyesowskie metody uaktualniania modelu probabilistycznego lub metody agregowania informacji z różnych źródeł, bazując na oszacowaniach i opiniach ekspertów.

Miarę ryzyka długoterminowego dla danego systemu technicznego wyznacza się na podstawie zbioru trójek zawierających [111, 113, 114]: scenariusz (rozważany przypadek) zdarzenia awaryjnego, częstość lub prawdopodobieństwo tego zdarzenia oraz niekorzystny skutek (szkodę) po jego wystąpieniu [111, 114]:

$$\Re = \{< S_k, F_k, N_k >\} \tag{2.11}$$

gdzie: S_k – potencjalne zdarzenie awaryjne zdefiniowane dla k-tego scenariusza; F_k – częstość k-tego scenariusza (prawdopodobieństwo na jednostkę czasu, np. rok); N_k – niekorzystny skutek w wyniku wystąpienia k-tego scenariusza, czyli szkoda (strata) w określonym zakresie, np. liczba obrażeń i/lub zejść śmiertelnych, poziom strat majątkowych (ekonomicznych).

Ryzyko indywidualne związane z poszkodowaniem osoby znajdującej się w miejscu o współrzędnych (x, y) w wyniku poważnej awarii przemysłowej wyznacza się następująco:

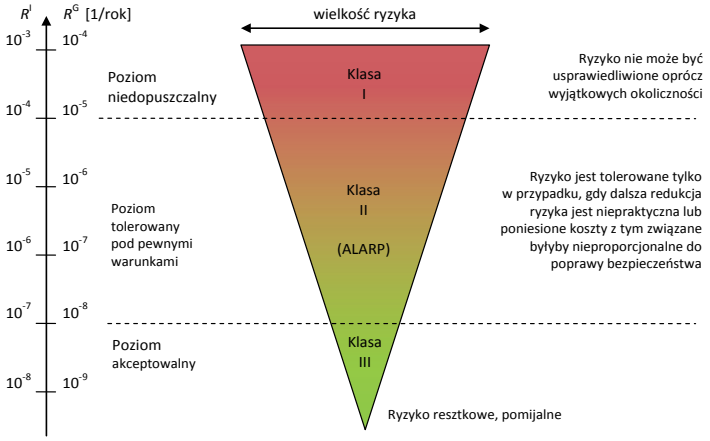
$$R^{\mathrm{I}}_{(x,y)} = \sum_k F_k \cdot P_{k(x,y)} \tag{2.12}$$

gdzie: F_k – częstość k-tego scenariusza awaryjnego szacowana w przedziale czasowym, zwykle rok [a]; $P_{k(x,y)}$ – prawdopodobieństwo warunkowe poszkodowania osoby w wyniku wystąpieniu k-tego scenariusza awaryjnego w miejscu o współrzędnych (x, y) na terenie instalacji technicznej lub w jej otoczeniu.

W literaturze proponuje się wartości (poziomy) kryterialne dozwolonego ryzyka indywidualnego o wielkości $10^{-4}\ a^{-1}$ i poniżej [111]. Zaleca się analizowanie możliwości zmniejszania tego ryzyka przy zastosowaniu zasady ALARP [161, 170, 206]. Jednym ze sposobów redukcji ryzyka indywidualnego w przemyśle jest zmniejszenie częstości scenariuszy awaryjnych F_k. Można to osiągnąć np. poprzez wprowadzanie nowoczesnych systemów zabezpieczeniowych, zgodnie z koncepcją bezpieczeństwa funkcjonalnego.

Zasadę analizy ALARP zilustrowano na rys. 2.11. Jeżeli poziom ryzyka w danej sytuacji należy do obszaru I (powyżej wartości $10^{-4}\ a^{-1}$), ryzyko musi być zmniejszone, aby eksploatacja obiektu złożonego była dozwolona. W przypadku występowania ryzyka

w obszarze II należy stosować zasadę ALARP. W obszarze ryzyka akceptowalnego (III) nie ma potrzeby stosowania tej zasady.



Rys. 2.11. Poziomy ryzyka i stosowalność zasady ALARP [107, 114]

Miarę ryzyka społecznego (grupowego) R związanego z potencjalnymi zdarzeniami awaryjnymi może stanowić oczekiwana strata, np. ekonomiczna, lub przeciętna śmiertelność w ciągu roku [111]:

$$R = \sum_k F_k \cdot N_k \tag{2.13}$$

gdzie: F_k – częstość k-tego scenariusza awaryjnego [a^{-1}]; N_k – prognozowana strata w wyniku k-tego scenariusza awaryjnego [jedn. straty].

Wyniki oszacowania ryzyka można przedstawić za pomocą matrycy ryzyka, w której wyróżniono kategorie strat i kategorie częstości potencjalnych zdarzeń awaryjnych (rys. 2.12).

N [j. strat] / F [a^{-1}]	N^A	N^B	N^C	N^D	N^E
F^0	*III*	*II*	*I*	*I*	*I*
F^{-1}	*III*	*III*	*II*	*I*	*I*
F^{-2}	*IV*	*III*	*III*	*II*	*I*
F^{-3}	*IV*	*IV*	*III*	*III*	*II*
F^{-4}	*IV*	*IV*	*IV*	*III*	*III*

Rys. 2.12. Matryca ryzyka dla przykładowego obiektu złożonego na tle obszarów wyróżnionych klas ryzyka [31, 111, 113, 114]

Na rys. 2.12 wyróżniono cztery klasy ryzyka dla potencjalnych zdarzeń awaryjnych zdefiniowanych dla danego obiektu złożonego podwyższonego ryzyka:

I. ryzyko niedozwolone, którego nie można tolerować ze względu na dużą częstość zdarzeń awaryjnych i ich poważne skutki;

II. ryzyko niepożądane, które należy redukować zgodnie z zasadą ALARP;
III. ryzyko tolerowane, jeśli koszt jego redukcji jest nieproporcjonalnie duży względem spodziewanych efektów (nieznaczne zmniejszenie ryzyka przy dużych kosztach), w przeciwnym razie ryzyko należy zmniejszać;
IV. ryzyko akceptowalne.

Do kalibracji matrycy ryzyka przedstawionej na rys. 2.12 można wykorzystać dane zawarte w tablicach 2.3 oraz 2.4.

Tablica 2.3

Wyniki przykładowych kategorii częstości zdarzeń awaryjnych przyjętych do kalibrowania matrycy ryzyka [107, 111, 114]

Kategorie częstości zdarzenia	F^{-4}	F^{-3}	F^{-2}	F^{-1}	F^{0}
Określenie słowne kategorii częstości	rzadkie	mało prawdopodobne	sporadyczne	prawdopodobne	częste
Przedziały wartości [a^{-1}]	$(10^{-5}, 10^{-4}]$	$(10^{-4}, 10^{-3}]$	$(10^{-3}, 10^{-2}]$	$(10^{-2}, 10^{-1}]$	$(10^{-1}, 10^{0}]$

Tablica 2.4

Wyniki przykładowych kategorii skutków przyjętych do kalibrowania matrycy ryzyka [107, 111, 114]

Kategoria skutku zdarzenia	N^A	N^B	N^C	N^D	N^E
Określenie słowne kategorii skutku	marginalne	małe	duże	krytyczne	katastrofalne
Orientacyjna liczba poszkodowanych	pojedyncze obrażenia	kilka obrażeń	pojedyncze zejście	kilka zejść	wiele zejść

Przedstawioną na rys. 2.12 matrycę ryzyka należy zweryfikować i ewentualnie zmodyfikować podczas analizy ryzyka innego złożonego obiektu technicznego. W definiowaniu obszarów klas ryzyka należy uwzględnić wyniki badań dotyczące wypadkowości i awaryjności w różnych sektorach gospodarki oraz akceptowalności ryzyka w nawiązaniu do aktualnych wartości społecznych.

2.7. Bezpieczeństwo komputerowych systemów sterowania i oprogramowania

Propozycja wykorzystywania koncepcji inżynierii systemowej w projektowaniu i użytkowaniu systemów komputerowych jest zawarta w normie międzynarodowej ISO/IEC 26702 [94]. Norma ta proponuje ogólny proces inżynierii systemów SEP (*systems engineering process*). Jest ona spójna z normą bezpieczeństwa funkcjonalnego PN-EN

61508 [161], chociaż dotyczy w dużym stopniu zagadnień jakości produkcji, ale również bezpieczeństwa i ochrony komputerowych systemów monitorowania i sterowania.

Wieloczęściowa norma ISO/IEC 15408 definiuje kryteria określane mianem wspólnych kryteriów (*Common Criteria* – CC), które mogą być wykorzystywane jako podstawa do oceny właściwości zabezpieczeń produktów i systemów informatycznych. Dzięki ustanowieniu takiej wspólnej bazy kryteriów wyniki oceny zabezpieczeń informatycznych będą zrozumiałe dla szerszego grona odbiorców [93].

Wspólne kryteria (CC) pozwalają na porównywanie wyników niezależnie od dokonywanych ocen zabezpieczeń. Jest to możliwe dzięki udostępnieniu na potrzeby oceny zabezpieczeń wspólnego zbioru wymagań, odnoszących się do funkcji zabezpieczających produkty i systemy informatyczne. Ocena określa poziom zaufania, że funkcje zabezpieczające tych produktów i systemów oraz stosowane do nich środki uzasadnionego zaufania spełniają te wymagania. Wyniki oceny mogą pomóc odbiorcom stwierdzić, czy dany produkt lub system informatyczny jest wystarczająco bezpieczny dla zamierzonego zastosowania i czy ryzyko naruszenia zabezpieczeń wynikające z jego użycia jest dopuszczalne.

Wspólne kryteria są użyteczne jako poradnik przy konstruowaniu produktów lub systemów wyposażonych w informatyczne funkcje zabezpieczające oraz przy zamawianiu komercyjnych produktów i systemów z takimi funkcjami. Podczas oceny produkt lub system informatyczny nazywany jest przedmiotem oceny (*target of evaluation*, TOE). Przedmiotami TOE mogą być np. systemy operacyjne, sieci komputerowe, systemy rozproszone i aplikacje.

Wspólne kryteria mogą być stosowane do zabezpieczeń informatycznych zrealizowanych w sprzęcie, oprogramowaniu układowym (*firmware*) lub oprogramowaniu. W przypadku, gdy pewne aspekty oceny będą przeznaczone tylko dla wybranych metod implementacji, będzie to sygnalizowane w opisie odpowiednich kryteriów.

Poziom uzasadnionego zaufania (*evaluation assurance level*, EAL) rozumie się jako pakiet składający się z komponentów uzasadnionego zaufania, pochodzących z części 3 rozważanej normy [93], który reprezentuje punkt na zdefiniowanej przez CC skali uzasadnionego zaufania. Poziomy te zostały opisane poniżej i w materiałach szkoleniowych z propozycją ich zastosowania do oceny ochrony informacji w rozwiązaniach bezpieczeństwa funkcjonalnego.

EAL1 jest poziomem podstawowym i najtańszym w implementacji, potwierdzającym spełnienie podstawowych wymagań ochrony informacji. Poziom EAL7 jest najbardziej rygorystyczny, ale rozwiązania ochrony informacji są wówczas znacznie droższe w implementacji. Aby osiągnąć odpowiedni poziom uzasadnionego zaufania, należy spełnić określone wymagania. Większość z nich odnosi się do dokumentacji i analizy projektu informatycznego, testów funkcjonalności bądź też wnikliwych testów poprawnego działania. Im wyższy poziom EAL, tym bardziej szczegółowe powinny być dokumentacja, wszelkie analizy i testy.

Idea poziomów EAL jest w pewnym sensie zbliżona do idei poziomów nienaruszalności bezpieczeństwa SIL, które są stosowane w ocenie bezpieczeństwa funkcjonalnego. Produkty i systemy informatyczne według ISO/IEC 15408 są określane wspólnym mianem przedmiotów oceny TOE. Nazwa ta akcentuje fakt prowadzenia niezależnej oceny. Pozytywny wynik oceny pozwala uzyskać certyfikat poświadczający, że zabezpieczenia produktu lub systemu cechują się określonym poziomem uzasadnionego zaufania EAL. Deklarowanym przez konstruktorów poziomom uzasadnionego zaufania dla TOE odpowiadają specjalnie opracowane zbiory komponentów uzasadniających zaufanie, zwane pakietami uzasadnionego zaufania.

Znaczenie poziomów EAL, czyli miar uzasadnionego zaufania, jest interpretowane w następujący sposób:
— EAL1 – TOE był testowany funkcjonalnie;
— EAL2 – TOE był testowany strukturalnie;
— EAL3 – TOE był metodycznie sprawdzany i testowany;
— EAL4 – TOE był metodycznie projektowany, testowany i przeglądany;
— EAL5 – TOE był półformalnie projektowany i testowany;
— EAL6 – TOE został półformalnie zweryfikowany i przetestowany;
— EAL7 – projekt TOE został formalnie zweryfikowany i przetestowany.

W odniesieniu do normy PN-EN 15408 [93] określenie „nieformalny" jest rozumiane jako „wyrażony w języku naturalnym"; „półformalny" – jako „wyrażony w języku o ściśle zdefiniowanej składni i zdefiniowanej semantyce"; „formalny" – jako „wyrażony w języku o ściśle zdefiniowanej składni oraz semantyce, która jest oparta na solidnych podstawach matematycznych".

Uważa się, że produkty lub systemy informatyczne o wyższym poziomie EAL są obdarzane większym zaufaniem, jednak koszt ich opracowania i oceny znacząco rośnie, a zatem deklarując EAL, należy się kierować kompromisem między przewidywanym ryzykiem w środowisku operacyjnym a kosztem opracowania, wytworzenia oraz utrzymania produktu lub systemu informatycznego [28, 93]. Zaleca się zatem, aby poziomy EAL dostosowywać w rozwiązaniach bezpieczeństwa funkcjonalnego do poziomów nienaruszalności bezpieczeństwa SIL [118, 120]. Propozycję tę rozwinięto w dalszej części książki.

Innym podejściem w integracji bezpieczeństwa funkcjonalnego z ochroną informacji jest wykorzystanie w tym procesie poziomów uzasadnionej ochrony SAL. Komitet ISA 99 opracował dokumenty ISA 99/IEC 62443 [89, 91] z których każdy opisuje różne aspekty cyberbezpieczeństwa dla systemów sterowania i automatyki przemysłowej (*industrial automation control system*, IACS) (rys. 2.13). Zbiór dokumentów IEC 62443 obejmuje takie kwestie, jak: podstawowe aspekty bezpieczeństwa, program bezpieczeństwa wewnątrz przedsiębiorstwa, techniczne wymogi bezpieczeństwa w celu ochrony systemów w przedsiębiorstwie oraz wymogi bezpieczeństwa dla poszczególnych komponentów w systemie [89, 92].

Standard IEC 62443 wprowadza cztery poziomy uzasadnionej ochrony SAL, każdy z rosnącym poziomem bezpieczeństwa, podobnie jak w przypadku poziomów nienaruszalności bezpieczeństwa SIL. Każdy poziom SAL określa wymagania bezpieczeństwa dla danego systemu, który może być z nimi zgodny lub nie. Poniżej przedstawiono definicje odnoszące się do poszczególnych poziomów SAL [89]:
— **SAL1 – ochrona przed zamierzonym lub przypadkowym naruszeniem**. Zamierzone lub przypadkowe naruszenia cyberbezpieczeństwa są skutkiem uchybień w realizacji polityki bezpieczeństwa. Mogą one być spowodowane zarówno przez pracowników, jak i przez osoby z zewnątrz. Wiele spośród tych naruszeń będzie chronionych przez programy oraz egzekwowanie obowiązujących zasad i procedur.
— **SAL2 – ochrona przed celowym naruszeniem przy użyciu prostych środków**. Proste sposoby nie wymagają dużej wiedzy ze strony atakującego. Atakujący nie potrzebuje szczegółowej wiedzy dotyczącej bezpieczeństwa, domeny lub konkretnego atakowanego systemu. Wektory ataków są dobrze znane i mogą być zautomatyzowanymi narzędziami wspomagającymi atakującego. Mogą one również zaatakować wiele systemów zamiast jednego.

— **SAL3 – ochrona przed celowym naruszeniem z wykorzystaniem zaawansowanych, tzn. bardziej wyrafinowanych środków**. Wyrafinowane sposoby wymagają zaawansowanej wiedzy dotyczącej cyberbezpieczeństwa, domeny, systemu docelowego lub dowolnej ich kombinacji. Intruz będzie atakował układ o poziomie SAL3 prawdopodobnie przy użyciu wektorów ataków, które zostały dostosowane do konkretnego systemu docelowego. Atakujący może wykorzystać luki w systemach, które nie są dobrze znane. Słabym punktem są protokoły przemysłowe zawierające informacje na temat konkretnego celu, aby móc naruszyć bezpieczeństwo systemu lub innych środków, które wymagają większych umiejętności i wiedzy, niż jest to wymagane dla SAL1 lub 2.
— **SAL4 – ochrona przed celowym naruszeniem z wykorzystaniem zaawansowanych, tzn. bardziej wyrafinowanych środków i rozszerzonych zasobów**. Ataki na układy o poziomach SAL3 i SAL4 przebiegają niemal identycznie; w obu przypadkach łączy się wyrafinowane środki w celu naruszenia wymogów cyberbezpieczeństwa systemu. Różnicę stanowi napastnik, który w wypadku SAL4 ma do dyspozycji więcej środków, takich jak wysokiej wydajności zasoby obliczeniowe, duża liczba komputerów lub dłuższy czas.

Grupa dokumentów zawierająca ogólne informacje na temat ISA 99		**IEC 62443-1-1** Terminologia, założenia, modele	**IEC 62443-1-2** Pojęcia i skróty	**IEC 62443-1-3** Wskaźniki jakościowe systemu bezpieczeństwa
Grupa dokumentów zawierająca informacje na temat programu ochrony		**IEC 62443-2-1** Ustanowienie programu ochrony	**IEC 62443-2-2** Obsługa programu ochrony IACS	**IEC 62443-2-3** Doskonalenie programu ochrony środowiska IACS
Grupa dokumentów zawierająca informacje na temat technicznych aspektów dotyczących systemów	**IEC 62443-3-1** Technologie bezpieczeństwa	**IEC 62443-3-2** Poziomy SAL dla stref i kanałów komunikacji	**IEC 62443-3-3** Wymagania systemu bezpieczeństwa	**IEC 62443-3-4** Wymagania rozwoju produktów
Grupa dokumentów zawierająca informacje na temat technicznych aspektów dotyczących komponentów	**IEC 62443-4-1** Urządzenia wbudowane	**IEC 62443-4-2** Urządzenia hostujące	**IEC 62443-4-3** Urządzenia sieciowe	**IEC 62443-4-4** Aplikacje, dane i funkcje

Rys. 2.13. Dokumenty serii IEC 62443 [89]

2.8. Zintegrowane podejście w analizach bezpieczeństwa funkcjonalnego i ochrony informacji

Mając zdefiniowane kategorie systemów oraz struktury, w jakich te systemy pracują, można skupić uwagę na zasadniczym problemie, jakim jest integracja zagadnień i analiz bezpieczeństwa funkcjonalnego oraz ochrony informacji. Systemy sterowania oraz automatyki zabezpieczeniowej, tak jak opisano to we wcześniejszej części niniejszego rozdziału, działają z wykorzystaniem przewodowych bądź też bezprzewodowych kanałów komunikacji. W analizach bezpieczeństwa funkcjonalnego informacje te należy wziąć pod uwagę jako czynniki mogące mieć wpływ na określenie wymagań SIL oraz ich weryfikację. Z przeprowadzonej wstępnej analizy wiadomo, że bezpośrednie integrowanie zagadnień ochrony informacji w procesie określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL może nie być rozwiązaniem najbardziej efektywnym. Dlatego zaproponowana metoda integracji dwóch różnych zagadnień bazuje na innym rozwiązaniu, w którym wyniki analizy ochrony informacji przeprowadzonej dla obiektu infrastruktury krytycznej

mogą służyć jako jedne z czynników wpływających na określenie wymaganej redukcji ryzyka dla tego obiektu. Ma to następnie bezpośrednie przełożenie na określenie wymaganego poziomu SIL, czyli redukcji ryzyka związanego z działaniem takiego obiektu [14, 15, 18, 19]. W takim przypadku analiza bezpieczeństwa funkcjonalnego będzie niezaprzeczalnie odgrywała rolę nadrzędną.

W celu utrzymania ryzyka dla systemu na poziomie akceptowalnym/tolerowanym należy zdefiniować pewne wymagania dotyczące spełnienia przez system związany z bezpieczeństwem odpowiednich funkcji, czyli opisywanych już wcześniej funkcji bezpieczeństwa. Istnieją dwa typy wymagań, które są konieczne do osiągnięcia bezpieczeństwa funkcjonalnego:

- wymagania nienaruszalności bezpieczeństwa, czyli prawdopodobieństwo, że dana funkcja bezpieczeństwa zrealizuje się zgodnie z założonym celem;
- wymagania bezpieczeństwa, czyli jakie zadanie ma spełniać dana funkcja bezpieczeństwa.

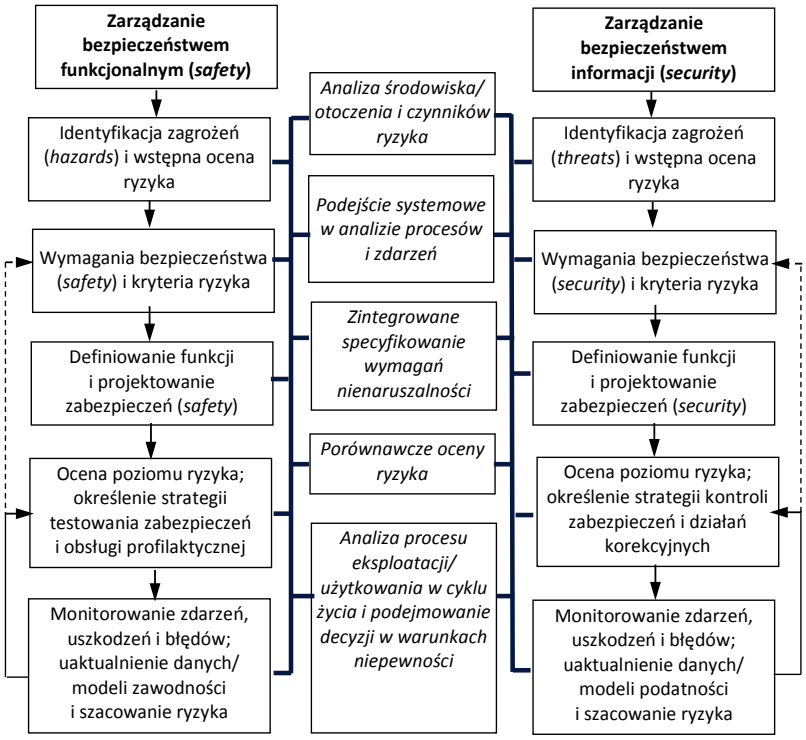
Po zdefiniowaniu funkcji bezpieczeństwa oraz przypisaniu im – każdej z osobna – wymagań nienaruszalności bezpieczeństwa należy opisać specyfikację wymagań funkcjonalnych dla funkcji bezpieczeństwa. Opisują one logikę działania systemu, który będzie realizował tę funkcję. W praktyce specyfikacja ta przybiera postać tabelarycznego bądź opisowego dokumentu lub też zbioru dokumentów, na podstawie których przebiega następnie etap projektowania struktury sprzętowej, która będzie realizować poszczególne funkcje bezpieczeństwa. Informacje na temat specyfikacji bezpieczeństwa są wykorzystywane także na etapie weryfikacji, czyli sprawdzenia, czy zaprojektowana struktura sprzętowa rzeczywiście spełnia wymagania nienaruszalności bezpieczeństwa. Wymagania nienaruszalności funkcji bezpieczeństwa określa się w trakcie oceny ryzyka w taki sposób, aby uzyskać redukcję ryzyka do poziomu akceptowalnego/ tolerowanego. Wymagania dla funkcji bezpieczeństwa są określane za pomocą analizy zagrożeń, czyli oceny, co należy zrobić, aby uniknąć zdarzenia niebezpiecznego. Po ich połączeniu z wymaganiami nienaruszalności bezpieczeństwa otrzymuje się całkowitą specyfikację bezpieczeństwa dla zbioru zdefiniowanych funkcji bezpieczeństwa.

Podstawowa koncepcja analizy związanej z określaniem wymaganego poziomu SIL przedstawia się następująco:

- zidentyfikowanie potencjalnych zagrożeń;
- określenie scenariuszy awaryjnych;
- zdefiniowanie funkcji bezpieczeństwa;
- zdefiniowanie tolerowanego poziomu ryzyka dla analizowanego systemu;
- ustalenie aktualnego poziomu ryzyka dla zdefiniowanych funkcji bezpieczeństwa;
- ustalenie wymaganego poziomu redukcji ryzyka (na podstawie oceny ryzyka);
- wyrażenie wymaganego poziomu redukcji ryzyka za pomocą poziomów nienaruszalności bezpieczeństwa SIL.

Od poprawnego przeprowadzenia wymienionych czynności zależy właściwe, czyli poprawne określenie poziomu SIL, a co za tym idzie – dobranie właściwej architektury systemu zabezpieczeniowego. Główną miarą określającą pewność rozwiązań zastosowanych przy implementacji funkcji bezpieczeństwa jest oczywiście poziom nienaruszalności bezpieczeństwa SIL. Dostępne metody określania tego poziomu oraz sposobność skorzystania z rozwiązań jakościowych, półilościowych oraz ilościowych dają dość elastyczne możliwości analizy problemów o różnych stopniach złożoności.

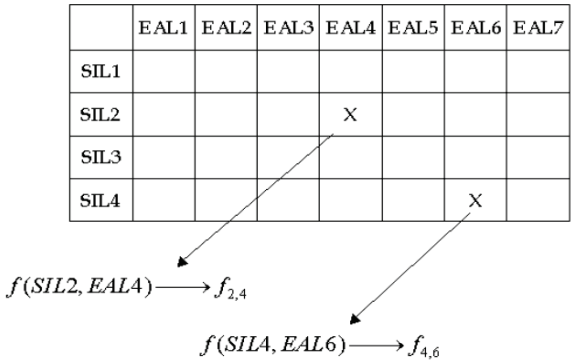
Zarys zintegrowanego podejścia w zarządzaniu bezpieczeństwem funkcjonalnym i bezpieczeństwem informacji w programowalnych systemach sterowania i zabezpieczeń zilustrowano na rys. 2.14. Integracja taka powinna być przeprowadzona w tworzeniu całościowego systemu zarządzania bezpieczeństwem takich systemów, szczególnie w obiektach i systemach infrastruktury krytycznej [208].



Rys. 2.14. Zintegrowane zarządzanie bezpieczeństwem funkcjonalnym i ochroną informacji [116]

Biorąc pod uwagę typową definicję ryzyka – wykorzystywaną w procesie oceny ryzyka – jako kombinacji częstości bądź prawdopodobieństwa wystąpienia zdarzenia awaryjnego oraz konsekwencji wystąpienia tego zdarzenia, poniżej zaproponowano uproszczoną metodę określania wymaganego poziomu SIL dla funkcji bezpieczeństwa, z uwzględnieniem aspektów ochrony informacji. Analiza taka bazuje oczywiście na informacji uzyskanej w procesie identyfikacji zagrożeń występujących w systemie technicznym, a także szacowania poziomu ryzyka z nimi związanego. Niektóre czynniki ryzyka brane pod uwagę podczas przeprowadzania tego typu analiz mają wpływ na oszacowaną wartość częstości bądź prawdopodobieństwa, niektóre zaś – na konsekwencje. Część ryzyka związana z parametrami częstości dotyczy najczęściej zagadnień niezawodności sprzętowej oraz niezawodności i pewności działania człowieka jako części systemu technicznego. Czynnik ryzyka związany z komunikacją i przesyłem danych pomiędzy poszczególnymi elementami systemu jest w takim przypadku pomijany. Może się jednak okazać, że w pewnych sytuacjach może on mieć dość znaczny wpływ na rzeczywisty poziom ryzyka analizowanego systemu.

W procesie integracji zagadnień bezpieczeństwa funkcjonalnego z ochroną informacji można zastosować pojęcie tzw. funkcji dwuparametrowej. W przypadku oszacowania niskiego poziomu ochrony informacji w analizowanym systemie infrastruktury krytycznej wymagania SIL dla funkcji bezpieczeństwa mogą ulec zmianie. Niski poziom ochrony informacji może być w takim przypadku potraktowany jako jeden z rodzajów potencjalnych błędów systematycznych systemu sterowania. Aby wymagania SIL pozostały bez zmian, konieczna staje się redukcja ryzyka związanego z poziomem ochrony informacji. Wiąże się to z podniesieniem wymagań, np. na poziom EAL, dla analizowanego systemu. W takiej sytuacji powstaje dwuparametrowa funkcja wymagań $f_{i,j}$, związana z funkcją bezpieczeństwa (poprzez wymagany poziom SIL) oraz analizowanym w ocenie ryzyka systemem sterowania, np. BPCS (poprzez wymagany poziom EAL). Sytuację taką przedstawiono na rys. 2.15 [24, 120].



Rys. 2.15. Generowanie wymagań w postaci funkcji dwuparametrowej łączącej zagadnienia bezpieczeństwa funkcjonalnego i ochrony informacji

Etap weryfikacji SIL dla struktury sprzętowej realizującej funkcje bezpieczeństwa opiera się w głównej mierze na modelowaniu probabilistycznym złożonych struktur sprzętowych realizujących funkcje bezpieczeństwa. Na etapie tym, podobnie jak to miało miejsce przy określaniu wymagań, można uwzględnić zagadnienia ochrony informacji na podstawie zaproponowanej klasyfikacji systemów sterowania, monitorowania i zabezpieczeń w obiektach i systemach infrastruktury krytycznej.

W tablicy 2.5 zawarto przykładową specyfikację zintegrowanych wymagań, obejmujących aspekty bezpieczeństwa funkcjonalnego i ochrony informacji. W tym celu zaproponowano określenie wymagań w postaci dwuparametrowej funkcji $f_{i,j}$, która reprezentuje symbolicznie konkretne wymagania odnoszące się zarówno do poziomów SIL, jak i EAL. Przykładowy system sterowania i zabezpieczeń, np. obsługujący rozległy rurociąg przesyłu ropy naftowej, powinien spełniać poziom nienaruszalności bezpieczeństwa SIL3 (na podstawie oceny ryzyka). Podane w tablicy 2.5 poziomy EAL związane z parametrem j funkcji dwuparametrowej (4 dla systemu II kategorii oraz 5 dla systemu III kategorii) zostały przyjęte przykładowo. Służą one pokazaniu, że wraz z wprowadzaniem do systemu zewnętrznych kanałów komunikacji wzrasta możliwość wystąpienia niepożądanego wpływu otoczenia na działanie systemu. Dlatego w rozważanych systemach należy zwiększyć poziom ochrony informacji.

Tablica 2.5

Zintegrowane podejście do określenia wymagań dotyczących poziomów SIL i EAL dla systemów kategorii I, II, III

System	Wymagania projektowe	
I	SIL3	EAL2
II	$f_{3,4}$	
III	$f_{3,5}$	

W przypadku systemu I kategorii, tj. takiego, w którym nie występują zewnętrzne kanały komunikacji, a co za tym idzie – nie istnieje możliwość ingerencji z zewnątrz do danych dotyczących stanu obiektu, wymagania projektowe potraktowano oddzielnie.

2.9. Podsumowanie

W niniejszym rozdziale przedstawiono bardzo aktualną problematykę związaną z analizą bezpieczeństwa funkcjonalnego rozproszonych systemów sterowania i automatyki zabezpieczeniowej w obiektach infrastruktury krytycznej wykorzystujących przemysłową sieć komputerową, z uwzględnieniem zagadnień ochrony informacji. W obiektach tego typu systemy sterowania i automatyki zabezpieczeniowej są projektowane jako systemy rozproszone, których nieprawidłowe działanie może doprowadzić do poważnych skutków, np.: skażenia środowiska, pożaru, wybuchu, utraty zdrowia i życia osób, spadku lub załamania produkcji, a w konsekwencji znacznych strat ekonomicznych. Zagadnienia bezpieczeństwa funkcjonalnego i ochrony informacji powinny być zatem rozpatrywane w sposób zintegrowany, w zależności od rodzaju kanałów komunikacji stosowanych do transmisji danych pomiędzy elementami systemu. Zagadnienia związane z zarządzaniem bezpieczeństwem funkcjonalnym systemów sterowania i automatyki zabezpieczeniowej są zawarte w normie PN-EN 61508 o charakterze ogólnym (dotyczącej różnych zastosowań) oraz normach sektorowych, np. PN-EN 61511 opracowanej dla potrzeb przemysłu procesowego i wydobywczego. Ogólne wymagania dotyczące zagadnień ochrony informacji w opisywanych systemach są zawarte w normach międzynarodowych ISO/IEC 15408, PN-ISO/IEC 17779 oraz PN-ISO/IEC 27001. Normy te dotyczą więc różnych aspektów bezpieczeństwa systemów komputerowych i ochrony informacji. W rozdziale tym omówiono konwencjonalne podejście do oceny bezpieczeństwa funkcjonalnego, nowe, integrujące aspekty bezpieczeństwa funkcjonalnego oraz czynniki związane z ochroną informacji w cyklu życia bezpieczeństwa systemów sterowania, monitorowania i zabezpieczeń obiektów infrastruktury krytycznej [208], w nawiązaniu do wymienionych norm [118, 119, 155].

Mimo że aspekty związane z analizami bezpieczeństwa funkcjonalnego i ochrony informacji zasadniczo się różnią i dotyczą odrębnych zagadnień (bezpieczeństwo funkcjonalne – automatyka zabezpieczeniowa; ochrona informacji – technologie informacyjne, informatyka), uwzględnienie zagadnień ochrony informacji w analizach bezpieczeństwa funkcjonalnego jest możliwe. W niniejszym rozdziale zarysowano podejście polegające na odpowiednim integrowaniu kryteriów bezpieczeństwa funkcjonalnego przy uwzględnieniu poziomów nienaruszalności bezpieczeństwa SIL z wykorzystaniem poziomów uzasadnionego zaufania EAL oraz poziomów uzasadnionej ochrony SAL w ramach rozszerzonej analizy i oceny ryzyka, a następnie weryfikowaniu tych poziomów dla rozważanych archi-

tektur sprzętowych i zastosowanych środków ochrony. Powstaje jednak pytanie, czy taka integracja jest właściwa i możliwa do przeprowadzenia. Z punktu widzenia analiz bezpieczeństwa funkcjonalnego można zastosować zbliżone ideowo do SIL poziomy uzasadnionego zaufania EAL. Ich praktyczna implementacja oraz trudności w ich interpretacji i zrozumieniu sprawiają jednak, że daje się zauważyć trend do ich niewykorzystywania w próbach integracji z bezpieczeństwem funkcjonalnym na rzecz poziomów uzasadnionej ochrony SAL. Poziomy EAL dotyczą w zdecydowanej większości pojedynczych rozwiązań technicznych (urządzeń, aplikacji komputerowych itp.), a nie podsystemów czy całych systemów. W związku z tym należy poważnie rozważyć stosowność korzystania z miar EAL na rzecz wartości bardziej ogólnych, będących urzeczywistnieniem realnego poziomu bezpieczeństwa związanego z ochroną informacji, a w istocie poziomu związanego z nią ryzyka. W integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji kluczową kwestią jest opracowanie skutecznych metod uwzględniających w czytelny sposób w modelach probabilistycznych wpływ infrastruktury przemysłowych sieci komputerowych. Nie można pominąć tych aspektów, gdyż uzyskane wyniki będą zbyt optymistyczne w stosunku do rzeczywistej sytuacji.

Krajowe wersje norm zarządzania jakością PN-EN ISO 9000, 9001 [167], środowiskiem PN-EN ISO 14001 [169] oraz bezpieczeństwem informacji PN-ISO/IEC 17779 [171], PN-ISO/IEC 27000 [172], ISO/IEC 27001 [95] zostały tak opracowane, aby mogły być odpowiednio integrowane w ramach systemu zarządzania przedsiębiorstwem. Zintegrowane podejście do zarządzania bezpieczeństwem funkcjonalnym i bezpieczeństwem informacji w przemysłowych systemach komputerowych w nawiązaniu do wymagań ogólnych oraz kryteriów zawartych w normach bezpieczeństwa funkcjonalnego serii: PN-EN 61508 [161] i PN-EN 61511 [162] oraz normie dotyczącej zarządzania ochroną informacji ISO/IEC 27001 [95] uwzględnia m.in. zagadnienia rozproszonych sieci komputerowych pełniących funkcje monitorowania, sterowania i zabezpieczeń, np. za pomocą systemów SCADA w różnych odpowiedzialnych zastosowaniach. W proponowanym podejściu zakłada się, że system SIS jest najważniejszy z punktu widzenia ochrony zasobów, gdyż do jego zadań należy realizacja zaprojektowanych i zaimplementowanych funkcji bezpieczeństwa, dla których wcześniej zostały określone wymagania SIL, a następnie wymagania te zostały poddane weryfikacji z uwzględnieniem stopnia ochrony informacji (niski, średni lub wysoki), reprezentowanego przez poziomy EAL, SAL lub liczbę pierścieni zabezpieczeniowo-ochronnych wokół niego [24, 176].

Na tym etapie pracy przedstawiono wiedzę dotyczącą wielu metod analizy i oceny zarówno bezpieczeństwa funkcjonalnego, jak i ochrony informacji obiektów przemysłowych, zwłaszcza systemów infrastruktury krytycznej. Są one podstawą do zaproponowania nowego, rozszerzonego podejścia w integracji obu zagadnień. To zintegrowane podejście – zarówno na etapie określenia wymagań, jak i ich weryfikacji – zaprezentowano w kolejnych rozdziałach niniejszej monografii. Zaproponowana metodyka została zaimplementowana w oprogramowaniu ProSIL-EAL, wspomagającym zarządzanie bezpieczeństwem funkcjonalnym; aplikacja ta stanowi rozszerzoną wersję programu ProSIL.

Rozdział 3

OKREŚLENIE WYMAGANEGO POZIOMU NIENARUSZALNOŚCI BEZPIECZEŃSTWA SIL

3.1. Wprowadzenie

System bądź obiekt, którego awaria może doprowadzić do utraty życia ludzkiego, zniszczenia mienia czy też zanieczyszczenia środowiska, można nazwać systemem krytycznym. System pełniący odpowiedzialną funkcję musi zostać poddany gruntownej analizie, w tym analizie bezpieczeństwa funkcjonalnego, mającej na celu określenie oraz późniejszą weryfikację jego poziomu bezpieczeństwa [110, 112, 121]. Każda awaria czy też niepoprawne zadziałanie elementu należącego do tego typu systemu może powodować bardzo poważne, trudne do oszacowania konsekwencje [36, 51]. Dlatego coraz częściej istotne znaczenie w redukcji ryzyka mają systemy sterowania oraz specjalistyczne systemy zabezpieczeń, instalowane w systemach podwyższonego ryzyka.

Analizę bezpieczeństwa funkcjonalnego można podzielić na kilka odrębnych, choć powiązanych ze sobą etapów w cyklu życia systemu związanego z bezpieczeństwem. Jednym z ważniejszych jest etap zdefiniowania funkcji bezpieczeństwa mogących się pojawić w systemie/ procesie, a także przypisania im wymagań bezpieczeństwa, w tym wymaganego poziomu nienaruszalności bezpieczeństwa. Poziom ten jest ściśle związany ze stopniem redukcji ryzyka przez wybraną funkcję bezpieczeństwa. Aby zaimplementować do systemu funkcję bezpieczeństwa (wraz z określoną dla niej całkowitą specyfikacją wymagań), należy wykonać szereg czynności opisanych w niniejszym rozdziale, poczynając od określenia zakresu analizy, poprzez dokonanie identyfikacji zagrożeń występujących w rozważanym systemie, po ocenę ryzyka i przypisanie odpowiedniego poziomu nienaruszalności bezpieczeństwa SIL do konkretnej funkcji bezpieczeństwa. Ogólnie wszystkie wymienione działania można określić mianem analizy ryzyka dla rozważanego systemu technicznego.

3.2. Specyfikacja wymagań bezpieczeństwa

W każdym systemie lub obiekcie infrastruktury krytycznej występują zagrożenia związane z jego pracą. W niektórych przypadkach jedynym rozwiązaniem pozwalającym na redukcję ryzyka związanego z takimi zagrożeniami jest wprowadzenie dodatkowych rozwiązań sprzętowych, które można uważać za system związany z bezpieczeństwem SRS (*safety-related system*). Systemy takie często są zbudowane na podstawie architektury E/E/PE i mają za zadanie realizować zdefiniowane funkcje bezpieczeństwa SRF (*safety-related function*).

W nawiązaniu do normy bazowej PN-EN 61508 oraz normy procesowej PN-EN 61511 przyjmuje się, że w celu utrzymania ryzyka dla systemu na poziomie akceptowalnym/ tolerowanym należy zdefiniować pewne wymagania dotyczące spełnienia takich funkcji przez realizujący je system. Istnieją dwa typy wymagań, które są konieczne do osiągnięcia bezpieczeństwa funkcjonalnego i które jednocześnie opisują funkcje bezpieczeństwa:

— wymagania funkcjonalne bezpieczeństwa, czyli jakie zadanie ma spełniać dana funkcja bezpieczeństwa;
— wymagania na nienaruszalność bezpieczeństwa, czyli prawdopodobieństwo, że dana funkcja bezpieczeństwa wykona się zgodnie z założonym celem.

Po zidentyfikowaniu funkcji bezpieczeństwa należy przypisać im – każdej z osobna – specyfikację wymagań funkcjonalnych, opisującą logikę działania systemu, który będzie realizował takie funkcje. W praktyce specyfikacja ta przybiera postać tabelarycznego bądź opisowego dokumentu lub też zbioru dokumentów, na podstawie których przebiega następnie etap projektowania struktury sprzętowej, która będzie realizować poszczególne funkcje bezpieczeństwa. Informacje na temat specyfikacji bezpieczeństwa są wykorzystywane także na etapie weryfikacji, czyli sprawdzenia, czy zaprojektowana struktura sprzętowa rzeczywiście spełnia wymagania na nienaruszalność bezpieczeństwa.

W części pierwszej PN-EN 61511 [162] wymieniono wymagania, które powinny być opisane przed przystąpieniem do procesu projektowania systemu zabezpieczającego. Przedstawiona tam lista jest bardzo obszerna i obejmuje swoim zasięgiem szereg szczegółowych informacji na temat procesu, systemu sterowania, jego budowy, zasady działania wraz z określeniem stanów bezpiecznych, przejściowych itp. Oprócz wymienionych powyżej zagadnień wyszczególnić można m.in.:
— wymagania dotyczące zidentyfikowania i uwzględnienia uszkodzeń o wspólnej przyczynie (*common cause failures*);
— przypuszczalne źródła przywołań oraz intensywności tych przywołań dla każdej funkcji bezpieczeństwa;
— opis wymagań dla odstępów pomiędzy okresami testów sprawdzających;
— wymagania dotyczące czasu odpowiedzi układu realizującego funkcję bezpieczeństwa w celu sprowadzenia procesu do stanu bezpiecznego;
— opis wartości pomiarowych w procesie oraz ich punkty włączenia;
— opis wyjść i ich działania w procesie oraz kryteria dla ich pomyślnego zadziałania;
— opis zależności funkcjonalnej pomiędzy wejściami a wyjściami w procesie (zależności logiczne, matematyczne itp.);
— wymagania dla wyłączeń ręcznych;
— wymagania dla zresetowania oraz ponownego włączenia funkcji bezpieczeństwa po jej wyłączeniu;
— określenie maksymalnej dopuszczalnej wartości zadziałania niepotrzebnego;
— opis rodzajów uszkodzeń oraz wymagane na nie odpowiedzi funkcji bezpieczeństwa;
— opis wszystkich specyficznych wymagań dotyczących procedury uruchamiania oraz restartowania funkcji bezpieczeństwa;
— opis wszystkich powiązań pomiędzy systemem realizującym funkcję bezpieczeństwa a innymi systemami (włączając w to operatora oraz BPCS);
— opis trybów pracy instalacji procesowej;
— specyfikację wymagań bezpieczeństwa oprogramowania.

Wszystkie te informacje mają na celu określenie wymagań funkcjonalnych stawianych projektowanemu systemowi związanemu z bezpieczeństwem.

W analizie bezpieczeństwa funkcjonalnego systemów sterowania i zabezpieczeń należy określić poziom nienaruszalności bezpieczeństwa SIL. Zdefiniowano cztery poziomy nienaruszalności bezpieczeństwa SIL, którym zgodnie z normą [30, 161] odpowiadają

ilościowe kryteria probabilistyczne, stanowiące przedziały prawdopodobieństwa dla pracy na żądanie systemu E/E/PE związanego z bezpieczeństwem.

Wymagania dotyczące nienaruszalności funkcji bezpieczeństwa określa się w trakcie oceny ryzyka w taki sposób, aby uzyskać redukcję ryzyka do poziomu akceptowalnego/ tolerowanego. Wymagania dla funkcji bezpieczeństwa są określane za pomocą analizy zagrożeń, czyli oceny, co należy wykonać, aby uniknąć zdarzenia niebezpiecznego. Po ich połączeniu z wymaganiami na nienaruszalność bezpieczeństwa otrzymuje się całkowitą specyfikację bezpieczeństwa dla zbioru zdefiniowanych funkcji bezpieczeństwa.

Ponieważ specyfikacja bezpieczeństwa jest wymagana w procesie projektowania struktury sprzętowej E/E/PE realizującej funkcję bezpieczeństwa, muszą być w niej zawarte wszystkie istotne informacje oraz – co również jest bardzo ważne – powinny one być dobrze udokumentowane. Przyjmuje się, że w ramach specyfikacji wymagań bezpieczeństwa powinny się znaleźć m.in. diagramy P&ID instalacji, diagramy przyczyn i skutków, diagramy logiczne itp. [8, 51, 59].

3.3. Wymagany SIL dla zdefiniowanych funkcji bezpieczeństwa

3.3.1. Identyfikacja oraz ocena zagrożeń

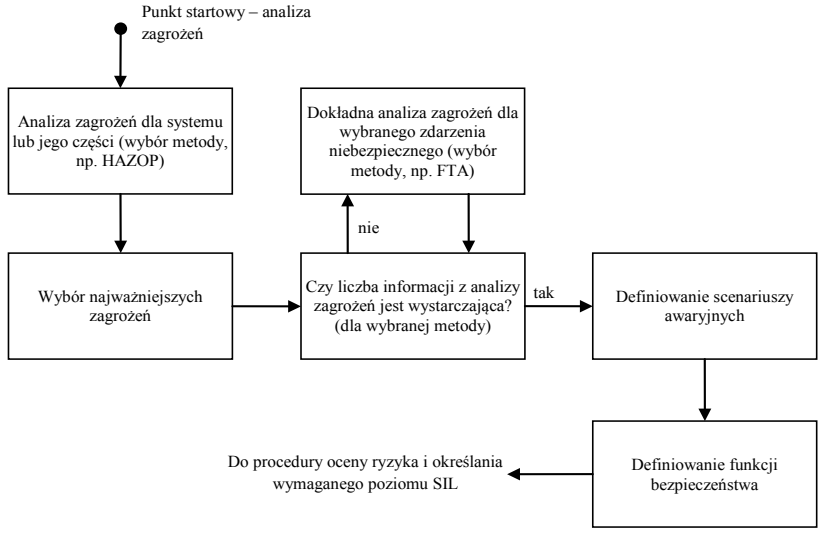
Jedną z najczęściej wykorzystywanych metod identyfikacji zagrożeń, które wprowadzają ryzyko dla personelu lub środowiska i mogą występować zarówno w nowych, jak i już istniejących obiektach przemysłowych, jest metoda HAZOP (*hazard and operability study*). Domyślnie była ona przeznaczona do oceny systemów procesowych – chemicznych, jednak jej zalety dostrzeżono również w innych branżach przemysłu i zaczęto ją stosować w innych złożonych systemach, jak również – w nieco zmodyfikowanej wersji – w analizie oprogramowania komputerowego.

Polega ona na ocenie poszczególnych elementów analizowanego systemu przez grupę ekspertów przy użyciu pewnych wytycznych i słów kluczowych [73]. Jest to metoda zespołowa, którą można wykorzystać na każdym etapie życia systemu, zalecane jest jednak, aby została zastosowana najwcześniej, jak jest to możliwe, tak by miała wpływ na późniejszy projekt końcowy systemu. Dzięki temu istnieje możliwość systematycznej i w pełni udokumentowanej oceny oraz wykrycia potencjalnych zagrożeń, które występują lub mogą występować w analizowanym systemie. Poprawne wykonanie analizy HAZOP wymaga posiadania szczegółowego schematu technologicznego rozważanego systemu, jak również bardzo dokładnej wiedzy o procesach w nim zachodzących. W przypadku braku takich informacji (najczęściej w pierwszej fazie projektowania systemu) można się posłużyć analizą HAZID (*hazard identification*), która także pozwala na zgrubną ocenę zagrożeń występujących bądź mogących wystąpić w systemie i nie wymaga dysponowania aż tak szczegółowymi danymi.

Jednym z najważniejszych aspektów cyklu życia systemów związanych z bezpieczeństwem jest rozpoznanie oraz zrozumienie zagrożeń, jakie mogą występować w systemie (procesie), z którym SRS będzie pracował. Identyfikacja oraz analiza zagrożeń występujących w takim systemie stanowią podstawową, integralną część analizy ryzyka, którą należy rozpocząć od zdefiniowania wartości poziomu ryzyka tolerowanego oraz właśnie od analizy zagrożeń. Z danych uzyskanych na tym etapie analizy można następnie uzyskać informacje na temat aktualnego poziomu ryzyka, wymaganej redukcji tego ryzyka, wymagań dla architektury systemu zabezpieczeniowego, pętli zabezpieczeniowych itp. Stąd wniosek, że budowa funkcji bezpieczeństwa powinna bezwzględnie być wynikiem analizy ryzyka.

Niestety, może się zdarzyć sytuacja odwrotna, kiedy architektura funkcji bezpieczeństwa będzie zaprojektowana jeszcze przed określeniem wymagań bezpieczeństwa oraz oszacowaniem wymaganego SIL [8, 30, 126]. Należy unikać takich sytuacji i skupiać się przede wszystkim na poprawnym zidentyfikowaniu zagrożeń mogących występować w analizowanym systemie, a dopiero potem, na podstawie wyszczególnionych zagrożeń, budować funkcje bezpieczeństwa. Proces analizy zagrożeń pozwala uzyskać odpowiedzi na pytania dotyczące zagrożeń mogących wystąpić w systemie, przyczyn ich powstania, prawdopodobieństwa (lub częstości) ich wystąpienia oraz konsekwencji, jakie się z nimi wiążą.

Ogólny schemat procedury przeprowadzania analizy zagrożeń przedstawiono na rys. 3.1. Po zrealizowaniu procesu identyfikacji zagrożeń uzyskuje się informacje na temat możliwych scenariuszy awaryjnych, a także zestawienie funkcji bezpieczeństwa, których zadaniem będzie zredukowanie prawdopodobieństwa wystąpienia zidentyfikowanych zagrożeń, a co za tym idzie – redukcja wartości ryzyka z nimi powiązanego.



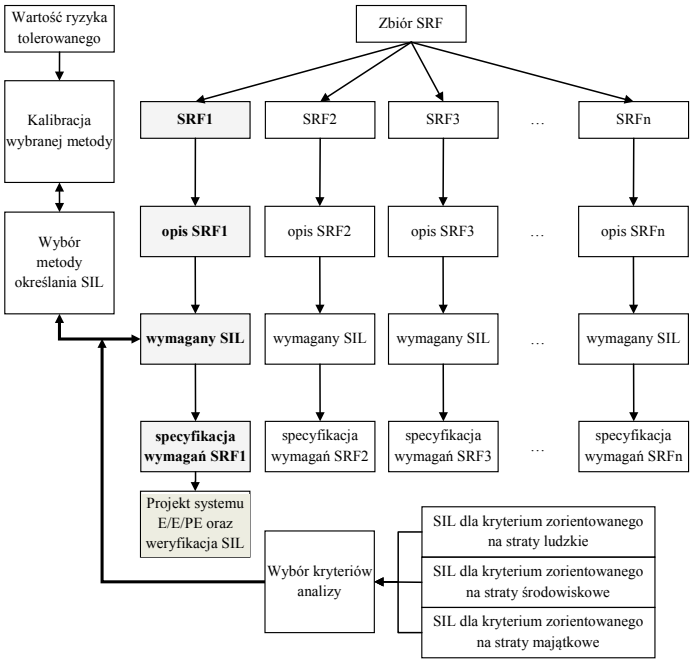
Rys. 3.1. Procedura analizy zagrożeń [7, 24]

3.3.2. Analiza ryzyka

W następnym kroku dla każdej funkcji bezpieczeństwa na podstawie przeprowadzonej analizy ryzyka należy określić wymagany poziom SIL oraz wymagania bezpieczeństwa. Obie te informacje zostaną potem wykorzystane w procesie tworzenia projektu systemu E/E/PE realizującego daną funkcję bezpieczeństwa, a także przy weryfikacji poziomu SIL dla projektu architektury sprzętowej. Ogólny schemat tej idei zarysowano na rys. 3.2.

Każda zidentyfikowana funkcja bezpieczeństwa SRF powinna zostać następnie szczegółowo opisana. Do każdej SRF powinna być przypisana specyfikacja jej działania pod względem funkcjonalnym. Kolejnym etapem jest określenie wymaganego poziomu nienaruszalności bezpieczeństwa dla każdej funkcji osobno na podstawie oceny ryzyka.

Podczas oceny ryzyka należy określić zakres analizy poprzez podanie kryteriów, dla których tworzone będą wymagania na nienaruszalność SRF [8, 23, 24].



Rys. 3.2. Ogólny schemat ideowy struktury funkcji bezpieczeństwa [8, 114]

I tak, analizę tę można przeprowadzić dla trzech głównych kryteriów zorientowanych na straty:
— ludzkie (kr_1);
— środowiskowe (kr_2);
— majątkowe (kr_3).

Wybór kryterium analizy zależy od specyfiki rozważanego systemu technicznego oraz od kontekstu analizy. Przy wyborze tylko jednego kryterium wynik oceny ryzyka będzie jednoznacznie identyfikował wymagany poziom SIL. Gdy wybrane zostaną przynajmniej dwa kryteria, ocena ryzyka będzie musiała zostać przeprowadzona dla każdego z nich z osobna. W takiej sytuacji poziom nienaruszalności bezpieczeństwa SIL będzie zatem określony jako [7, 15, 22]:

$$SIL = \max_i SIL_{kr_i} \tag{3.1}$$

Zapis ten wynika bezpośrednio z konserwatywnych założeń mówiących o konieczności wyboru maksymalnej wymaganej wartości SIL spośród wszystkich wartości określonych dla różnych kryteriów w procesie oceny ryzyka. System związany z bezpieczeństwem realizujący taką funkcję będzie musiał zatem spełnić takie wymagania. Istnieje możliwość wyboru metody, za pomocą której zostanie przeprowadzona ocena ryzyka związanego z zagrożeniami, dla których projektowana jest funkcja bezpieczeństwa.

Jak już wspomniano, podczas określania wymaganego poziomu SIL należy dokonać wyboru metody oceny ryzyka, jaka zostanie wykorzystana. Dostępne metody można podzielić według podanych typów:
— jakościowe;

— półjakościowe;
— ilościowe.

Przy ocenie ryzyka wykorzystuje się wiedzę na temat skutków oraz częstości lub prawdopodobieństwa występujących zdarzeń awaryjnych. Skojarzone z nimi parametry ryzyka mogą mieć pewne cechy opisujące ich charakter i umożliwiające lepsze oszacowanie przypisanych dla nich wartości [59]. I tak, przykładowo, dla parametru prawdopodobieństwa zajścia zdarzenia awaryjnego można rozważać takie cechy, jak:
— istnienie warstw zabezpieczeń;
— dane historyczne o występowaniu podobnych zdarzeń awaryjnych.

Po określeniu wymaganego poziomu SIL należy wyszczególnić specyfikację wymagań dla kolejnych funkcji bezpieczeństwa. Specyfikacja ta, oprócz wymagań funkcjonalnych oraz SIL, powinna zawierać informacje o wymogach nakładanych na urządzenia (w ich skład wchodzą m.in. elementy pomiarowe, logiczne oraz wykonawcze), które będą realizować wybraną funkcję. Wymogi te są najczęściej ściśle związane z analizowanym procesem technologicznym oraz systemami, które pracują lub będą z nim pracować. Ważne jest, aby w specyfikacji bezpieczeństwa znalazły się informacje o wszystkich warunkach operacyjnych rozważanego procesu, od jego uruchomienia, poprzez utrzymywanie, po wyłączanie (np. planowane przeglądy, kolejność załączania lub odstawiania poszczególnych systemów, podsystemów czy też urządzeń). Należy też tutaj umieścić informacje na temat warunków, w jakich pracować będą urządzania przypisane do systemu związanego z bezpieczeństwem, np. o podwyższonym ryzyku powstawania korozji, itp.

Podsumowując, proces analizy i oceny ryzyka związanego z bezpieczeństwem funkcjonalnym powinien się zakończyć wygenerowaniem zestawu wymagań dla wszystkich zidentyfikowanych funkcji bezpieczeństwa. Może on mieć postać jednego dokumentu lub zbioru wielu dokumentów, jednak zawsze powinien zawierać opis wymagań bezpieczeństwa (czyli jakie zadanie ma spełniać dana funkcja bezpieczeństwa), jak również wyszczególnienie wymagań na nienaruszalność bezpieczeństwa (czyli jak bardzo niezawodny ma być system realizujący tę funkcję bezpieczeństwa).

3.4. Określenie wymagań SIL – metody jakościowe

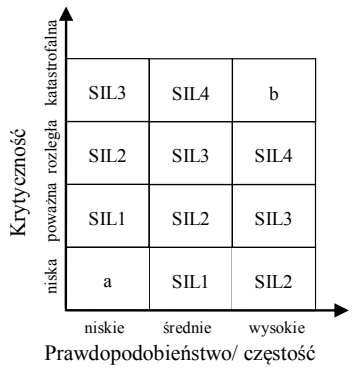
Poziom nienaruszalności bezpieczeństwa SIL jest wyznacznikiem tego, jak dobry powinien być system realizujący funkcję bezpieczeństwa, tzn. z jakim prawdopodobieństwem wykona on powierzone mu zadania. Procedura określania wymaganego poziomu SIL dla wybranej funkcji bezpieczeństwa powinna przebiegać w podobny sposób, jak ma to miejsce przy identyfikacji zagrożeń. Ponieważ jest to proces wymagający szerokiej wiedzy, powinien być przeprowadzany przez grupę ekspertów z różnych dziedzin. Wybór samej metody określania SIL zależy od doświadczenia, liczby informacji wymaganych przy podejmowaniu tego typu decyzji, a także od odgórnej polityki bezpieczeństwa.

W literaturze opisano wiele metod określania wymaganego SIL. Wciąż pojawiają się publikacje naukowe obrazujące nowe lub ulepszające już istniejące i ogólnie znane metody [13, 26, 30, 140, 151, 189]. Nie można jednoznacznie stwierdzić, która metoda jest dobra lub lepsza od innej. Można natomiast wybierać spomiędzy metod bazujących na kryteriach jakościowych lub ilościowych. Pierwsze z wymienionych są łatwiejsze i szybsze do realizacji. Wymagają mniejszej liczby informacji i z reguły bazują na kategoryzacji poziomów ryzyka. Metody ilościowe są z kolei bardziej rozbudowane, wymagają większej wiedzy

i umiejętności ich wykorzystywania, a przede wszystkim danych ilościowych, których uzyskanie jest często bardzo utrudnione lub wręcz niemożliwe. Wadę metod *stricte* jakościowych stanowi jednak fakt, że w pewnych okolicznościach mogą prowadzić do zbyt rygorystycznych decyzji, a co za tym idzie – mogą narażać firmę na dużo większe koszty wdrożenia technologii bezpieczeństwa [35, 51, 99]. Metody ilościowe w praktyce dają niższy wymagany poziom SIL, co przekłada się na znaczącą redukcję kosztów związanych z realizacją funkcji bezpieczeństwa [59]. Różnica kosztów przy implementacji sprzętowej funkcji bezpieczeństwa wymagającej poziomu nienaruszalności bezpieczeństwa SIL2 i funkcji bezpieczeństwa wymagającej poziomu nienaruszalności bezpieczeństwa SIL3 może być liczona w setkach tysięcy złotych. Do problemu określania wymaganego SIL należy zatem podchodzić poważnie i mieć świadomość, że ten krok analizy bezpieczeństwa funkcjonalnego będzie w przyszłości determinował kolejne etapy tej analizy, takie jak m.in. stworzenie projektu systemu zabezpieczeniowego oraz weryfikacji SIL.

Jedną z metod określania wymaganego poziomu nienaruszalności bezpieczeństwa, bazującą na parametrach opisywanych jakościowo, są tzw. tablice krytyczności. Metoda ta jest chętnie wykorzystywana w analizach przeprowadzanych dla przemysłu procesowego, chemicznego oraz petrochemicznego [193]. Matrycę taką buduje się na bazie tzw. tablicy krytyczności zdarzenia zagrażającego, która precyzuje zakres wymaganej redukcji ryzyka dla każdej kombinacji parametrów częstości wystąpienia takiego zdarzenia oraz jego krytyczności. Przykładową matrycę przedstawiono na rys. 3.3. Każde pole takiej tablicy odpowiada wymaganemu poziomowi SIL, który będzie musiał być spełniony przez system realizujący badaną funkcję bezpieczeństwa.

Warto zwrócić w tym miejscu uwagę na to, że metoda jakościowej matrycy ryzyka jest często stosowana w zmodyfikowanej wersji analizy zagrożeń HAZOP. Służy ona w takiej sytuacji do szybkiego i zgrubnego oszacowania ryzyka dla każdej zidentyfikowanej sytuacji awaryjnej w analizowanym systemie [39]. Dzięki wiedzy ekspertów, którzy przeprowadzają analizę HAZOP, można już na tym etapie wyróżnić zagrożenia, które mogą powodować powstanie ryzyka na poziomie nieakceptowalnym.

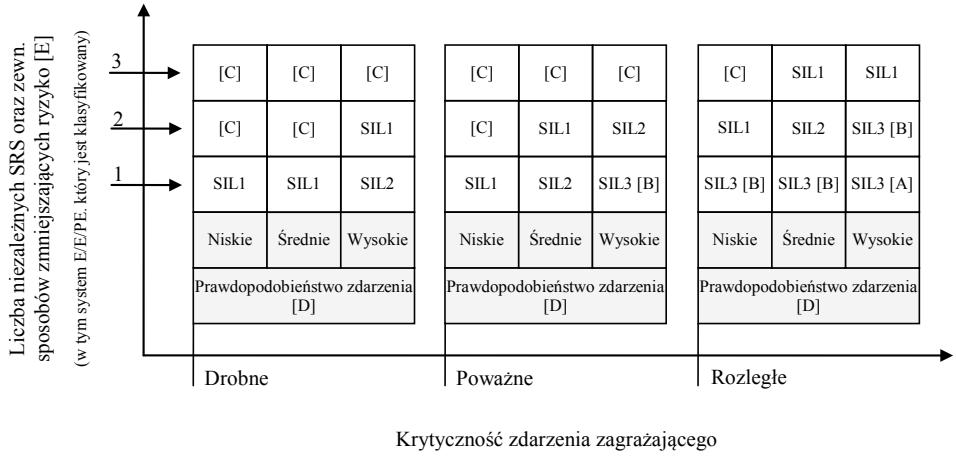


Rys. 3.3. Przykładowa matryca ryzyka [7, 8]

Metodę matrycy ryzyka stosuje się często wraz z analizą warstw zabezpieczeń występujących w rozpatrywanym systemie, z tym że nie uwzględnia się ich oddziaływania na parametr prawdopodobieństwa wystąpienia zdarzenia awaryjnego. Zakłada się przy tym, że metoda ta ma zastosowanie, gdy:

— każdy system związany z bezpieczeństwem (E/E/PE oraz wykonane w innych technikach) oraz każdy zewnętrzny sposób zmniejszania ryzyka są od siebie niezależne, jak również są traktowane jako osobne poziomy ochrony, samodzielnie zmniejszające ryzyko;
— każdy kolejny poziom ochrony poprawia poziom nienaruszalności bezpieczeństwa o rząd wielkości;
— wykorzystywany jest tylko jeden system związany z bezpieczeństwem wykonany w technice E/E/PE, dla którego tą metodą ustala się niezbędny poziom SIL.

Gdy uwzględni się wszystkie powyższe założenia, można otrzymać tablice krytyczności zdarzenia zagrażającego (awaryjnego). Przykładowe tablice przedstawiono na rys. 3.4.



Rys. 3.4. Tablice krytyczności zdarzenia zagrażającego wg PN-EN 61508 [126, 161]

Ogólne zasady opisanej metody są następujące [161]:
— przy poziomie ryzyka [A] jeden system E/E/PE związany z bezpieczeństwem SIL3 nie zapewnia wystarczającego zmniejszenia ryzyka – wymagane są dodatkowe sposoby zmniejszania ryzyka;
— przy poziomie ryzyka [B] jeden system E/E/PE związany z bezpieczeństwem może nie zapewniać wystarczającego zmniejszenia ryzyka – wymagana jest analiza zagrożeń i ryzyka w celu określenia, czy niezbędne jest zastosowanie dodatkowych metod zmniejszających ryzyko;
— najprawdopodobniej niezależny system E/E/PE związany z bezpieczeństwem nie jest wymagany – [C];
— prawdopodobieństwo zdarzenia jest prawdopodobieństwem wystąpienia zdarzenia zagrażającego bez udziału jakiegokolwiek systemu E/E/PE związanego z bezpieczeństwem lub zewnętrznego sposobu zmniejszającego ryzyko – [D];
— prawdopodobieństwo zdarzenia zagrażającego oraz całkowita liczba niezależnych poziomów ochrony są określane w odniesieniu do konkretnych zastosowań – [E].

W przypadku, gdy wartość ryzyka lub jego część odnosząca się do częstości zdarzenia awaryjnego nie może być wyrażona liczbowo, z pomocą przychodzą metody jakościowe. Przykładem najczęściej wykorzystywanej metody jakościowej jest graf ryzyka. Metoda ta

bazuje na pewnej liczbie parametrów ryzyka, opisujących charakter sytuacji niebezpiecznej, mogącej spowodować poważne skutki dla zdrowia i życia jednostki ludzkiej lub grupy ludzi, środowiska lub mogącej wywołać poważne straty finansowe, przy niezadziałaniu lub nieistnieniu systemu zabezpieczającego. Parametry te posiadają zdefiniowane zbiory przedziałów (czynników) opisujące ich wartości jakościowe. Dzięki wykorzystaniu tych parametrów można dokonać oceny oraz stopniowania ryzyka. Wyszczególniono cztery parametry ryzyka, które są wystarczająco ogólne, aby mogły być wykorzystane w szerokim spektrum zastosowań. Może się jednak zdarzyć sytuacja, w której wymagane będzie rozszerzenie liczby parametrów opisujących sytuację zagrożenia [15].

Graf ryzyka wykorzystuje model ryzyka oparty na równaniu [161]:

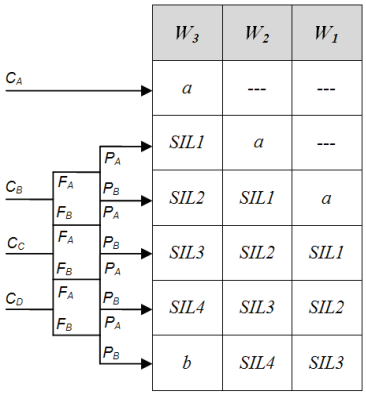
$$R = f \cdot C \tag{3.2}$$

gdzie: R – ryzyko bez zastosowania systemów związanych z bezpieczeństwem; f – częstość wystąpienia zdarzenia zagrażającego bez zastosowania systemów związanych z bezpieczeństwem; C – konsekwencje tego zdarzenia.

Częstość zdarzenia jest rozpatrywana jako składowa trzech czynników:

a) częstości i czasu przebywania w strefie zagrożenia (F);
b) możliwości uniknięcia zagrożenia (P);
c) prawdopodobieństwa wystąpienia zagrożenia bez użycia systemu związanego z bezpieczeństwem (W).

Parametry te są określone za pomocą jakościowych przedziałów kryterialnych, które zostały zestawione w tablicy 3.1. Kombinacja wyżej wymienionych parametrów tworzy z kolei ogólną strukturę grafu ryzyka dla kryterium strat personalnych, który przedstawiono na rys. 3.5.



Rys. 3.5. Struktura grafu ryzyka wg PN-EN 61508 [161]

Wymagania określone są następująco:

— --- – brak wymagań bezpieczeństwa;
— A – brak specjalnych wymagań bezpieczeństwa;
— SIL1÷SIL4 – poziom nienaruszalności bezpieczeństwa;
— b – pojedynczy system E/E/PE jest niewystarczający do zapewnienia wymaganego poziomu bezpieczeństwa.

Tablica 3.1

Parametry ryzyka dla grafu ryzyka na podstawie PN-EN 61508 [161]

Parametr ryzyka		Klasyfikacja	Opis
Konsekwencje C	C_A C_B C_C C_D	Drobne obrażenie Poważne lub trwałe uszkodzenie ciała jednej lub wielu osób; śmierć jednej osoby Śmierć wielu osób Bardzo wiele ofiar śmiertelnych	W ramach tego parametru ryzyka uwzględnia się uszkodzenia ciała lub utratę życia osób narażonych na skutki zdarzenia awaryjnego. Należy wziąć pod uwagę konsekwencje takiego zdarzenia oraz normalnego leczenia.
Częstość i czas ekspozycji w strefie zagrożenia F	F_A F_B	Rzadkie do częstszych Częste do stałych	Prawdopodobieństwo przebywania osób narażonych na skutki zdarzenia awaryjnego w strefie jego oddziaływania.
Możliwość uniknięcia zdarzenia zagrażającego P	P_A P_B	Możliwe w określonych warunkach Prawie niemożliwe	W ramach tego parametru ryzyka należy brać pod uwagę takie czynniki, jak: – sposób obsługi procesu; – szybkość rozwoju zdarzenia awaryjnego; – łatwość rozpoznania zagrożenia; – możliwości uniknięcia skutków zagrożenia; – doświadczenie w dziedzinie bezpieczeństwa.
Prawdopodobieństwo wystąpienia zdarzenia niepożądanego W	W_1 W_2 W_3	Bardzo nieznaczne Nieznaczne Względnie duże	Dla tego parametru należy oszacować prawdopodobieństwo wystąpienia zdarzenia awaryjnego bez stosowania jakichkolwiek systemów związanych z bezpieczeństwem (wykonanych w technice E/E/PE lub innych) lecz z wykorzystaniem wszystkich zewnętrznych sposobów zmniejszających ryzyko.

Mogą się pojawić sytuacje, w których dla określonych konsekwencji pojedynczy system E/E/PE związany z bezpieczeństwem będzie niewystarczający dla zapewnienia koniecznego zmniejszenia ryzyka (sytuacja z wartością b w grafie).

Użycie parametrów ryzyka C, F oraz P prowadzi do sześciu wyjść z grafu, które są przyporządkowane do jednej ze skal: W_1, W_2 i W_3. Każdy punkt na tych skalach jest wskazaniem koniecznej nienaruszalności bezpieczeństwa, którą musi posiadać system E/E/PE związany z bezpieczeństwem. Część tabelaryczna przedstawionego powyżej grafu stanowi wskazanie koniecznego zmniejszenia ryzyka, które musi być spełnione przez system zwią-

zany z bezpieczeństwem i jest powiązane z wymaganymi poziomami nienaruszalności bezpieczeństwa SIL.

Przy określaniu wymaganego poziomu SIL dla funkcji bezpieczeństwa należy stwierdzić, według jakiego kryterium dokonuje się oceny ryzyka. Podstawowe kryteria określają:
— poziom uszczerbku na zdrowiu lub utraty życia ludzi;
— poziom strat środowiskowych;
— poziom strat majątkowych.

Wykorzystanie grafów ryzyka w procesie określania wymaganego poziomu nienaruszalności bezpieczeństwa, choć bardzo popularne, stwarza niestety także pewne problemy interpretacyjne [15, 101]. Stąd liczne próby udoskonalenia tego narzędzia, przedstawiane w literaturze [13, 26, 30, 140, 151, 189].

Kalibrowany graf ryzyka został przedstawiony w dokumencie PN-EN 61511 jako próba dostosowania metody grafu ryzyka do potrzeb przemysłu procesowego. Jest to metoda typu półjakościowego, tzn. graf ryzyka jest częściowo kalibrowany jakościowo. Założono, że w grafie tym wykorzystywane będą te same parametry ryzyka co w metodzie przedstawionej w dokumencie PN-EN 61508, z tym że zmodyfikowano ich opis i znaczenie (tabl. 3.2).

Tablica 3.2

Parametry ryzyka dla grafu ryzyka na podstawie PN-EN 61511 [162]

Parametr ryzyka	Opis
Konsekwencje *C*	Liczba wypadków i/lub poważnych obrażeń, które mogą być spowodowane wystąpieniem zdarzenia awaryjnego, określona przez obliczenie średniego czasu przebywania w obszarze zagrożonym, przy uwzględnieniu podatności na skutki zdarzenia awaryjnego.
Częstość i czas ekspozycji w strefie zagrożenia *F*	Prawdopodobieństwo przebywania osób narażonych na skutki zdarzenia awaryjnego w strefie jego oddziaływania, określana jako ułamek czasu przebywania podczas zdarzenia.
Możliwość uniknięcia zdarzenia zagrażającego *P*	Prawdopodobieństwo, że osoba przebywająca w strefie zagrożonej oddziaływaniem zdarzenia awaryjnego, przy niezadziałaniu systemu bezpieczeństwa, będzie w stanie się z niej wydostać.
Częstość zdarzenia niepożądanego *W*	Prawdopodobna liczba zdarzeń awaryjnych na rok, z uwzględnieniem sytuacji, gdy nie ma systemu związanego z bezpieczeństwem. Można się posłużyć informacją na temat wszystkich uszkodzeń mogących wywołać zdarzenie awaryjne, szacując ogólny stopień częstości jego wystąpienia. Uwzględnione powinno zostać istnienie innych warstw zabezpieczeń.

W procesie kalibracji grafu ryzyka należy rozważyć dwa aspekty ryzyka skierowanego na straty ludzkie: ryzyko indywidualne oraz ryzyko społeczne. Pierwsze z nich odnosi się do osoby najbardziej narażonej na skutki działania zdarzenia niebezpiecznego i liczone jest w skali roku. Wartość maksymalna tego poziomu ryzyka jest związana ze wszystkimi zagrożeniami; określa się maksymalną wartość ryzyka, która jest tolerowana. Dla tego typu ryzyka można oszacować wartość parametru ryzyka związanego z czasem ekspozycji w strefie zagrożenia. Ryzyko społeczne z kolei odnosi się do wszystkich osób narażonych na skutki działania zdarzenia niebezpiecznego w skali roku. Najczęściej do obliczenia poziomu tego ryzyka stosuje się krzywe *F*-*N*. Wymaga się, aby wartość tego poziomu ryzyka

była zredukowana przynajmniej do maksymalnej wartości tolerowanej przez grupę osób zainteresowanych i aż do poziomu, który nie powoduje dysproporcji pomiędzy przedziałem zmniejszonego ryzyka a kosztami związanymi z tą redukcją.

W przedstawionym przykładzie kalibracji grafu ryzyka wprowadzono pojęcie podatności V (*vulnerability*) na skutki zdarzenia awaryjnego, które jest częścią parametru ryzyka związanego z konsekwencjami. Wiąże się to z doświadczeniem praktycznym, mówiącym, że nie każde zdarzenie awaryjne powoduje natychmiastowe powstanie poważnych konsekwencji. Jest to więc parametr związany z czasem i opisuje, w jaki sposób dana konsekwencja będzie postępować w czasie. W przypadku wystąpienia zdarzenia awaryjnego, którego konsekwencje będą bardzo poważne, ale czas potrzebny na rozwój tych konsekwencji jest relatywnie długi, istnieje duże prawdopodobieństwo, że da się ich uniknąć poprzez wprowadzenie odpowiednich działań. Skoro mowa jest o możliwości uniknięcia konsekwencji, należy wyjaśnić ważny aspekt, tzn. jaka jest różnica pomiędzy opisywaną podatnością a osobnym parametrem ryzyka P, opisującym możliwość uniknięcia zdarzenia awaryjnego, aby nie doszło do sytuacji, w której dwukrotnie weźmie się pod uwagę ten sam czynnik. Mogłoby to prowadzić do niewłaściwych wyników oceny ryzyka. Otóż podatność V odnosi się do szybkości eskalacji zjawiska związanego z wystąpieniem zdarzenia awaryjnego i jego konsekwencji, parametr P jest natomiast związany z zapobieganiem wystąpieniu sytuacji awaryjnej, np. poprzez odpowiednie działanie operatora po stwierdzeniu awarii i niezadziałaniu systemu związanego z bezpieczeństwem.

Kalibrowany półilościowy graf ryzyka może być z powodzeniem stosowany w przypadku istnienia dużej liczby funkcji bezpieczeństwa. Metoda ta umożliwia eliminację tych funkcji, które nie odgrywają zbyt dużej roli w eliminacji całkowitego ryzyka, oraz uwydatnienie tych, które w dużym stopniu wpływają na jego redukcję. Z drugiej strony wymaga żmudnego procesu kalibracji i najlepiej nadaje się do analizy funkcji, w których wartość ryzyka resztkowego jest relatywnie mała w porównaniu z wartością ryzyka tolerowanego.

Parametr W, który określa, podobnie jak to miało miejsce w przypadku grafu jakościowego, prawdopodobieństwo lub częstość wystąpienia zdarzenia awaryjnego, ma tutaj jednak nieco inne znaczenie. Jest bowiem określony przez wartość, która nie powinna uwzględniać obecności systemu związanego z bezpieczeństwem wykonanego w technice E/E/PE, lecz (i tutaj różnica w stosunku do grafu jakościowego) musi uwzględniać redukcję ryzyka związaną z innymi warstwami zabezpieczeń [63, 162].

3.5. Określenie wymagań SIL – metoda ilościowa

Podejście ilościowe do określania wymaganego poziomu SIL dla wybranej funkcji bezpieczeństwa daje możliwość oszacowania wartości liczbowych redukcji ryzyka. Jest ono szczególnie przydatne i polecane do wykorzystywania w sytuacji, gdy:

— wartość ryzyka tolerowanego może być opisana liczbowo (np. tolerowany przedział od 10^{-5} do 10^{-4} zgonów/rok);
— istnieją opisane liczbowe wartości docelowe dla poziomów nienaruszalności bezpieczeństwa systemów związanych z bezpieczeństwem (np. poziomy SIL wg normy).

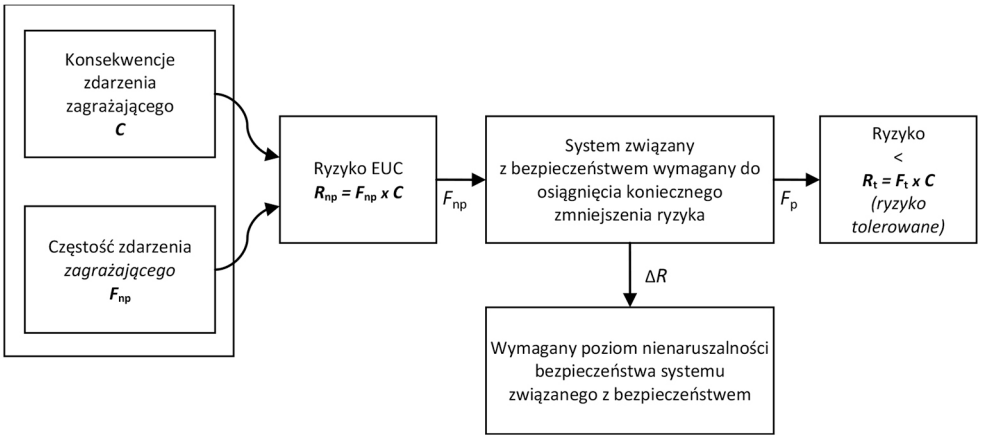
Korzystając z ogólnej koncepcji zmniejszania ryzyka, przedstawionej w dokumencie PN-EN 61508 [161], należy dla każdej zdefiniowanej funkcji bezpieczeństwa (rys. 3.6):

— określić wartość ryzyka tolerowanego;
— określić wartość ryzyka wyposażenia sterowanego EUC;

— określić poziom niezbędnego zmniejszenia ryzyka w celu osiągnięcia wartości ryzyka tolerowanego;
— przypisać niezbędny poziom zmniejszenia ryzyka do systemów E/E/PE mających realizować funkcję bezpieczeństwa, systemów związanych z bezpieczeństwem wykonanych w innych technikach oraz zewnętrznych sposobów zmniejszających ryzyko.

Zgodnie z wykorzystywanym modelem ryzyka w jego skład wchodzą dwa elementy. Jednym z nich jest oznaczona jako F_{np} częstość skojarzona z ryzykiem, które istnieje w przypadku danego EUC, z jaką zdarzenie zagrażające mogłoby wystąpić w sytuacji braku systemu zabezpieczającego. Drugim elementem jest parametr konsekwencji tego zdarzenia, oznaczony jako C.

Parametr częstości może zostać wyznaczony na podstawie:
— analizy wskaźnika uszkodzeń systemu sterowania EUC z porównywalnych sytuacji;
— danych z odpowiednich baz danych;
— obliczeń wykorzystujących odpowiednie metody prognozowania.



Rys. 3.6. Obliczanie wartości nienaruszalności bezpieczeństwa SIL [114, 161]

Określenia osiągniętego SIL dokonuje się poprzez oszacowanie wartości średniego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na żądanie przez system związany z bezpieczeństwem przy pracy na rzadkie przywołanie PFD_{avg} (dla stałej konsekwencji C):

$$PFD_{avg} \leq F_t \,/\, F_{np} \tag{3.3}$$

gdzie: F_t – częstość związana z ryzykiem tolerowanym; F_{np} – częstość przywołań systemu związanego z bezpieczeństwem; F_p – częstość po zastosowaniu zabezpieczeń.

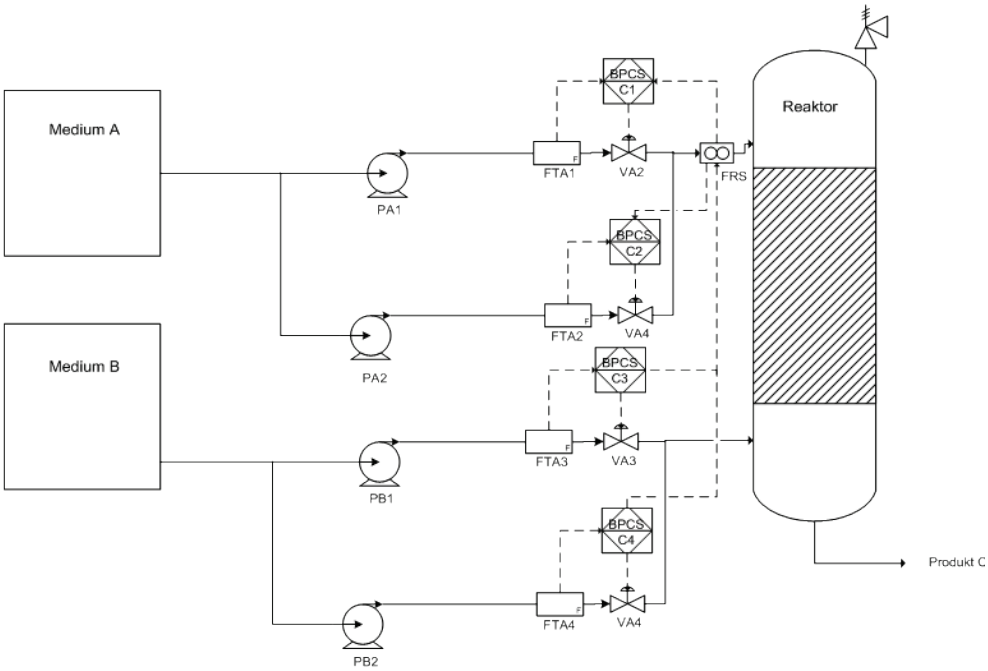
Przy założeniu, że konsekwencje C pozostają stałe, system E/E/PE realizujący funkcję bezpieczeństwa musi się cechować zdolnością zmniejszenia częstości zdarzenia niebezpiecznego co najmniej z wartości F_{np} do wartości tolerowanej F_t.

Należy pamiętać, że przy określaniu poszczególnych wartości związanych z obliczanym ryzykiem zakłada się pewną klasyfikację ryzyka, a następnie wykonuje następujące kroki:
— określenie wartości F_n bez dodawania jakichkolwiek sposobów zabezpieczających;

— określenie konsekwencji C bez dodawania jakichkolwiek sposobów zabezpieczających;
— określenie, poprzez użycie tablicy klasyfikacji ryzyka, czy dla częstości F_{np} oraz konsekwencji C osiągnięty zostanie poziom ryzyka tolerowalnego;
— jeśli po zastosowaniu tablicy klasyfikacji ryzyka otrzyma się klasę ryzyka I, to wymagana jest dalsza redukcja ryzyka; ryzyko klasy IV lub III byłoby tolerowalne; ryzyko klasy II wymagałoby dalszych analiz;
— określenie prawdopodobieństwa PFD_{avg}, po to by uzyskać wartość koniecznego zmniejszenia ryzyka (ΔR), dla stałych konsekwencji C w konkretnej opisanej sytuacji $PFD_{avg} = (F_t/F_{np}) = \Delta R$;
— określenie poziomu SIL dla $PFD_{avg} = (F_t/F_{np})$.

3.6. Przykład określenia poziomu nienaruszalności bezpieczeństwa SIL

Na podstawie opisanej we wcześniejszym rozdziale metody grafu ryzyka poniżej zaprezentowano prosty przykład procedury określenia wymaganego poziomu SIL dla jednej z funkcji bezpieczeństwa, która ma zostać zaimplementowana na rozpatrywanym obiekcie technicznym. Przykładową instalację technologiczną przedstawiono na rys. 3.7.



Rys. 3.7. Przykładowa instalacja technologiczna [114]

Biorąc pod uwagę proces identyfikacji zagrożeń (HAZOP, tabl. 3.3) i ich wstępną ocenę na podstawie jakościowego rankingu ryzyka (tabl. 3.4), wyszczególniono zagrożenia prowadzące do poważniejszych awarii.

Tablica 3.3

Przykładowa analiza zagrożeń HAZOP [7, 8, 114]

Nazwa:			*Przykład HAZOP*						**Arkusz:** *1 z 10*	
Skład zespołu:			*EP, MŚ, PK, TB*						**Data:** *10.08.2017*	
Rozważana część systemu:			*Linia przesyłowa ze zbiornika A do reaktora*						**Data spotkania:** *09.07.2017*	
Szczegóły:			**Materiał:** *A* **Czynność:** *Ciągły przepływ materiału A w dawce większej niż dawka materiału B* **Źródło:** *Zbiornik medium A* **Cel:** *Reaktor*							
Nr	Słowo kluczowe	Element/ węzeł	Odchyłka	Przyczyna	Skutek	Zabezpieczenie	Komentarze	Ranking	Wymagane działania	Odpowiedzialny
1	BRAK	Medium A	Brak medium A	Zbiornik medium A jest pusty	Brak dopływu medium A do reaktora Eksplozja	Brak	Nieakceptowalne		Rozważyć: – zainstalowanie alarmu niskiego poziomu medium A w zbiorniku – automatyczne wyłączenie pompy B	EP
2	BRAK	Przepływ A (dawka większa od dawki medium B)	Brak przepływu medium A	Pompa A zatrzymana, linia przesyłowa A zablokowana	Eksplozja	Brak	Nieakceptowalne		Rozważyć: – pomiar przepływu medium A – zainstalowanie alarmu niskiego przepływu medium A – automatyczne wyłączenie pompy B	MŚ
3	WIĘCEJ	Medium A	Za dużo medium A (zbiornik źródła przepełniony)	Wypełnianie zbiornika przy braku wystarczającej wolnej przestrzeni	Wyciek medium A poza zbiornik	Brak	Identyfikacja poprzez przegląd zbiornika		Rozważyć zainstalowanie alarmu wysokiego stanu medium A w zbiorniku	TB
4	WIĘCEJ	Przepływ A	Za duży przepływ Zwiększony przepływ medium A w linii przesyłowej	Za duży rozmiar wirnika pompy Zły wybór pompy	Potencjalne straty w produkcji Finalny produkt ze zbyt dużą zawartością medium A	Brak	Brak		Sprawdzić charakterystykę pompy w czasie odbioru Powtórzyć odbiór pompy	MŚ
5	WIĘCEJ	Reaktor	Za duże ciśnienie w reaktorze	Uszkodzenie systemu pomiarowego	Uszkodzenie zbiornika (wybuch)	BPCS	Nieakceptowalne		Poprawić niezawodność pętli pomiarowej Zainstalować osobny system pomiarowy i odcinający	MŚ

Klasy ryzyka określono w następujący sposób: IV – ryzyko pomijalne; III – ryzyko tolerowalne, jeśli koszt zmniejszenia ryzyka przewyższałby uzyskaną poprawę; II – ryzyko niepożądane i tolerowalne tylko wówczas, gdy zmniejszenie ryzyka jest niewykonalne lub koszty tego zmniejszenia są rażąco nieproporcjonalne do osiągniętej poprawy; I – ryzyko nietolerowane.

Tablica 3.4

Jakościowy ranking ryzyka [8, 114]

Ryzyko		**Konsekwencje**			
		krytyczne	wysokie	średnie	minimalne
Częstość	częste	I	I	II	III
	prawdopodobne	I	II	II	III
	sporadyczne	I	II	III	IV
	mało prawdopodobne	II	III	IV	IV

Do przykładowej oceny ryzyka wybrano zdarzenie awaryjne – zbyt duże ciśnienie w reaktorze. Może ono spowodować bardzo poważne konsekwencje z punktu widzenia strat ludzkich. Na podstawie analizy takich czynników, jak m.in. średnie zaludnienie terenu objętego zagrożeniem czy też typ wybuchu, jego zakres, szkodliwość substancji (chmury gazu i dymu) oraz kierunki i siła wiatrów, oszacowano, że zdarzenie to może być przyczyną zgonu bardzo wielu osób. Nanosząc te informacje na przedziały kryterialne parametru konsekwencji C, otrzymuje się wartość C_D.

Prawdopodobieństwo przebywania na terenie objętym zagrożeniem osób narażonych na działanie zdarzenia awaryjnego oszacowano na częste do stałego ($F \Rightarrow F_B$).

Po przeanalizowaniu złożoności procesu, w tym szybkości rozprzestrzeniania się zagrożenia, i biorących w nim udział substancji możliwość uniknięcia konsekwencji wybuchu oceniono jako minimalną ($P \Rightarrow P_B$).

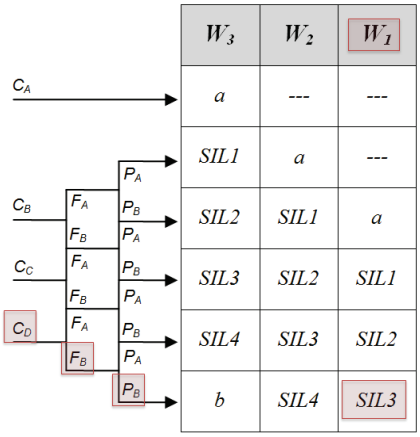
Ustalono, że prawdopodobieństwo wystąpienia zdarzenia awaryjnego bez stosowania jakichkolwiek systemów związanych z bezpieczeństwem (wykonanych w technice E/E/PE lub innych), lecz z udziałem wszystkich zewnętrznych sposobów zmniejszających ryzyko, jest bardzo małe. Wzięto pod uwagę m.in. niezawodność urządzeń BPCS, istnienie systemu alarmowego oraz działania operatorów. Stąd wybór przedziału $W \Rightarrow W_1$.

Wszystkie powyższe spostrzeżenia pozwalają na ich naniesienie bezpośrednio na parametry tworzące graf ryzyka, który został wcześniej odpowiednio skalibrowany na potrzeby analizowanej instalacji. Na tej podstawie można uzyskać wymagany stopień redukcji ryzyka, powiązany bezpośrednio z wymaganym poziomem nienaruszalności bezpieczeństwa SIL3. Zobrazowano to na rys. 3.8 oraz 3.9. Struktura sprzętowa realizująca analizowaną funkcję bezpieczeństwa będzie musiała spełnić właśnie takie wymagania.

parametry ryzyka

Scenariusz awaryjny	Konsekwencje	Przyczyny	Istniejące zabezpieczenia	C	F	P	W	SIL	Wymagane akcje
Zbyt duże ciśnienie w reaktorze	Uszkodzenie zbiornika	Uszkodzenie systemu pomiarowego	BPCS	C_D	F_B	P_B	W_1	SIL3	Poprawić niezawodność pętli pomiarowej Zainstalować osobny system pomiarowy i odcinający

Rys. 3.8. Wynik oceny ryzyka – widok tabelaryczny [8, 13]



Rys. 3.9. Wynik oceny ryzyka przedstawiony na grafie [15, 17]

Dokumenty normatywne [161, 162] wprowadzają oparte na analizie ryzyka podejście do określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla funkcji bezpieczeństwa, podając przy tym pewne przykłady metod wykorzystywanych w tym celu. Koncepcja ta odnosi się do wymagań technicznych dla systemu związanego z bezpieczeństwem. Opisywane normy dostarczają również informacji ogólnych na temat podstawowej koncepcji ryzyka i powiązania ryzyka z poziomami nienaruszalności bezpieczeństwa wraz z przedstawieniem wykorzystywanego modelu ryzyka.

3.7. Podsumowanie

Niniejszy rozdział nawiązuje do zagadnień związanych z etapem określania wymagań nienaruszalności bezpieczeństwa SIL dla zidentyfikowanych funkcji bezpieczeństwa. Wymagania dotyczące funkcji bezpieczeństwa SIF dzielą się na dwie podstawowe grupy: wymagania funkcjonalne oraz wymagania dotyczące nienaruszalności bezpieczeństwa. Pierwsza z nich definiuje zadania funkcji bezpieczeństwa oraz pewne założenia funkcjonalne dla rozwiązań sprzętowych, które będą implementowały te funkcje. Druga grupa dotyczy bezpośrednio określenia wymaganego poziomu nienaruszalności bezpieczeństwa SIL. W rozdziale tym zaprezentowano metodykę realizacji specyfikacji bezpieczeństwa oraz oceny ryzyka nakierowanej na określanie wymagań SIL dla kolejnych funkcji związanych

z bezpieczeństwem, jak również przedstawiono narzędzia i metody stosowane w realizacji tego procesu.

Niezrozumienie idei stojącej za etapem analizy ryzyka, a także nieumiejętne posługiwanie się dostępnymi metodami służącymi tej analizie może się stać jedną z przyczyn występowania zdarzeń niebezpiecznych w systemach nowo projektowanych lub już istniejących. Analizując przypadki wystąpienia zdarzeń niebezpiecznych, można stwierdzić, że wielu z nich można było uniknąć [23, 37, 55, 62, 64, 99, 104]. Co ważne, zdecydowana większość tego typu zagrożeń (44%) wynikała z niepoprawnej lub niekompletnej specyfikacji bezpieczeństwa dla zbudowanego systemu [23, 206]. Specyfikacja taka składa się z opisu funkcjonalnego (czyli jakie zadania ma realizować taki system) oraz z opisu integralności (czyli jak dobrze potrafi wykonywać swoje zadania). Specyfikacja ta wynika bezpośrednio z rezultatów analizy i oceny ryzyka. Stąd wniosek, że należy zwracać szczególną uwagę na ten etap, będący częścią całościowej analizy bezpieczeństwa funkcjonalnego.

Dokumenty normatywne dotyczące tematyki bezpieczeństwa funkcjonalnego podają definicję systemu E/E/PE związanego z bezpieczeństwem jako systemu, który realizuje funkcje bezpieczeństwa konieczne do osiągnięcia lub utrzymania stanu bezpiecznego, który zapobiega przejściu procesu do stanu niebezpiecznego. Wiąże się to z zagadnieniem bezpieczeństwa funkcjonalnego, czyli określaniem wymagań dla funkcji bezpieczeństwa, ich specyfikacji technicznej oraz wymaganych poziomów nienaruszalności bezpieczeństwa. Poziomy te należy następnie zweryfikować dla zaprojektowanej architektury systemu E/E/PE realizującej funkcje bezpieczeństwa. Zagadnienie to jest bardzo rozbudowane – dotyczy wielu aspektów wiedzy technicznej oraz eksperckiej.

Analizę bezpieczeństwa należy przeprowadzać według wcześniej zdefiniowanych procedur, aby cały proces był wyczerpujący, dobrze zorganizowany oraz odpowiednio zarządzany. Poczynając od analizy zagrożeń, poprzez identyfikację funkcji bezpieczeństwa, ocenę ryzyka oraz wyznaczenie wymaganego poziomu redukcji ryzyka, uzyskuje się wymagania, jakie zostaną postawione projektowanemu systemowi związanemu z bezpieczeństwem. Ocena ryzyka może dotyczyć strat wiążących się z utratą zdrowia lub życia pracowników i osób postronnych, szkodami majątkowymi oraz szkodami w środowisku naturalnym. Jest to więc bardzo ważne zagadnienie w procesie analizy bezpieczeństwa.

Dostępne i opisane w literaturze przedmiotu metody, m.in. graf ryzyka, służące do określania wymaganego poziomu SIL dla funkcji bezpieczeństwa mogą być bezpośrednio wykorzystywane w analizach konkretnych systemów. Źle zastosowane i skalibrowane na niewłaściwą wartość ryzyka tolerowanego mogą prowadzić do zbyt rygorystycznych lub – co gorsze – do zbyt optymistycznych rezultatów.

Jednocześnie należy także pamiętać o nowo powstałych zagrożeniach, których dotąd nie uwzględniało się w analizach, a których zajście w dzisiejszych czasach okazuje się coraz bardziej możliwe (np. działania terrorystyczne, a w szczególności cyberataki itp.) [74, 75, 118, 187, 212]. Stanowią one nowe wyzwanie, co skutkuje badaniami mającymi na celu opracowanie nowych lub rozszerzenie już istniejących rozwiązań służących analizie bezpieczeństwa funkcjonalnego [7, 17, 18]. Dzięki nim w analizach będą mogły być uwzględniane wszelkie nowe formy zagrożeń, co zapewne przyczyni się do znacznego wzrostu poziomu bezpieczeństwa w obiektach i systemach infrastruktury krytycznej. Podejście to zostanie rozwinięte w kolejnych rozdziałach niniejszej monografii.

Rozdział 4

WERYFIKACJA POZIOMÓW NIENARUSZALNOŚCI BEZPIECZEŃSTWA SIL

4.1. Wprowadzenie

Funkcje związane z bezpieczeństwem są realizowane przez systemy sterowania i zabezpieczeń zawierające elementy elektryczne, elektroniczne i programowalne elektroniczne (E/E/PE). Systemy te są jednym ze środków pozwalających na zmniejszenie ryzyka pochodzącego od instalacji technicznej i procesu. Istnieje problem właściwego zaprojektowania systemu E/E/PE realizującego funkcje związane z bezpieczeństwem. Problematyka dotycząca weryfikacji poziomów nienaruszalności bezpieczeństwa SIL zawarta jest w części szóstej normy PN-EN 61508 oraz w normach sektorowych PN-EN 61511 i PN-EN 62061.

Do weryfikacji SIL systemów E/E/PE oraz SIS realizujących funkcje bezpieczeństwa normy PN-EN 61508, PN-EN 61511 oraz PN-EN 62061 proponują metody jakościowe i ilościowe [161, 162, 166]. Należy jednak zaznaczyć, że metody jakościowe mogą być stosowane jedynie w zgrubnej ocenie systemu, w przypadku braku danych niezawodnościowych. Metody ilościowe pozwalają na weryfikację poziomu nienaruszalności bezpieczeństwa w warunkach posiadania danych niezawodnościowych analizowanego systemu [14, 15, 124, 195–201]. Dane te są zwykle fragmentaryczne i obarczone niepewnością, nie tylko na etapie projektowania systemu, ale również w początkowej fazie jego eksploatacji [6, 15, 17, 18, 25, 155, 191, 194].

Według przykładów zawartych w normie PN-EN 61508 wyniki uzyskane dla przykładowych kategorii systemów stanowią punktowe wartości prawdopodobieństw, które mogą się znajdować w pobliżu dolnej lub górnej granicy przedziału odpowiadającego danemu poziomowi SIL. Powstaje zatem pytanie, czy wyznaczony poziom SIL dla systemu E/E/PE spełnia wymagania danej kategorii [192, 195, 198]. Metoda ilościowa weryfikacji poziomów nienaruszalności bezpieczeństwa SIL systemów E/E/PE i SIS powinna być uzupełniona analizą wrażliwości i niepewności modelu probabilistycznego, ponieważ zarówno przyjęte wartości dotyczące parametrów modelu, jak i sama jego postać mogą istotnie wpływać na uzyskane wyniki [14, 17, 18, 77, 79, 198].

4.2. Modelowanie probabilistyczne systemów E/E/PE i SIS realizujących funkcje związane z bezpieczeństwem

Poszczególnym poziomom SIL projektowanego systemu E/E/PE odpowiadają ilościowe kryteria probabilistyczne. W analizie bezpieczeństwa funkcjonalnego kluczowe znaczenie ma określenie poziomu nienaruszalności bezpieczeństwa SIL dla obiektu (instalacji) podwyższonego ryzyka, a następnie zaprojektowanie takiego systemu zabezpieczeniowego, który spełni te wymagania. Dowód spełnienia przez system zabezpieczeniowy wymagań dotyczących określonego poziomu nienaruszalności bezpieczeństwa SIL nazywa się weryfikacją [155, 161, 162].

Model probabilistyczny dowolnego systemu sterowania lub zabezpieczeń można przedstawić za pomocą schematów blokowych niezawodności RBD, grafów Markowa, równań uproszczonych oraz drzew niezdatności FTA z wykorzystaniem struktury ścieżek lub cięć minimalnych [14, 17, 18, 139, 198]. W przypadku gdy system rozpatrywany jest z punktu widzenia jego uszkadzalności, wygodnym podejściem jest skorzystanie z metody cięć minimalnych.

Prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez system zabezpieczeniowy realizujący funkcje związane z bezpieczeństwem można określić na podstawie zależności [15, 17, 18, 198]:

$$\begin{gathered} PFD(t) \cong (1-e^{-\lambda_D \cdot t}) \cong 1-1+\lambda_D \cdot t-\frac{\lambda_D^2 \cdot t^2}{2!}+\frac{\lambda_D^3 \cdot t^3}{3!}+... \\ \text{przy} \quad \lambda_D \cdot t << 1 \\ PFD(t) \cong (1-e^{-\lambda_D \cdot t}) \cong \lambda_D \cdot t \end{gathered} \tag{4.1}$$

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

Wykorzystując zależność (4.1), można określić przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie, zakładając, że poszczególne podsystemy są testowane z czasem T_I między testami okresowymi, mającymi na celu wykrycie uszkodzeń niebezpiecznych [161]:

$$PFD_{avg} = \frac{1}{T_I}\int_0^{T_I} PFD(t)dt \tag{4.2}$$

gdzie: T_I – interwał przeprowadzania testów okresowych.

Średnia częstość występowania uszkodzenia niebezpiecznego na godzinę PFH może zostać oszacowana na podstawie wzoru [79, 161]:

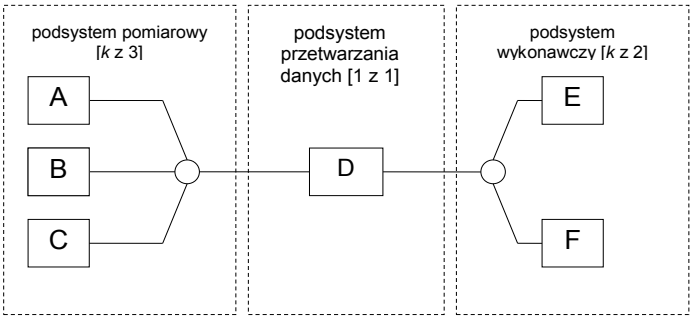
$$\begin{gathered} PFH \cong \frac{F(t)}{t} \underset{t\in(0,T)}{\Longrightarrow} \frac{F(T)}{T} \\ PFH \cong \frac{1-R(T)}{T} = 1-\frac{\exp(-\int_0^T \lambda(t)dt}{T} = \frac{1-\exp(-\lambda_{avg} \cdot T)}{T} \\ gdy \quad \lambda_{avg} \cdot T << 1 \\ PFH \cong \frac{\lambda_{avg} \cdot T}{T} = \lambda_{avg} \end{gathered} \tag{4.3}$$

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

Architektura sprzętu realizującego funkcję bezpieczeństwa jest przedstawiana za pomocą schematów blokowych z wyróżnieniem podsystemów i modułów. Przykładową postać fizyczną struktury systemu E/E/PE (BPCS lub SIS) zaprezentowano na rys. 4.1 [161, 197, 198].

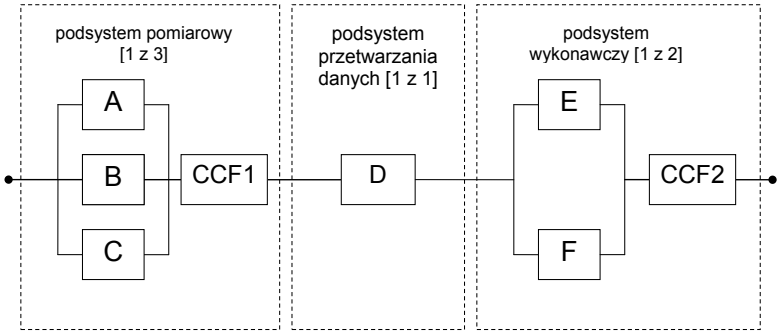
W systemie E/E/PE BPCS lub SIS wyróżnia się trzy podsystemy: pomiarowy, przetwarzania danych oraz wykonawczy. Przedstawiona struktura składa się z trzech czujników

A, B, C konfiguracji *k* z 3, podsystemu logicznego D (np. sterownika PLC) oraz elementów wykonawczych E oraz F (*k* z 2) [17, 161, 197].



Rys. 4.1. Przykładowa struktura systemu E/E/PE (SIS lub BPCS)

Na rys. 4.2 przedstawiono przykładową strukturę systemu E/E/PE lub SIS w postaci schematu blokowego niezawodności, przy założeniu, że podsystem pomiarowy posiada konfigurację 1 z 3, a podsystem wykonawczy – konfigurację 1 z 2.

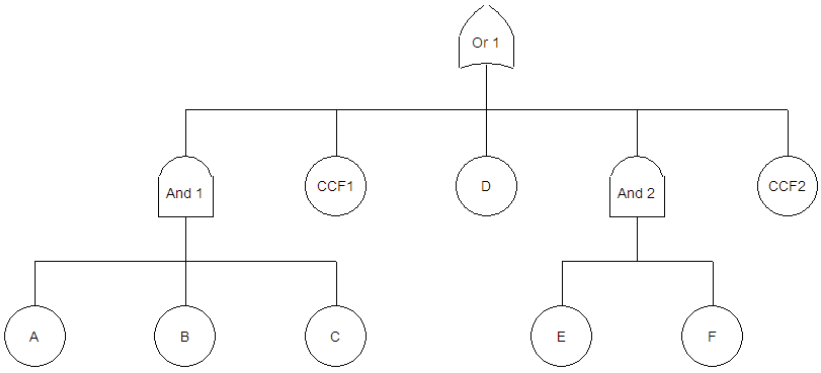


Rys. 4.2. Schemat blokowy niezawodności RBD przykładowej struktury systemu E/E/PE lub SIS

Na powyższym schemacie uwzględniono uszkodzenia o wspólnej przyczynie CCF (common cause failure) dla podsystemu pomiarowego CCF1 od elementów A, B i C oraz dla podsystemu wykonawczego CCF2 od elementów E i F. W systemie z rys. 4.2 można wyróżnić pięć cięć minimalnych:

$$\{A, B, C\};\ \{CCF1\};\ \{D\};\ \{E, F\};\ \{CCF2\}$$

Na rys. 4.3 przedstawiono drzewo niezdatności systemu E/E/PE lub SIS z rys. 4.2 z uwzględnieniem uszkodzeń o wspólnej przyczynie.



Rys. 4.3. Drzewo niezdatności systemu E/E/PE lub SIS

Przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie dla systemu z rys. 4.2 można wyznaczyć na podstawie sumy prawdopodobieństw dla poszczególnych podsystemów [161, 162, 197]:

$$PFD_{\text{avg}} \cong PFD_{\text{avg}}^{\text{ABC}} + PFD_{\text{avg}}^{\text{CCF1}} + PFD_{\text{avg}}^{\text{D}} + PFD_{\text{avg}}^{\text{EF}} + PFD_{\text{avg}}^{\text{CCF2}} \tag{4.4}$$

gdzie: $PFD_{\text{avg}}^{\text{ABC}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie przez podsystem pomiarowy; $PFD_{\text{avg}}^{\text{CCF1}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa o wspólnej przyczynie CCF1 dla elementów podsystemu pomiarowego; $PFD_{\text{avg}}^{\text{D}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie przez podsystem przetwarzania danych; $PFD_{\text{avg}}^{\text{EF}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie przez podsystem wykonawczy; $PFD_{\text{avg}}^{\text{CCF2}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa o wspólnej przyczynie CCF2 dla elementów podsystemu wykonawczego.

Analogicznie, średnia częstość występowania uszkodzenia niebezpiecznego na godzinę *PFH* (dla systemu pracującego w trybie częstego przywołania lub ciągłym) wynosi [124, 161, 162, 197, 198]:

$$PFH \cong PFH^{\text{ABC}} + PFH^{\text{CCF1}} + PFH^{\text{D}} + PFH^{\text{EF}} + PFH^{\text{CCF2}} \tag{4.5}$$

Korzystając z metody cięć minimalnych, przy określaniu prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie $PFD(t)$, a następnie wartości PFD_{avg} i PFH można zaproponować dwa podejścia. Pierwsze bazuje na klasycznej metodzie uwzględnienia uszkodzeń zależnych, w której odsetek uszkodzeń niewykrytych β spowodowanych wspólną przyczyną, uwzględniony w modelu probabilistycznym, wiąże się ze schematem zastępczym rozpatrywanego układu. Drugie podejście uwzględnia uszkodzenia spowodowane wspólną przyczyną w sposób wynikający z drzewa niezdatności rozpatrywanego podsystemu [76, 77, 161, 197, 198].

4.3. Miary i wskaźniki probabilistyczne oraz dane niezawodnościowe

W modelowaniu probabilistycznym systemów związanych z bezpieczeństwem podstawowym parametrem jest intensywność uszkodzeń λ, która dzieli się na intensywność uszkodzeń bezpiecznych λ_S oraz intensywność uszkodzeń niebezpiecznych λ_D. Relację pomiędzy intensywnością uszkodzeń bezpiecznych a całkowitą intensywnością uszkodzeń ilustruje parametr *FS* (współczynnik uszkodzeń bezpiecznych):

$$FS = \frac{\lambda_S}{\lambda} = \frac{\lambda - \lambda_D}{\lambda} = 1 - \frac{\lambda_D}{\lambda} \tag{4.6}$$

gdzie: λ – intensywność uszkodzeń; λ_S – intensywność uszkodzeń bezpiecznych; λ_D – intensywność uszkodzeń niebezpiecznych.

Jeżeli brakuje danych niezawodnościowych dla podsystemów sterowania lub zabezpieczeniowych, zakłada się, że współczynnik uszkodzeń bezpiecznych $FS = 50\%$ [161]. W takim przypadku intensywność uszkodzeń niebezpiecznych jest równa intensywności uszkodzeń bezpiecznych, co w efekcie powoduje, że każda z nich stanowi połowę całkowitej intensywności uszkodzeń rozpatrywanego elementu/ podsystemu [161].

$$\lambda_D = \lambda_S = \frac{\lambda}{2} \tag{4.7}$$

Bardzo ważnym parametrem z punktu widzenia analiz bezpieczeństwa funkcjonalnego jest odsetek błędów bezpiecznych *SFF*, wyrażony zależnością:

$$SFF = \frac{\lambda_{DD} + \lambda_S}{\lambda} \tag{4.8}$$

gdzie: λ_{DD} – intensywność uszkodzeń niebezpiecznych wykrywalnych przez testy diagnostyczne.

Intensywności uszkodzeń niebezpiecznych i bezpiecznych można podzielić na wykrywalne i niewykrywalne przez testy diagnostyczne. Intensywność uszkodzeń niebezpiecznych dzieli się na intensywność uszkodzeń niebezpiecznych niewykrywalnych przez testy diagnostyczne λ_{DU} oraz na intensywność uszkodzeń niebezpiecznych wykrywalnych poprzez testy diagnostyczne λ_{DD}. Natomiast intensywność uszkodzeń bezpiecznych dzieli się na intensywność uszkodzeń bezpiecznych niewykrywalnych w testach diagnostycznych λ_{SU} oraz intensywność uszkodzeń bezpiecznych wykrywalnych przez testy diagnostyczne λ_{SD}.

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \tag{4.9}$$

$$\lambda_S = \lambda_{SU} + \lambda_{SD} \tag{4.10}$$

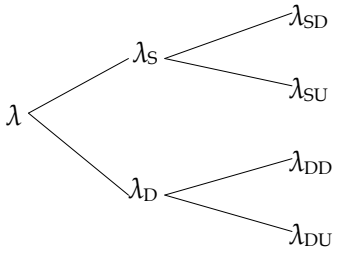
Zatem całkowita intensywność uszkodzeń ma postać:

$$\lambda = \lambda_{DU} + \lambda_{DD} + \lambda_{SU} + \lambda_{SD} \tag{4.11}$$

gdzie: λ_{DU} – intensywność uszkodzeń niebezpiecznych niewykrywalnych w testach diagnostycznych; λ_{DD} – intensywność uszkodzeń niebezpiecznych wykrywalnych przez testy diagnostyczne; λ_{SU} – intensywność uszkodzeń bezpiecznych niewykrywalnych w testach dia-

gnostycznych; λ_{SD} – intensywność uszkodzeń bezpiecznych wykrywalnych poprzez testy diagnostyczne.

Na rys. 4.4 przedstawiono w sposób symboliczny rozkład intensywności uszkodzeń λ na cztery składowe: $\lambda_{DU}, \lambda_{DD}, \lambda_{SU}, \lambda_{SD}$.



Rys. 4.4. Podział intensywności uszkodzeń λ rozpatrywanego podsystemu na składowe

Uzyskanie poszczególnych składowych całkowitej intensywności uszkodzeń jest możliwe dzięki współczynnikowi pokrycia diagnostycznego *DC* (*diagnostic coverage*):

$$DC = \frac{\lambda_{DD}}{\lambda_D} \Rightarrow \lambda_{DD} = DC \cdot \lambda_D \tag{4.12}$$

$$DC = \frac{\lambda_{SD}}{\lambda_S} \Rightarrow \lambda_{SD} = DC \cdot \lambda_S \tag{4.13}$$

Dysponując pokryciem diagnostycznym *DC*, można określić wartości pozostałych intensywności uszkodzeń $\lambda_{DU}, \lambda_{SU}$:

$$\lambda_{DU} = (1 - DC)\lambda_D \tag{4.14}$$

$$\lambda_{SU} = (1 - DC)\lambda_S \tag{4.15}$$

gdzie: *DC* – współczynnik pokrycia diagnostycznego.

Dysponując λ oraz jej składowymi $\lambda_{DU}, \lambda_{DD}, \lambda_{SU}, \lambda_{SD}$, można przystąpić do wyznaczania przeciętnego prawdopodobieństwa niewykonania funkcji bezpieczeństwa na żądanie PFD_{avg} oraz średniej częstości wystąpienia uszkodzenia niebezpiecznego na godzinę dla systemu pracującego w sposób ciągły lub na częste przywołanie *PFH*. Poszczególne intensywności uszkodzeń można także uzyskać na podstawie przeprowadzonej analizy rodzajów, skutków i krytyczności uszkodzeń FMECA. Analiza FMECA pozwala oszacować współczynniki *FS*, *SFF* oraz *DC* [14, 195, 198]. W tablicy 4.1 znajduje się przykładowy zestaw danych niezawodnościowych elementów systemów związanych z bezpieczeństwem. Dane te zostały opracowane na podstawie bazy danych niezawodnościowych OREDA oraz poradników SINTEF [69, 70, 71, 197].

Niektóre bazy danych niezawodnościowych podają jako podstawowe parametry intensywność uszkodzeń niebezpiecznych niewykrywalnych przez testy diagnostyczne λ_{DU} oraz odsetek błędów bezpiecznych *SFF*. Poniższa zależność przedstawia relację pomiędzy współczynnikiem pokrycia diagnostycznego *DC* oraz a wskaźnikami *SFF* i *FS*:

$$DC = \frac{SFF - FS}{100 - FS}\% \tag{4.16}$$

Tablica 4.1

Dane niezawodnościowe dla przykładowych elementów systemów E/E/PE

Element	λ_{DU} [h^{-1}]	*SFF* [%] odsetek uszkodzeń bezpiecznych	T_I [h]	β^* udział uszkodzeń niewykrytych, które mają wspólną przyczynę	PFD_{avg}
Czujniki					
Czujnik ciśnienia	$0{,}3\cdot10^{-6}$	77	8760	2%	$1{,}3\cdot10^{-3}$
Czujnik poziomu	$0{,}6\cdot10^{-6}$	80	8760	2%	$2{,}6\cdot10^{-3}$
Czujnik temperatury	$0{,}3\cdot10^{-6}$	83	8760	2%	$1{,}3\cdot10^{-3}$
Detektory					
Detektor dymu	$0{,}8\cdot10^{-6}$	78	4380	5%	$1{,}8\cdot10^{-3}$
Detektor ciepła	$0{,}5\cdot10^{-6}$	79	4380	5%	$1{,}1\cdot10^{-3}$
Detektor płomieni	$1{,}6\cdot10^{-6}$	80	4380	5%	$3{,}5\cdot10^{-3}$
Detektor gazu, katalityczny	$1{,}8\cdot10^{-6}$	64	4380	5%	$3{,}9\cdot10^{-3}$
Systemy logiczne					
Sterownik PLC	$4{,}1\cdot10^{-6}$	95	8760	1%	$1{,}8\cdot10^{-2}$
Sterownik *safety* PLC	$2{,}2\cdot10^{-8}$	99,5	8760	1%	$9{,}64\cdot10^{-5}$
SRS	$8\cdot10^{-8}$	99,5	8760	1%	$3{,}5\cdot10^{-4}$
Elementy wykonawcze					
ESV/XV element wykonawczy	$2{,}0\cdot10^{-6}$	62	8760	2%	$8{,}8\cdot10^{-3}$
Zawór pneumatyczny	$2{,}0\cdot10^{-6}$	62	8760	2%	$8{,}8\cdot10^{-3}$
Zawór WV	$0{,}8\cdot10^{-6}$	62	8760	2%	$3{,}5\cdot10^{-3}$
Zawór MV	$0{,}8\cdot10^{-6}$	62	8760	2%	$3{,}5\cdot10^{-3}$

* Odnosi się wyłącznie do podsystemów z nadmiarowością strukturalną *k* z *n*, zbudowaną na bazie elementów wymienionych w tablicy (np. dwa jednakowe czujniki ciśnienia pracujące w konfiguracji 1 z 2).

Przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na żądanie oraz średnią częstość występowania uszkodzenia niebezpiecznego na godzinę należy traktować jako funkcję pięciu zmiennych [124, 161, 195, 197, 198]:

$$\begin{aligned} PFD_{avg} &= f(T_I, DC, MTTR, \beta, \lambda) \\ PFH &= f(T_I, DC, MTTR, \beta, \lambda) \end{aligned} \tag{4.17}$$

gdzie: T_I – interwał przeprowadzania testów okresowych; DC – współczynnik pokrycia diagnostycznego; MTTR – średni czas naprawy; β – udział uszkodzeń niewykrytych, które mają wspólną przyczynę; λ – intensywność uszkodzeń.

Pomocnym wskaźnikiem w procesie weryfikacji SIL jest procentowy stosunek wartości PFD_{avgi} lub PFH_i podsystemu/ elementu do ogólnej wartości PFD_{avgsys} bądź PFH_{sys} wyznaczonej dla części sprzętowej systemu realizującego funkcje bezpieczeństwa [197]:

$$x_i = \frac{PFD_{avgi}(PFH)_i}{PFD_{avgsys}(PFH)_{sys}} \cdot 100\% \tag{4.18}$$

gdzie: x_i – wskaźnik procentowego stosunku wartości prawdopodobieństwa i-tego podsystemu/ elementu do całkowitej wartości prawdopodobieństwa systemu; PFD_{avgi} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie dla i-tego podsystemu/ elementu; PFH_i – średnia częstość występowania uszkodzenia niebezpiecznego na godzinę dla i-tego podsystemu/ elementu; PFD_{avgsys} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie dla systemu; PFH_{sys} – średnia częstość występowania uszkodzenia niebezpiecznego na godzinę dla systemu.

Dane niezawodnościowe są takie same dla wszystkich modeli probabilistycznych, bez względu na rodzaj metody zastosowanej do ich wyznaczenia (PN-EN 61508 oraz CM (cięć minimalnych)) [161, 195, 198].

4.4. Modele probabilistyczne elementów i podsystemów systemów E/E/PE i SIS

Dysponując danymi niezawodnościowymi elementów, z których zbudowana jest warstwa sprzętowa realizująca funkcje bezpieczeństwa, można obliczyć wartości prawdopodobieństw PFD_{avg} oraz PFH na podstawie gotowych modeli probabilistycznych zawartych w szóstej części normy PN-EN 61508 [161]. Poniżej przedstawiono modele probabilistyczne (wg PN-EN 61508) dla podstawowych struktur podsystemów [161]. Należy zwrócić uwagę na fakt, że zaprezentowane modele probabilistyczne mają zastosowanie do podsystemów składających się z jednakowych elementów.

Uzyskane wartości prawdopodobieństw mają charakter punktowy; duży wpływ na finalny rezultat może mieć uwzględnienie zagadnień niepewności [6, 15, 17, 192]. Chcąc zamodelować system, którego podsystemy składają się z różnych elementów, pochodzących od różnych producentów, należy wykorzystać inne techniki analiz niezawodnościowych. Można do nich zaliczyć metodę drzewa niezdatności FTA i metodę schematów blokowych niezawodności RBD. Najbardziej efektywną metodą modelowania probabilistycznego systemów E/E/PE lub SIS będzie wówczas wykorzystanie techniki cięć minimalnych przy określaniu prawdopodobieństwa $PFD(t)$, a następnie wartości PFD_{avg} i PFH.

Struktura 1 z 1:
(wg PN-EN 61508-6) [161]:

$$PFD_{avg1z1} \cong \lambda_D \cdot t_{CE} \tag{4.19}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_I}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{4.20}$$

$$PFH_{1z1} \cong \lambda_{DU} \tag{4.21}$$

gdzie: t_{CE} – średni czas przestoju wyposażenia kanału (wyrażony w godzinach), odnoszący się do architektur 1 z 1, 1 z 2, 2 z 2 oraz 2 z 3 (jest to łączny czas przestoju wszystkich elementów w kanale podsystemu); T_I – interwał przeprowadzania testów okresowych; $MTTR$ – średni czas naprawy; λ_D – intensywność uszkodzeń niebezpiecznych; λ_{DU} – intensywność uszkodzeń niebezpiecznych niewykrywalnych.

Struktura 1 z 2:
(wg PN-EN 61508-6):

$$PFD_{avg1z2} \cong 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU}\left(\frac{T_I}{2} + MTTR\right) \tag{4.22}$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_I}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{4.23}$$

$$\beta = 2 \cdot \beta_D \tag{4.24}$$

$$PFH_{1z2} \cong 2[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \tag{4.25}$$

gdzie: β – udział uszkodzeń niewykrytych, które mają wspólną przyczynę; β_D – udział uszkodzeń wykrytych, które mają wspólną przyczynę; t_{GE} – średni czas przestoju wyposażenia grupy głosowania (wyrażony w godzinach), odnoszący się do architektur 1 z 2 oraz 2 z 3.

Struktura 2 z 2:
(wg PN-EN 61508-6):

$$PFD_{avg2z2} \cong 2 \cdot \lambda_D \cdot t_{CE} \tag{4.26}$$

$$PFH_{2z2} \cong 2 \cdot \lambda_{DU} \tag{4.27}$$

Struktura 2 z 3:
(wg PN-EN 61508-6):

$$PFD_{avg2z3} \cong 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU}\left(\frac{T_I}{2} + MTTR\right) \tag{4.28}$$

$$PFH_{2z3} \cong 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^2 t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \tag{4.29}$$

Struktura 1 z 2D (z wewnętrznym testowaniem diagnostycznym):
(wg PN-EN 61508-6):

$$\begin{aligned} PFD_{avg1z2D} \cong\ & 2(1-\beta)\lambda_{DU}[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU} + \lambda_{SD}]t_{CE'} \cdot t_{GE'} + \\ & + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU}\left(\frac{T_I}{2} + MTTR\right) \end{aligned} \tag{4.30}$$

$$t_{CE'} = \frac{\lambda_{DU}(\frac{T_I}{2} + MTTR) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}} \quad gdzie: \quad \lambda_{SD} = \frac{\lambda}{2} DC \tag{4.31}$$

$$t_{GE'} = \frac{\lambda_{DU}(\frac{T_I}{3} + MTTR) + (\lambda_{DD} + \lambda_{SD})MTTR}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}} \tag{4.32}$$

gdzie: $t_{CE'}$ – średni czas przestoju wyposażenia kanału (wyrażony w godzinach), odnoszący się do architektury 1 z 2D; $t_{GE'}$ – średni czas przestoju wyposażenia grupy głosowania (wyrażony w godzinach), odnoszący się do architektury 1 z 2D.

$$PFH_{1z2D} \cong 2(1-\beta)\lambda_{DU}[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU} + \lambda_{SD}]t_{CE'} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \tag{4.33}$$

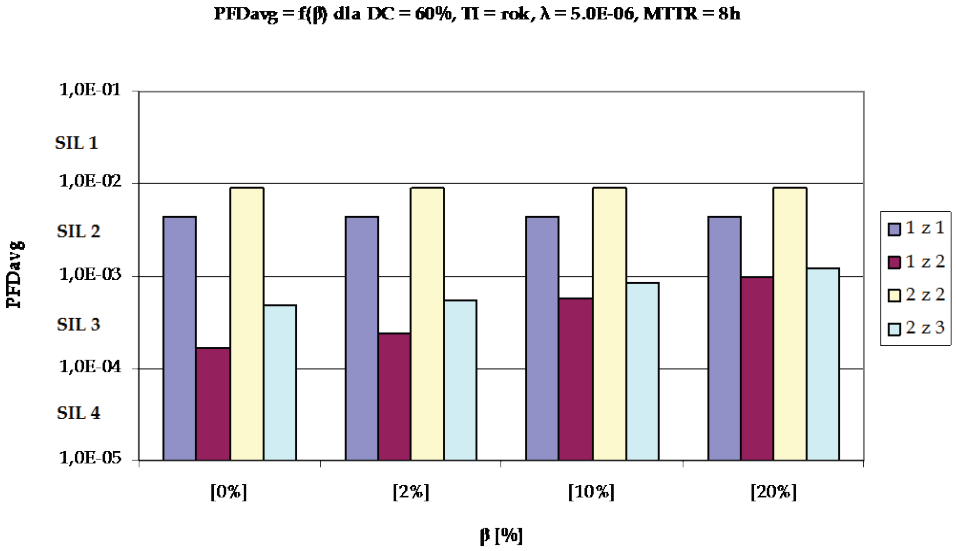
Struktura 1 z 3:
(wg PN-EN 61508-6):

$$PFD_{avg1z3} \cong 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^3 t_{CE} \cdot t_{GE} \cdot t_{G2E} + \beta_D \cdot \lambda_{DD} \cdot MTTR + \beta \cdot \lambda_{DU}(\frac{T_I}{2} + MTTR) \tag{4.34}$$

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}(\frac{T_I}{4} + MTTR) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{4.35}$$

$$PFH_{1z3} \cong 6[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}]^3 t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} \tag{4.36}$$

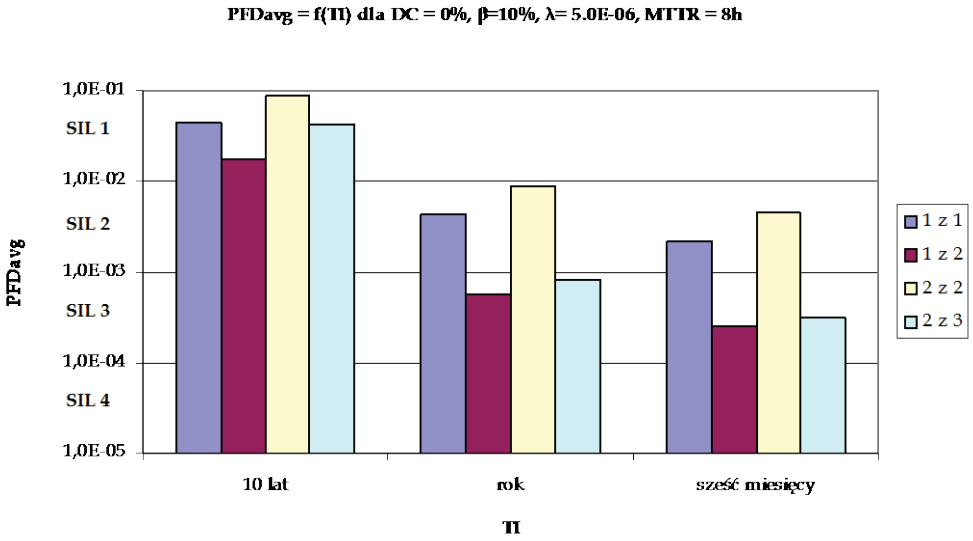
Na rys. 4.5 przedstawiono porównanie wartości przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania w funkcji udziału uszkodzeń niewykrytych β o wspólnej przyczynie wg PN-EN 61508, przy założeniu, że DC = 60%, T_I = 8760 [h] (rok), $\lambda = 5 \cdot 10^{-6}$ [h^{-1}] oraz $MTTR$ = 8 [h]. Porównanie zostało przeprowadzone dla czterech struktur k z n. Intensywności uszkodzeń pochodzą z PN-EN 61508 [161, 195, 198].



Rys. 4.5. PFD_{avg} w funkcji β, czyli udziału uszkodzeń niewykrytych, które mają wspólną przyczynę

Zwiększenie β, czyli udziału uszkodzeń niewykrytych, które mają wspólną przyczynę (dotyczy tylko architektur podsystemów E/E/PE z nadmiarowością strukturalną), powoduje wzrost wartości prawdopodobieństw PFD_{avg} (oraz *PFH*). Nieuwzględnienie udziału uszkodzeń niewykrytych, które mają wspólną przyczynę (reprezentowaną poprzez wskaźnik β), w modelowaniu probabilistycznym systemów E/E/PE może doprowadzić do tego, że uzyskane poziomy SIL będą zbyt optymistyczne. Rozpatrując konfigurację 1 z 2 przy $\beta = 0$, otrzymano SIL3; przy $\beta = 20\%$ ta sama architektura spełnia wymagania SIL2 (zatem poziom SIL zmalał z SIL3 na SIL2).

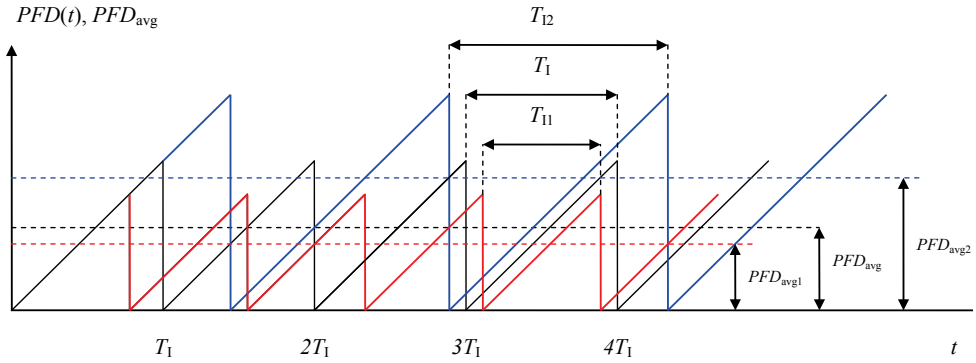
Na rys. 4.6 przedstawiono wpływ interwału pomiędzy testami okresowymi na wartość punktową prawdopodobieństwa PFD_{avg} dla czterech różnych konfiguracji nadmiarowych systemów E/E/PE i SIS.



Rys. 4.6. PFD_{avg} w funkcji czasu między testami okresowymi T_I

Im dłuższy przedział czasu między testami sprawdzającymi, tym większa wartość PFD_{avg} (*PFH*). Ważnym aspektem w procesie weryfikacji jest możliwość graficznej prezentacji przebiegów czasowych niewypełnienia funkcji bezpieczeństwa *PFD*(*t*). Wykreślając kilka przebiegów *PFD*(*t*) pojedynczego elementu systemu E/E/PE (konfiguracja 1 z 1) dla różnych przedziałów czasu pomiędzy testami sprawdzającymi T_I (rys. 4.7), można obserwować zmiany wartości prawdopodobieństwa PFD_{avg} w zależności od stosowanego interwału.

Wydłużenie okresów między testami sprawdzającymi wpływa na wzrost wartości punktowej przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie PFD_{avg} oraz wzrost wartości średniej częstości występowania uszkodzenia niebezpiecznego na godzinę *PFH* (tryb pracy ciągłej lub częstego przywołania do działania).



Rys. 4.7. Przebiegi trójkątne $PFD(t)$ oraz wartości przeciętne PFD_{avg} elementu systemu E/E/PE dla trzech okresów testowania ($T_{I1} < T_I < T_{I2}$)

4.5. Uszkodzenia o wspólnej przyczynie w modelowaniu probabilistycznym systemów E/E/PE i SIS

W modelowaniu probabilistycznym systemów E/E/PE z nadmiarowością strukturalną w procesie weryfikacji SIL należy uwzględnić wpływ uszkodzeń o wspólnej przyczynie poprzez zastosowanie wskaźnika β (modelu beta). Można wykorzystać różne sposoby przyjmowania wartości β, czyli udziału uszkodzeń niewykrytych, które mają wspólną przyczynę, w zależności od aktualnej architektury systemu nadmiarowego [66, 76, 79, 197]:

$$\beta_{kzn} = \beta \cdot C_{kzn} \tag{4.37}$$

gdzie: β_{kzn} – udział uszkodzeń niewykrytych, które mają wspólną przyczynę, dla struktury nadmiarowej k z n; β – udział uszkodzeń niewykrytych, które mają wspólną przyczynę, dla najprostszej struktury nadmiarowej 1 z 2 (wskaźnik bazowy); C_{kzn} – mnożnik uzależniony od rozpatrywanej architektury podsystemu, który wynosi, odpowiednio: $C_{1z2} = 1$, $C_{1z3} = 0{,}5$, $C_{2z3} = 1{,}5$.

Wartość bazowa β udziału uszkodzeń niewykrytych, które mają wspólną przyczynę, przyjmowana jest w zależności od podsystemu, z jakim aktualnie ma się do czynienia, oraz od tego, gdzie dany system ma zostać zainstalowany. W przypadku podsystemu logicznego, np. PLC, β mieści się w granicach: $0{,}5\% < \beta < 5\%$, dla układu czujników i elementów wykonawczych: $1\% < \beta < 10\%$, dla modułów wejść/ wyjść: $1\% < \beta < 50\%$. Wartości β określa się na podstawie systemu punktowego i tablic estymacji zawartych w części szóstej normy PN-EN 61508-6 oraz w normie PN-EN 62061 [161, 166].

W tablicy 4.2 przedstawiono sposób wyznaczania wartości udziału uszkodzeń niewykrytych, które mają wspólną przyczynę, dla struktur nadmiarowych β_{kzn} z wykorzystaniem bazowego wskaźnika β obliczonego na podstawie punktowych tablic estymacji (według norm PN-EN 61508 i 62061). Przyjęto wartość maksymalną $n = 5$.

Tablica 4.2

Wyznaczenie β_{kzn} udziału uszkodzeń niewykrytych, które mają wspólną przyczynę, dla struktur nadmiarowych k z n [161]

k* z *n		***n***			
		2	**3**	**4**	**5**
k	**1**	β	$0{,}5\beta$	$0{,}3\beta$	$0{,}2\beta$
	2	–	$1{,}5\beta$	$0{,}6\beta$	$0{,}4\beta$
	3	–	–	$1{,}75\beta$	$0{,}8\beta$
	4	–	–	–	β

Intensywność uszkodzeń λ elementu (podsystemu) o strukturze k z n jest sumą intensywności uszkodzeń niezależnych λ_I oraz zależnych λ_C:

$$\lambda = \lambda_I + \lambda_C \tag{4.38}$$

gdzie: λ_I – intensywność uszkodzeń niezależnych dla podsystemu z nadmiarowością strukturalną; λ_C – intensywność uszkodzeń zależnych dla podsystemu z nadmiarowością strukturalną.

Wskaźnik β określa równanie:

$$\beta = \frac{\lambda_C}{\lambda} \tag{4.39}$$

Biorąc pod uwagę równania (4.38) oraz (4.39), intensywność uszkodzeń zależnych wynosi:

$$\lambda_C = \beta \cdot \lambda \tag{4.40}$$

Zatem intensywność uszkodzeń niezależnych jest równa:

$$\lambda_I = (1-\beta) \cdot \lambda \tag{4.41}$$

Korzystając z intensywności uszkodzeń wyrażonych równaniami (4.40) oraz (4.41), prawdopodobieństwo uszkodzeń zależnych można wyznaczyć ze wzoru:

$$q_C(t) = \beta \cdot q(t) \tag{4.42}$$

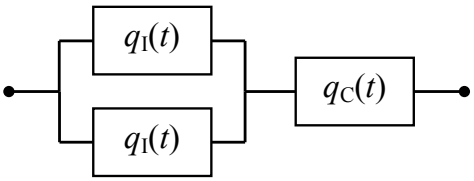
gdzie: $q_C(t)$ – prawdopodobieństwo uszkodzeń zależnych; β – udział uszkodzeń o wspólnej przyczynie; $q(t)$ – prawdopodobieństwo uszkodzenia elementu w strukturze nadmiarowej.

Prawdopodobieństwo uszkodzeń niezależnych można zaś opisać wzorem:

$$q_I(t) = (1-\beta) \cdot q(t) \tag{4.43}$$

gdzie: $q_I(t)$ – prawdopodobieństwo uszkodzeń niezależnych; β – udział uszkodzeń spowodowanych wspólną przyczyną; $q(t)$ – prawdopodobieństwo uszkodzenia elementu w strukturze nadmiarowej.

Na rys. 4.8 przedstawiono schemat blokowy systemu o strukturze 1 z 2 z uwzględnieniem uszkodzeń zależnych.



Rys. 4.8. Schemat blokowy niezawodności systemu o architekturze 1 z 2

Przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie dla struktury 1 z 2 z uwzględnieniem uszkodzeń o wspólnej przyczynie określa zależność [124, 197, 198]:

$$PFD_{\text{avg1z2}} \cong [(1-\beta)\lambda_D]^2(\frac{T_I^2}{3} + T_I \cdot MTTR + MTTR^2) + \beta \cdot \lambda_{DU}(\frac{T_I}{2} + MTTR) \tag{4.44}$$

Średnią częstość występowania uszkodzenia niebezpiecznego na godzinę dla struktury 1 z 2 po uwzględnieniu uszkodzeń niewykrytych, które mają wspólną przyczynę, można obliczyć ze wzoru:

$$PFH_{1z2} \cong 2[(1-\beta)\lambda_D]^2(\frac{T_I}{2} + MTTR) + \beta \cdot \lambda_{DU} \tag{4.45}$$

Zależności proponowane w normie PN-EN 61508 dotyczą jedynie przypadku, w którym poszczególne podsystemy układu sterowania/ zabezpieczeniowego składają się z jednakowych elementów, przykładowo – takich samych czujników, układów przetwarzania, elementów wykonawczych. Postać modelu probabilistycznego systemu sterowania lub zabezpieczeniowego znacznie się komplikuje, jeżeli poszczególne podsystemy składają się z *n* różnych elementów. Zależności proponowane przez PN-EN 61508 są więc w danym przypadku niewystarczające.

Zastosowanie metodyki bazującej na technice cięć minimalnych wyznaczonych dla rozpatrywanego systemu umożliwia zbudowanie modeli probabilistycznych przy dowolnej konfiguracji podsystemów złożonych z różnych elementów. Pojęcie różnych elementów w danym przypadku będzie równoznaczne z tym, że każdy z nich będzie się charakteryzował odmienną intensywnością uszkodzeń λ. W modelach probabilistycznych systemów, w których każdy element jest inny, tzn. takich, które cechują się różną intensywnością uszkodzeń, tak samo jak wcześniej ważnym parametrem jest wskaźnik β. Jednak zamodelowanie i uwzględnienie go w finalnej postaci modelu dla konkretnej struktury stwarza wiele problemów i nie jest zadaniem trywialnym. W przypadku modeli probabilistycznych systemów sterowania i zabezpieczeń dla struktur 1 z 2, 2 z 3, 4 z 6, *k* z *n*, przy założeniu, że $k < n$, należy uwzględnić wskaźnik β, którego model został przedstawiony poniżej.

Intensywność uszkodzeń systemu λ o strukturze nadmiarowej *k* z *n*, składającego się z *n* różnych elementów, można przedstawić w postaci sumy przeciętnej intensywności uszkodzeń niezależnych λ_{Iavg} oraz intensywności uszkodzeń zależnych λ_C [15, 76, 77, 79, 197, 198]:

$$\lambda = \lambda_{\text{Iavg}} + \lambda_C \tag{4.46}$$

gdzie: λ_{Iavg} – przeciętna intensywność uszkodzeń niezależnych.

Wskaźnik β ma postać:

$$\beta = \frac{\lambda_{\mathrm{C}}}{\lambda_{\mathrm{C}} + \lambda_{\mathrm{Iavg}}} = \frac{\lambda_C}{\lambda} \tag{4.47}$$

Wykorzystując (4.46) oraz (4.47), intensywność uszkodzeń zależnych można opisać równaniem:

$$\lambda_{\mathrm{C}} = \beta \cdot \lambda \tag{4.48}$$

Przeciętną intensywność uszkodzeń λ_{Iavg} można przedstawić w postaci:

$$\lambda_{\mathrm{Iavg}} = \frac{\sum_{i=1}^{n} \lambda_{\mathrm{I}i}}{n} = \frac{\sum_{i=1}^{n} (1-\beta)\lambda_i}{n} \tag{4.49}$$

gdzie: $\lambda_{\mathrm{I}i}$ – intensywność uszkodzeń niezależnych dla pojedynczego i-tego elementu; n – liczba elementów.

Uwzględniając zależności (4.48) i (4.49), intensywność uszkodzeń zależnych λ_{C} można opisać następująco:

$$\lambda_{\mathrm{C}} = \frac{\beta \cdot \lambda_{\mathrm{Iavg}}}{(1-\beta)} = \frac{\beta(\frac{\sum_{i=1}^{n} \lambda_{\mathrm{I}i}}{n})}{(1-\beta)} = \frac{\beta(1-\beta)(\frac{\sum_{i=1}^{n} \lambda_i}{n})}{(1-\beta)}$$

$$\lambda_{\mathrm{C}} = \beta(\frac{\sum_{i=1}^{n} \lambda_i}{n}) \tag{4.50}$$

Traktując wartość przeciętną intensywności uszkodzeń niezależnych $\lambda_{\mathrm{Iavg}}{}^{\mathrm{g}}$ jako średnią geometryczną, intensywność uszkodzeń zależnych można wyznaczyć ze wzoru:

$$\lambda_{\mathrm{C^g}} = \frac{\beta \cdot \lambda_{\mathrm{Iavg}}{}^{\mathrm{g}}}{(1-\beta)} = \frac{\beta \cdot \sqrt[n]{\lambda_{\mathrm{I1}} \cdot \lambda_{\mathrm{I2}} \cdot \ldots} \cdot \lambda_{\mathrm{I}n}}{(1-\beta)} = \frac{\beta \cdot (1-\beta) \cdot \sqrt[n]{\lambda_1 \cdot \lambda_2 \cdot \ldots} \cdot \lambda_n}{(1-\beta)}$$

$$\lambda_{\mathrm{C^g}} = \beta \cdot \sqrt[n]{\lambda_1 \cdot \lambda_2 \cdot \ldots} \cdot \lambda_n \tag{4.51}$$

Powyżej przedstawiono ogólny model β. Uwzględnienie w budowanym modelu uszkodzeń o wspólnej przyczynie ma zasadnicze znaczenie. W sytuacji gdy układ będzie się składał z takich samych elementów, powyższe zależności zostaną sprowadzone do postaci przedstawionej równaniami opisującymi przypadek dla jednakowych elementów. Do wyznaczania bazowej wartości β dla konfiguracji 1 z 2 można wykorzystać punktowe tablice estymacji według PN-EN 61508-6.

4.6. Wyznaczanie bazowej wartości β na podstawie punktowych tablic estymacji według PN-EN 61508

W przypadku korzystania z modelu opartego na współczynniku β w celu uwzględnienia w modelowaniu probabilistycznym systemów E/E/PE uszkodzeń o wspólnej przyczynie występują dwie następujące trudności:

— Powstaje pytanie, jaką wartość należy przyjąć dla współczynnika β. Wiele źródeł wskazuje na zakresy, w których współczynnik ten może występować, ale nie podają żadnej konkretnej wartości, pozostawiając analitykowi dokonanie subiektywnego wyboru. Z myślą o rozwiązaniu tego problemu metoda przedstawiona w załączniku D normy PN-EN 61508-6 została oparta na wykorzystaniu punktowych tablic estymacji.
— Druga trudność polega na tym, że model oparty na współczynniku β nie uwzględnia zaawansowanych możliwości współczesnych systemów PES, które mogą być wykorzystywane do wykrywania niejednoczesnych uszkodzeń spowodowanych wspólną przyczyną, zanim uszkodzenie takie ma wystarczająco dużo czasu, żeby się w pełni przejawić.

Model oparty na współczynniku β ustala związek między prawdopodobieństwem uszkodzeń spowodowanych wspólną przyczyną a prawdopodobieństwem przypadkowych uszkodzeń sprzętu. Prawdopodobieństwo uszkodzeń spowodowanych wspólną przyczyną, które obejmują system jako całość, zależy od złożoności systemu (prawdopodobnie zdominowanej przez oprogramowanie użytkownika), a nie tylko od samego sprzętu. Oczywiście, żadne obliczenia oparte na prawdopodobieństwie przypadkowych uszkodzeń sprzętu nie mogą uwzględniać złożoności oprogramowania.

Duża część uszkodzeń spowodowanych wspólną przyczyną nie występuje jednocześnie we wszystkich kanałach dotkniętych tymi uszkodzeniami. Dlatego jeśli częstość powtarzania testów diagnostycznych jest wystarczająco wysoka, to znaczna część uszkodzeń spowodowanych wspólną przyczyną może zostać wykryta i dzięki temu wyeliminowana, zanim obejmą one wszystkie dostępne kanały.

Przy zastosowaniu modelu opartego na współczynniku β intensywność uszkodzeń niebezpiecznych spowodowanych wspólną przyczyną wynosi:

$$\lambda_{D_{CCF}} = \lambda_D \cdot \beta \tag{4.52}$$

W powyższym wzorze λ_D jest intensywnością uszkodzeń niebezpiecznych dla przypadkowego uszkodzenia sprzętu każdego pojedynczego kanału, a β – udziałem uszkodzeń niewykrytych w przypadku braku testów diagnostycznych, tzn. stanowią tę część uszkodzeń pojedynczych kanałów, które oddziałują na wszystkie kanały. Przyjmuje się, że uszkodzenia spowodowane wspólną przyczyną oddziałują na wszystkie kanały oraz że przedział czasu pomiędzy uszkodzeniem pierwszego kanału a momentem, gdy uszkodzeniem zostaną objęte wszystkie kanały, jest mały w porównaniu z odstępem czasu do następnego uszkodzenia spowodowanego wspólną przyczyną.

Zakłada się, że w każdym kanale są wykonywane testy diagnostyczne, które wykrywają i ujawniają część uszkodzeń. Wszystkie uszkodzenia można podzielić na dwie kategorie: niewykrywalne przez testy diagnostyczne oraz wykrywalne przez testy diagnostyczne. Całkowitą intensywność uszkodzeń niebezpiecznych spowodowanych wspólną przyczyną można określić zależnością:

$$\lambda_{D_{CCF}} = \lambda_{DU} \cdot \beta + \lambda_{DD} \cdot \beta_D \tag{4.53}$$

gdzie: β – udział uszkodzeń niewykrytych, które mają wspólną przyczynę; β_D – udział uszkodzeń wykrytych, które mają wspólną przyczynę; λ_{DU}– intensywność uszkodzeń niebezpiecznych niewykrywalnych w testach diagnostycznych; λ_{DD} – intensywność uszkodzeń niebezpiecznych wykrywalnych w testach diagnostycznych.

Wartość współczynnika β otrzymuje się, stosując punktację $S = X + Y$, natomiast współczynnik β_D otrzymuje się, stosując punktację $S_D = X(Z + 1) + Y$ (tabl. 4.3).

Tablica 4.3

Obliczanie współczynnika β oraz β_D [161]

Liczba punktów S lub S_D	Odpowiadające wartości β lub β_D dla:	
	podsystemu logicznego	czujników lub elementów wykonawczych
120 lub więcej	0,5%	1%
od 70 do 120	1%	2%
od 45 do 70	2%	5%
mniej niż 45	5%	10%
UWAGA 1. Maksymalne poziomy β_D podane w niniejszej tablicy są niższe niż te, które byłyby stosowane, co odzwierciedla zastosowanie technik wyszczególnionych w innych miejscach niniejszej normy w celu zmniejszenia prawdopodobieństwa uszkodzeń systematycznych w ogóle i w wyniku tego uszkodzeń spowodowanych wspólną przyczyną. UWAGA 2. Wartości β_D mniejsze niż 0,5% dla podsystemu logicznego i 1% dla czujników byłyby trudne do uzasadnienia.		

Współczynnik β powinien być obliczony oddzielnie dla czujników, podsystemu logicznego i elementów wykonawczych. Zaleca się, aby w celu zminimalizowania prawdopodobieństwa wystąpienia uszkodzeń spowodowanych wspólną przyczyną ustalić najpierw, jakie środki prowadzą do skutecznej obrony przed ich wystąpieniem. Implementacja odpowiednich środków w systemie prowadzi do zmniejszenia wartości współczynnika β, stosowanego do oceny prawdopodobieństwa uszkodzeń spowodowanych wspólną przyczyną.

W tablicy 4.4 zestawiono sposoby i związane z nimi wartości oparte na ocenie technicznej, które reprezentują udział, jaki ma każdy ze środków w zmniejszeniu uszkodzeń spowodowanych wspólną przyczyną. Ponieważ czujniki i elementy wykonawcze są traktowane odmiennie niż elektronika programowalna, w tablicy wyodrębniono oddzielne kolumny punktacji odnoszącej się do elektroniki programowalnej oraz do czujników i elementów wykonawczych.

Tablica 4.4

Ocena punktowa czujników, systemów E/E/PE i elementów wykonawczych [161]

Pozycja	Podsystem logiczny		Czujniki i elementy wykonawcze	
	X_{LS}	Y_{LS}	X_{SF}	Y_{SF}
Oddzielnie/ segregacja				
Czy wszystkie kable sygnałowe poszczególnych kanałów są prowadzone oddzielnie we wszystkich miejscach?	1,5	1,5	1,0	2,0
Czy kanały podsystemów logicznych są montowane na oddzielnych płytkach drukowanych?	3,0	1,0	–	–
Czy kanały podsystemów logicznych są w oddzielnych obudowach?	2,5	0,5	–	–
Jeśli czujniki/ elementy wykonawcze mają wydzieloną elektronikę sterującą, to czy ta elektronika w przypadku każdego kanału jest na oddzielnych płytkach drukowanych?	–	–	2,5	1,5

Jeśli czujniki/ elementy wykonawcze mają wydzieloną elektronikę sterującą, to czy ta elektronika w przypadku każdego kanału znajduje się w pomieszczeniu zamkniętym i w oddzielnych obudowach?	–	–	2,5	0,5
Zróżnicowanie/ redundancja				
Czy w kanałach są stosowane różne techniki elektryczne, np. w jednym elektroniczna lub programowalna elektroniczna, a w drugim przekaźnikowa?	7,0	–	–	–
Czy w kanałach są stosowane różne techniki elektroniczne, np. w jednym elektroniczna, a w drugim programowalna elektroniczna?	5,0	–	–	–
Czy w elementach czujnikowych urządzeń wykorzystywane są różne zasady fizyczne, np. ciśnienie i temperatura, anemometr skrzydełkowy i przetwornik dopplerowski itp.?	–	–	7,5	–
Czy w urządzeniach są wykorzystywane różne zasady elektrotechniki/ rozwiązania, np. cyfrowe i analogowe, różni wytwórcy (bez zmiany oznakowania) lub różne techniki?	–	–	5,5	–
Czy w kanałach stosowana jest udoskonalona redundancja z architekturą *M*z*N*, gdzie $N > M + 2$?	2,0	0,5	2,0	0,5
Czy w kanałach stosowana jest udoskonalona redundancja z architekturą MzN, gdzie $N = M + 2$?	1,0	0,5	1,0	0,5
Czy stosowany jest niski poziom zróżnicowania, np. testowanie diagnostyczne sprzętu wykorzystujące tę samą technikę?	2,0	1,0	–	–
Czy stosowany jest średni poziom zróżnicowania, np. testowanie diagnostyczne sprzętu wykorzystujące inną technikę?	3,0	1,5	–	–
Czy kanały były projektowane przez różnych projektantów bez jakiejkolwiek komunikacji między nimi podczas projektowania?	1,0	1,0	–	–
Czy przy przekazywaniu do eksploatacji w przypadku każdego kanału wykorzystywane są odrębne metody badań i angażowane są inne osoby do ich wykonania?	1,0	0,5	1,0	1,0
Czy prace związane z obsługą w przypadku każdego kanału wykonywane są przez różne osoby w różnym czasie?	2,5	–	2,5	–
Złożoność/ konstrukcja/ zastosowanie/ dojrzałość/ doświadczenie				
Czy połączenie skrośne między kanałami uniemożliwia wymianę jakiejkolwiek informacji innej niż używana do testowania diagnostycznego lub głosowania?	0,5	0,5	0,5	0,5
Czy konstrukcja jest oparta na technikach stosowanych w urządzeniach, które są pomyślnie wykorzystywane w danej dziedzinie przez >5 lat?	0,5	1,0	1,0	1,0
Czy istnieje większe niż 5-letnie doświadczenie z tym samym sprzętem stosowanym w podobnym otoczeniu?	1,0	1,5	1,5	1,5
Czy system jest prosty, np. ma nie więcej niż 10 wejść lub wyjść na kanał?	–	1,0	–	–
Czy wejścia i wyjścia są zabezpieczone przed przepięciami i przeciążeniami o poziomach, które mogą wystąpić?	1,5	0,5	1,5	0,5
Czy wszystkie urządzenia/ elementy mają bezpiecznie dobrane obciążenie (np. z uwzględnieniem współczynnika 2 lub większego)?	2,0	–	2,0	–
Ocena/ analiza i wprowadzanie danych z analizy				
Czy wyniki analizy rodzajów i skutków niezdatności lub analizy drzewa niezdatności były badane w celu ustalenia źródeł uszkodzeń spowodowanych wspólną przyczyną oraz czy z góry ustalone źródła uszkodzeń spowodowanych wspólną przyczyną zostały wyeliminowane na drodze projektowej?	–	3,0	–	3,0

Czy uszkodzenia spowodowane wspólną przyczyną były rozpatrywane w przeglądach projektu z wprowadzeniem wyników do projektu? (Wymagany jest dowód z dokumentów czynności przeglądu projektu).	–	3,0	–	3,0
Czy wszystkie rodzaje uszkodzeń zostały w pełni przeanalizowane z wprowadzeniem wyników do projektu? (Wymagany jest dowód z dokumentu tej procedury).	0,5	3,5	0,5	3,5
Procedury/ interfejs użytkownika				
Czy istnieje opracowana w formie pisemnej organizacja pracy, mająca na celu zapewnienie, aby wykrywane były wszystkie uszkodzenia (lub zużycia) elementów, ustalane przyczyny źródłowe oraz sprawdzane inne podobne zagadnienia, które mogą stanowić podobną przyczynę uszkodzeń?	–	1,5	0,5	1,5
Czy są gotowe do wdrożenia procedury mające na celu zapewnienie, że konserwacja (łącznie z regulacją i kalibracją) jakiejkolwiek części niezależnych kanałów odbywać się będzie w różnym czasie oraz w uzupełnieniu do sprawdzania ręcznego wykonywanego po konserwacji dopuszczone jest satysfakcjonujące wykonywanie testów diagnostycznych pomiędzy końcem konserwacji jednego kanału a początkiem konserwacji innego?	1,5	0,5	2,0	1,0
Czy ujęte w dokumentach procedury konserwacji wyszczególniają, że wszystkie części układów redundancyjnych (np. kable itp.), zaplanowane jako niezależne od siebie, nie powinny być przemieszczane?	0,5	0,5	0,5	0,5
Czy cała obsługa płytek drukowanych itp. wykonywana jest na zewnątrz w kwalifikowanym centrum napraw oraz czy wszystkie naprawione pozycje przechodzą pełne badania przedinstalacyjne?	0,5	1,0	0,5	1,5
Czy system cechuje się niskim pokryciem diagnostycznym (od 60% do 90%) i zgłaszaniem uszkodzeń do poziomu modułów łatwo wymienialnych na miejscu?	0,5	–	–	–
Czy system cechuje się średnim pokryciem diagnostycznym (od 90% do 99%) i zgłaszaniem uszkodzeń do poziomu modułów łatwo wymienialnych na miejscu?	1,5	1,0	–	–
Czy system cechuje się wysokim pokryciem diagnostycznym (>99%) i zgłaszaniem uszkodzeń do poziomu modułów łatwo wymienialnych na miejscu?	2,5	1,5	–	–
Czy testy diagnostyczne systemu informują o uszkodzeniach do poziomu modułów łatwo wymienialnych na miejscu?	–	–	1,0	1,0
Kompetencje/ szkolenie/ kultura bezpieczeństwa				
Czy projektanci odbyli przeszkolenie (z potwierdzeniem w postaci dokumentów) w celu zrozumienia przyczyn i konsekwencji uszkodzeń spowodowanych wspólną przyczyną?	2,0	3,0	2,0	3,0
Czy dokonujący obsługi odbyli przeszkolenie (z potwierdzeniem w postaci dokumentów) w celu zrozumienia przyczyn i konsekwencji uszkodzeń spowodowanych wspólną przyczyną?	0,5	4,5	0,5	4,5
Kontrola środowiska				
Czy dostęp personelu jest ograniczony (np. zamknięte obudowy, niedostępne umiejscowienie)?	0,5	2,5	0,5	2,5
Czy jest prawdopodobne, że system zawsze będzie pracował w granicach temperatury, wilgotności, korozyjności, zapylenia, wibracji itp., w których był badany, bez stosowania zewnętrznej kontroli środowiska?	3,0	1,0	3,0	1,0
Czy kable zasilające i sygnałowe są rozdzielone we wszystkich miejscach?	2,0	1,0	2,0	1,0

Badania środowiskowe				
Czy system był badany na odporność na wszystkie wymagające uwzględnienia wpływy środowiska (np. kompatybilność elektromagnetyczną EMC, temperaturę, drgania, wstrząsy, wilgotność) do poziomu wymaganego w uznanych normach?	10,0	10,0	10,0	10,0
UWAGA 1 Pewna liczba pozycji odnosi się do pracy systemu i ich prognozowanie w czasie projektowania może być trudne. Zaleca się, aby w tych przypadkach projektanci przyjęli racjonalne założenia i następnie zapewnili to, aby ostateczny użytkownik systemu był świadomy np. procedur, jakie powinny być zastosowane w celu osiągnięcia zaprojektowanego poziomu nienaruszalności bezpieczeństwa. Mogłoby to być osiągnięte przez włączenie niezbędnych informacji do dokumentacji towarzyszącej systemowi. UWAGA 2 Wartości w kolumnach *X* i *Y* są oparte na ocenie uzyskanej na drodze oceny technicznej oraz uwzględnieniu pośredniego i bezpośredniego wpływu pozycji z kolumny 1. Na przykład, zastosowanie modułów łatwo wymienialnych na miejscu prowadzi do: — napraw wykonywanych przez wytwórcę w warunkach kontrolowanych zamiast (możliwe, że nieprawidłowych) napraw wykonywanych w mniej właściwych warunkach na miejscu. Skutkuje to wzrostem w kolumnie Y, ponieważ możliwość wystąpienia uszkodzenia systematycznego (a zatem i wspólnej przyczyny) jest mniejsza; — zmniejszenia potrzeby ręcznego oddziaływania na miejscu i uzyskania zdolności do szybkiej wymiany wadliwego modułu, być może online, oraz zwiększenia w ten sposób skuteczności diagnostyki mającej na celu identyfikację uszkodzeń, zanim staną się one uszkodzeniami spowodowanymi wspólną przyczyną. Prowadzi to do dużego zapisu w kolumnie X.				

Systemy elektroniki programowalnej mogą być wyposażone w wielostronne testy diagnostyczne, które pozwalają na wykrycie niejednoczesnych uszkodzeń spowodowanych wspólną przyczyną. Aby umożliwić uwzględnienie testów diagnostycznych przy określaniu wartości współczynnika β, całkowity udział każdego ze sposobów w tablicy 4.4 został podzielony, za pomocą oceny technicznej, na dwa zbiory wartości: *X* i *Y*. Dla każdego sposobu iloraz *X*/*Y* ilustruje stopień, w jakim udział danego sposobu w ograniczeniu uszkodzeń spowodowanych wspólną przyczyną może być zwiększony przez testowanie diagnostyczne.

Zaleca się, aby korzystając z tablicy 4.4, dokładnie ustalić, jakie sposoby są stosowane w rozważanym systemie, i zsumować odpowiednie wartości z kolumny X_{LS} i Y_{LS} dla podsystemów logicznych lub X_{SF} i Y_{SF} dla czujników lub elementów wykonawczych. Zsumowane wartości są oznaczane są, odpowiednio, jako *X* i *Y*.

Tablice 4.5 i 4.6 mogą być użyte do określenia współczynnika *Z* z częstości przeprowadzania testów diagnostycznych i pokrycia testami diagnostycznymi, przy uwzględnieniu zapewnienia, że wyposażenie sterowane będzie wprowadzone w stan bezpieczny, zanim niejednoczesne uszkodzenie spowodowane wspólną przyczyną obejmie wszystkie kanały (ogranicza to zalecane stosowanie niezerowych wartości *Z*).

Tablica 4.5

Współczynnik *Z* dla systemów E/E/PE

Pokrycie diagnostyczne *DC*	Odstęp testu diagnostycznego		
	mniej niż 1 min	między 1 min a 5 min	więcej niż 5 min
≥99%	2,0	1,0	0
≥90%	1,5	0,5	0
≥60%	1,5	0	0

Tablica 4.6

Współczynnik *Z* dla czujników i elementów wykonawczych

Pokrycie diagnostyczne *DC*	Odstęp testu diagnostycznego			
	mniej niż 2 h	między 2 h a 2 dniami	między 2 dniami a jednym tygodniem	więcej niż 1 tydzień
≥99%	2,0	1,5	1,0	0
≥90%	1,5	1,0	0,5	0
≥60%	1,0	0,5	0	0

Tablica 4.7

Przykłady oszacowania β oraz β_D dla wartości *X* i *Y* przykładowych systemów E/E/PE

Kategoria		System ze zróżnicowaniem z dobrym testowaniem diagnostycznym	System ze zróżnicowaniem z niedostatecznym testowaniem diagnostycznym	System z redundancją z dobrym testowaniem diagnostycznym	System z redundancją z niedostatecznym testowaniem diagnostycznym
Oddzielenie/ segregacja	*X*	3,5	3,5	3,5	3,5
	Y	1,5	1,5	1,5	1,5
Zróżnicowanie/ redundancja	*X*	14,5	14,5	2,0	2,0
	Y	3,0	3,0	1,0	1,0
Złożoność/ konstrukcja	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Ocena/ analiza	*X*	0,25	0,25	0,25	0,25
	Y	4,75	4,75	4,75	4,75
Procedury/ interfejs użytkownika	*X*	3,5	3,5	3,50	3,5
	Y	3,0	3,0	3,0	3,0
Kompetencje/ szkolenie	*X*	1,25	1,25	1,25	1,25
	Y	3,75	3,75	3,75	3,75
Kontrola środowiska	*X*	2,75	2,75	2,75	2,75
	Y	2,25	2,25	2,25	2,25
Badania środowiskowe	X	5,0	5,0	5,0	5,0
	Y	5,0	5,0	5,0	5,0
Pokrycie diagnostyczne	*Z*	2,0	0,0	2,0	0,0
Suma *X*		33,5	33,5	21	21
Suma *Y*		25,5	25,5	23,5	23,5
Liczba punktów *S*		59	59	44,5	44,5
β		2%	2%	5%	5%
Liczba punktów S_D		126	59	86,5	44,5
β_D		0,5%	2%	1%	5%

Następnie w celu otrzymania wartości współczynnika β dla uszkodzeń niewykrytych należy obliczyć liczbę punktów S:

$$S = X + Y \tag{4.54}$$

oraz S_D:

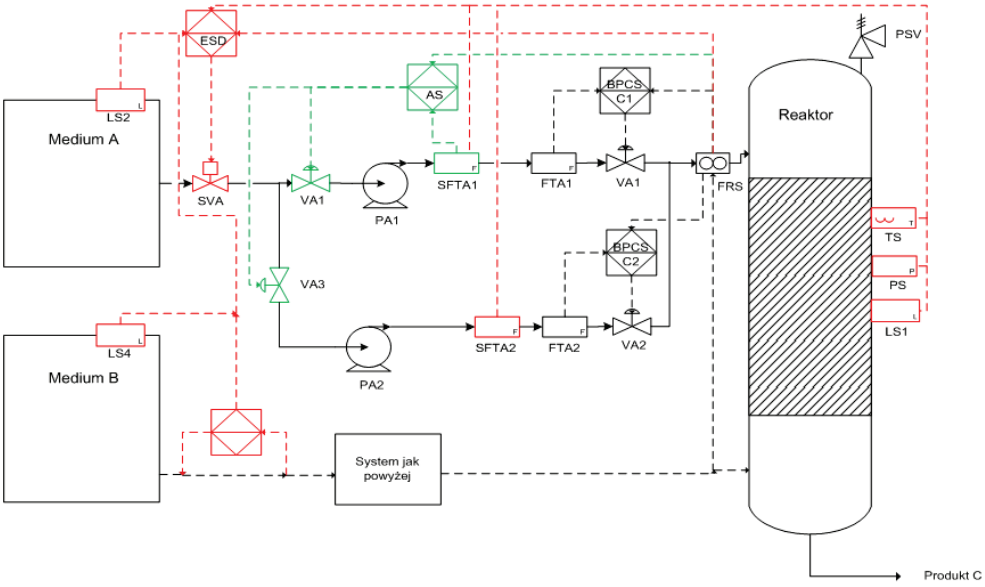
$$S_D = X(Z+1) + Y \tag{4.55}$$

w celu otrzymania wartości współczynnika β_D dla uszkodzeń wykrytych (przykład – tabl. 4.7).

W równaniach tych S lub S_D oznacza ocenę punktową, która jest używana w tablicy 4.3 do określenia odpowiedniej wartości współczynnika β oraz β_D (przykład – tabl. 4.7).

4.7. Weryfikacja SIL

Instalacja technologiczna (rys. 4.9) składa się ze zbiornika wysokociśnieniowego, dwóch zbiorników z substancjami A i B oraz rurociągów transportujących substancje ze zbiorników A i B do zbiornika wysokociśnieniowego, w którym zachodzi reakcja chemiczna. W wyniku reakcji i wymieszania substancji A i B otrzymywany jest produkt C.



Rys. 4.9. Przykładowa instalacja wraz z systemem sterowania i zabezpieczeń

Każdy rurociąg jest wyposażony w zestaw czujników, mierzących najważniejsze zmienne procesowe, oraz elementów wykonawczych, realizujących funkcje odpowiednie do kontekstu sytuacji. Aby proces mógł przebiegać w bezpieczny sposób, łatwopalne medium A powinno być bez przerwy dostarczane do zbiornika reakcyjnego w ilości większej od łatwopalnego medium B, tak aby nie doprowadzić do wybuchu. Reakcja mieszania musi się odbywać w określonej temperaturze oraz przy odpowiednim ciśnieniu.

Zbyt wysokie ciśnienie w zbiorniku reaktora może doprowadzić do eksplozji. Na podstawie analizy ryzyka określono wymagania dla funkcji bezpieczeństwa na poziomie SIL3.

Projektowana część sprzętowa realizująca funkcję bezpieczeństwa, która zapobiega eksplozji reaktora, musi spełniać kryteria probabilistyczne odpowiadające poziomowi SIL3. Na podstawie przeprowadzonych analiz częstości przywołań oraz częstości testów sprawdzających wykazano, że funkcja bezpieczeństwa spełnia kryteria działania na rzadkie przywołanie.

Warstwa sprzętowa realizująca funkcję bezpieczeństwa zapobiegającą powstaniu eksplozji zbiornika składa się z trzech podsystemów: pomiarowego, w skład którego wchodzą dwie matryce detektorów ciśnienia PS i temperatury TS; podsystemu ESD, którego integralną częścią jest system przetwarzający dane (PLC, sterownik *safety* PLC, SRS – *safety related system*), oraz układu wykonawczego – w tym przypadku zaworu SVA odcinającego dopływ medium do reaktora. Konfiguracja architektury warstwy sprzętowej realizującej funkcję bezpieczeństwa może wymagać nadmiarowości strukturalnej. W danym przypadku analizie zostaną poddane struktury przykładowych systemów SIS, których schematy przedstawiono na rys. 4.10 – system SIS (I), rys. 4.12 – system SIS (II), rys. 4.13 – system SIS (III) oraz rys. 4.14 – SIS (IV). Wartości PFD_{avg} dla systemu zabezpieczeniowego zostały wyznaczone z wykorzystaniem danych niezawodnościowych znajdujących się bazie danych ProSIL (opracowanej na podstawie bazy danych OREDA i poradników SINTEF) [70, 150, 197, 198].

W tablicy 4.8 zestawiono dane niezawodnościowe elementów systemów SIS poddanych weryfikacji. W danym przypadku rozpatrzone zostaną cztery różne podsystemy ESD: standardowy sterownik przemysłowy PLC, sterownik *safety* PLC, system SRS (np. programowalny przekaźnik bezpieczeństwa MMS) oraz sterowniki PLC w konfiguracji 1 z 2.

Tablica 4.8

Dane niezawodnościowe dla elementów systemu zabezpieczeniowego

	PS	**TS**	**PLC**	***Safety* PLC**	**SRS**	**SVA**
DC [%]	54	66	90	99	99	24
λ_{DU} [h^{-1}]	$3\cdot10^{-7}$	$3\cdot10^{-6}$	$4{,}1\cdot10^{-6}$	$2{,}2\cdot10^{-8}$	$8\cdot10^{-8}$	$8\cdot10^{-7}$
MTTR [h]	8	8	8	8	8	8
T_{I} [h]	8760	8760	8760	8760	8760	8760
β	0,02	0,02	0,01	0,01	0,01	0,02

Na rys. 4.10 pokazano pierwszą strukturę sprzętową systemu SIS (I), która została oparta na układzie sterownika PLC.

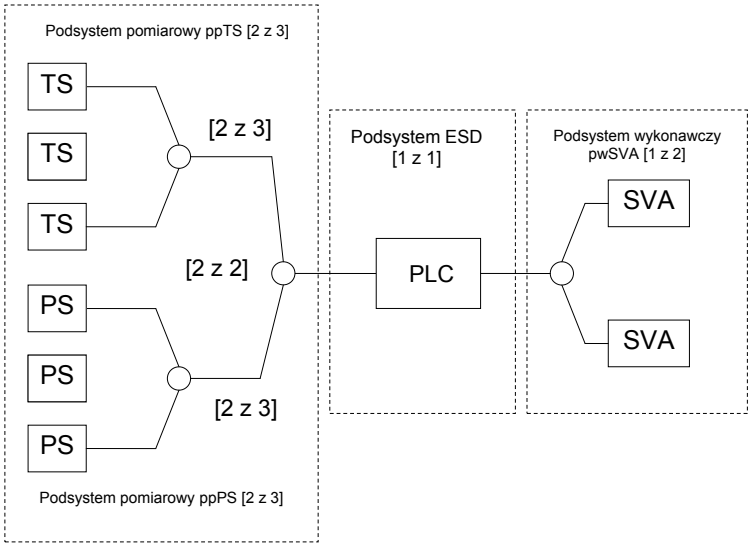
Na rys. 4.11 znajduje się drzewo niezdatności systemu SIS (I), na podstawie którego można wyznaczyć cięcia minimalne potrzebne do budowy modelu probabilistycznego.

Uwzględniając dane niezawodnościowe zawarte w tablicy 4.8, uzyskano wyniki, które wraz z całościową specyfikacją sprzętową systemu SIS (I) zestawiono w raporcie końcowym znajdującym się w tablicy 4.9.

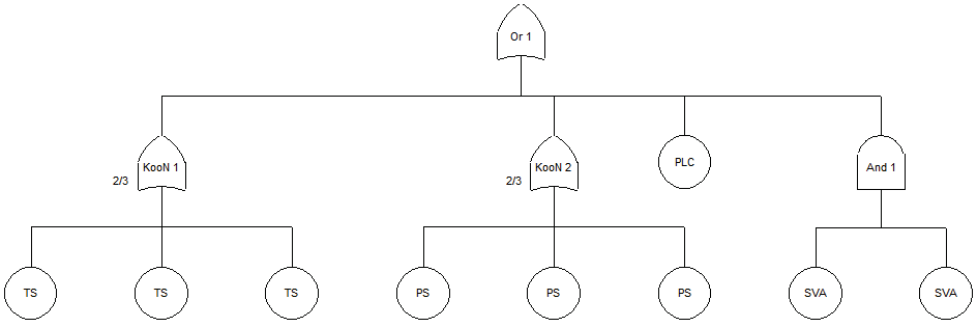
$$\begin{aligned} PFD_{\text{avgSIS(I)}} &\cong PFD_{\text{avgTS(2z3)}} + PFD_{\text{avgPS(2z3)}} + PFD_{\text{avgPLC}} + PFD_{\text{avgSVA(1z2)}} \cong \\ &\cong 2{,}93\cdot10^{-5} + 3{,}11\cdot10^{-5} + 1{,}8\cdot10^{-2} + 7{,}14\cdot10^{-5} \cong 1{,}81\cdot10^{-2} \end{aligned} \tag{4.56}$$

gdzie: $PFD_{\text{avgSIS(I)}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania przez system SIS (I); $PFD_{\text{avgTS(2z3)}}$ – przeciętne

prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu pomiaru temperatury ppTS w konfiguracji 2 z 3; $PFD_{avgPS(2z3)}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu pomiaru ciśnienia ppPS w konfiguracji 2 z 3; PFD_{avgPLC} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie dla sterownika PLC; $PFD_{avgSVA(1z2)}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu wykonawczego pwSVA w konfiguracji 1 z 2.



Rys. 4.10. Architektura systemu SIS (I) wyposażona w sterownik PLC
(matryce detektorów pracują w konfiguracji 2 z 2)



Rys. 4.11. Model FT systemu SIS (I)

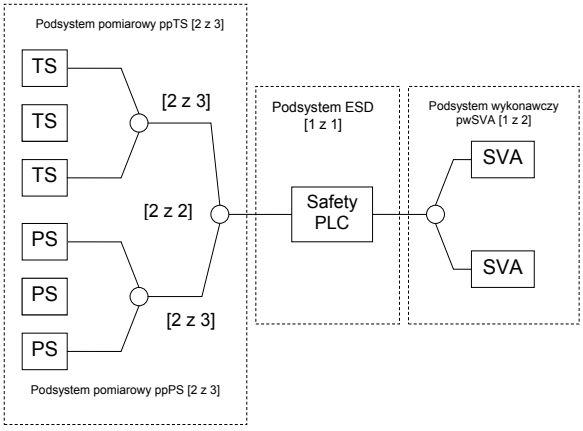
Tablica 4.9

Raport końcowy weryfikacji SIL dla systemu SIS (I)

System/ podsystem/ element		*k* z *n*	β [%]	PFD_{avg}	SIL	x_i [%] PFD_{avgS}
SIS (I)	**0**	**–**	**–**	**$1{,}81\cdot10^{-2}$**	**1**	**100**
ppTS	**.1**	**2 z 3**	**3**	**$2{,}93\cdot10^{-5}$**	**4**	**0,18**
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
ppPS	**.1**	**2 z 3**	**3**	**$3{,}11\cdot10^{-5}$**	**4**	**0,2**
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
ESD	**.1**	**1 z 1**	**–**	**$1{,}8\cdot10^{-2}$**	**1**	**99,3**
PLC	..2	–	–	$1{,}8\cdot10^{-2}$	1	–
pwSV	**.1**	**1 z 2**	**2**	**$7{,}14\cdot10^{-5}$**	**4**	**0,32**
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2	–
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2	–

Z powyższego raportu wynika, że struktura sprzętowa systemu SIS (I) nie spełnia wymagań SIL3. Duży udział w tym stanie rzeczy ma zastosowanie sterownika PLC w podsystemie ESD bez nadmiarowości strukturalnej (SIL1).

Na rys. 4.12 znajduje się druga struktura sprzętowa systemu SIS (II), zrealizowana na podstawie sterownika bezpieczeństwa safety PLC.



Rys. 4.12. Architektura systemu SIS (II) wyposażona w sterownik *safety* PLC (matryce detektorów pracują w konfiguracji 2 z 2)

Uwzględniając dane niezawodnościowe zawarte w tablicy 4.8, uzyskano wyniki, które wraz z całościową specyfikacją sprzętową systemu SIS (II) zestawiono w raporcie końcowym znajdującym się w tablicy 4.10.

Tablica 4.10

Raport końcowy weryfikacji SIL dla systemu SIS (II)

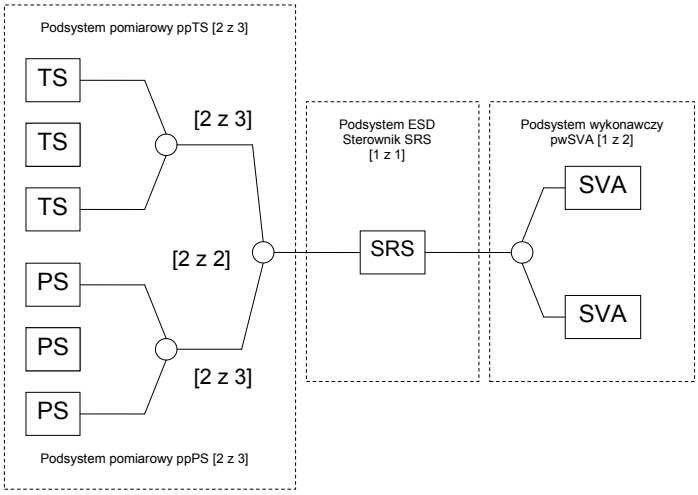
System/ podsystem/ element		k z n	β [%]	PFD_{avg}	SIL	x_i [%] PFD_{avgS}
SIS (II)	**0**	**–**	**–**	**$2{,}28\cdot10^{-4}$**	**3**	**100**
ppTS	**.1**	**2 z 3**	**3**	**$2{,}93\cdot10^{-5}$**	**4**	**12,8**
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
ppPS	**.1**	**2 z 3**	**3**	**$3{,}11\cdot10^{-5}$**	**4**	**13,6**
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
ESD	**.1**	**1 z 1**	**–**	**$9{,}64\cdot10^{-5}$**	**4**	**42,2**
Safety PLC	..2	–	–	$9{,}64\cdot10^{-5}$	4	–
pwSV	**.1**	**1 z 2**	**2**	**$7{,}14\cdot10^{-5}$**	**4**	**31,4**
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2	–
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2	–

$$PFD_{\text{avgSIS(II)}} \cong PFD_{\text{avgTS(2z3)}} + PFD_{\text{avgPS(2z3)}} + PFD_{\text{avg}_{\text{SafetyPLC}}} + PFD_{\text{avgSVA(1z2)}} \cong$$
$$\cong 2{,}93\cdot10^{-5} + 3{,}11\cdot10^{-5} + 9{,}64\cdot10^{-5} + 7{,}14\cdot10^{-5} \cong 2{,}28\cdot10^{-4} \tag{4.57}$$

gdzie: $PFD_{\text{avgSIS(I)}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania przez system SIS (II); $PFD_{\text{avgTS(2z3)}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu pomiaru temperatury ppTS w konfiguracji 2 z 3; $PFD_{\text{avgPS(2z3)}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu pomiaru ciśnienia ppPS w konfiguracji 2 z 3; $PFD_{\text{avgSafetyPLC}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie dla sterownika PLC w wersji *safety*; $PFD_{\text{avgSVA(1z2)}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu wykonawczego pwSVA w konfiguracji 1 z 2.

Z powyższego raportu wynika, że struktura sprzętowa systemu SIS (II) spełnia wymagania SIL3.

W trzecim z rozpatrywanych przypadków w systemie SIS (III) zastosowano w podsystemie ESD układ SRS (przekaźnik programowalny) (rys. 4.13).



Rys. 4.13. Architektura systemu SIS (III) wyposażona w układ SRS (przekaźnik programowalny)

Szczegółowy raport z weryfikacji struktury sprzętowej SIS (III) realizującej funkcję bezpieczeństwa znajduje się w tablicy 4.11.

Tablica 4.11

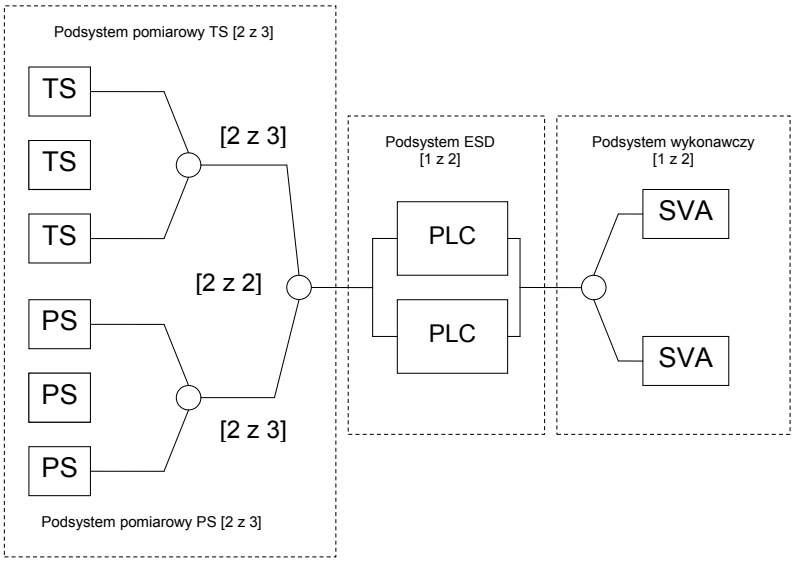
Raport wynikowy weryfikacji SIL dla systemu SIS (III)

System/ podsystem		*k* z *n*	β [%]	PFD_{avg}	SIL	x_i [%] PFD_{avgS}
SIS (III)	**0**	**–**	**–**	**$4{,}82\cdot10^{-4}$**	**3**	**100**
ppTS	**.1**	**2 z 3**	**3**	**$2{,}93\cdot10^{-5}$**	**4**	**6,15**
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2	–
ppPS	**.1**	**2 z 3**	**3**	**$3{,}11\cdot10^{-5}$**	**4**	**6,45**
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2	–
ESD	**.1**	**1 z 1**	**–**	**$3{,}5\cdot10^{-4}$**	**3**	**72,6**
SRS	..2	–	–	$3{,}5\cdot10^{-4}$	3	–
pwSV	**.1**	**1 z 2**	**2**	**$7{,}14\cdot10^{-5}$**	**4**	**14,8**
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2	–
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2	–

$$PFD_{\text{avgSIS(III)}} \cong PFD_{\text{avgTS(2z3)}} + PFD_{\text{avgPS(2z3)}} + PFD_{\text{avgSRS}} + PFD_{\text{avgSVA(1z2)}} \cong 4{,}82 \cdot 10^{-4} \quad (4.58)$$

Mimo braku nadmiarowości w konfiguracji podsystemu ESD system SIS (III) spełnia wymagania SIL3.

Na rys. 4.14 przedstawiono system SIS (IV), dla którego w podsystemie ESD zastosowano dwa sterowniki PLC w konfiguracji 1 z 2.



Rys. 4.14. Architektura systemu SIS (IV) wyposażona w dwa sterowniki PLC (1 z 2)

Szczegółowy raport z weryfikacji warstwy sprzętowej systemu SIS (IV) znajduje się w tablicy 4.12.

$$PFD_{\text{avgSIS(IV)}} \cong PFD_{\text{avgTS(2z3)}} + PFD_{\text{avgPS(2z3)}} + PFD_{\text{avgPLC(1z2)}} + PFD_{\text{avgSVA(1z2)}} \cong 6{,}36 \cdot 10^{-4} \quad (4.59)$$

Raporty z weryfikacji SIL przedstawione powyżej dla czterech systemów SIS pracujących w trybie pracy rzadkiego przywołania do działania zawierają procentowy udział wartości PFD_{avg} podsystemu/ elementu w ogólnej wartości PFD_{avgS}, wyznaczonej dla systemu (ostatnia kolumna) na podstawie zależności (4.18) prezentującej procentowy udział wartości PFD_{avg} lub PFH podsystemu/ elementu w ogólnej wartości PFD_{avg} lub PFH, wyznaczonej dla części sprzętowej systemu realizującego funkcje bezpieczeństwa.

Systemy SIS (II) zrealizowany z wykorzystaniem sterownika *safety* PLC, SIS (III) z układem SRS (np. przekaźnikiem programowalnym) oraz SIS (IV) z redundancją w podsystemie ESD z przemysłowych sterowników PLC spełniają wymagania SIL3. System SIS (IV) jest w danym przypadku rozwiązaniem tańszym od SIS (II) i (III).

Tablica 4.12

Raport wynikowy weryfikacji SIL dla systemu SIS (IV)

System/ podsystem/ element		*k* z *n*	β [%]	PFD_{avg}	SIL	x_i [%] PFD_{avgS}
SIS (IV)	**0**	**–**	**–**	**$6{,}36 \cdot 10^{-4}$**	**3**	100
ppTS	**.1**	**2 z 3**	**3**	**$2{,}93 \cdot 10^{-5}$**	**4**	**4,6**
TS	..2	–	–	$1{,}53 \cdot 10^{-3}$	2	–
TS	..2	–	–	$1{,}53 \cdot 10^{-3}$	2	–
TS	..2	–	–	$1{,}53 \cdot 10^{-3}$	2	–
ppPS	**.1**	**2 z 3**	**3**	**$3{,}11 \cdot 10^{-5}$**	**4**	**4,9**
PS	..2	–	–	$1{,}58 \cdot 10^{-3}$	2	–
PS	..2	–	–	$1{,}58 \cdot 10^{-3}$	2	–
PS	..2	–	–	$1{,}58 \cdot 10^{-3}$	2	–
ESD	**.1**	**1 z 2**	**1**	**$5{,}04 \cdot 10^{-4}$**	**3**	**79,3**
PLC	..2	–	–	$1{,}8 \cdot 10^{-2}$	1	–
PLC	..2	–	–	$1{,}8 \cdot 10^{-2}$	1	–
pwSV	**.1**	**1 z 2**	**2**	**$7{,}14 \cdot 10^{-5}$**	**4**	**11,2**
SVA	..2	–	–	$3{,}5 \cdot 10^{-3}$	2	–
SVA	..2	–	–	$3{,}5 \cdot 10^{-3}$	2	–

4.8. Podsumowanie

W niniejszym rozdziale przedstawiono wybrane zagadnienia dotyczące weryfikacji poziomów nienaruszalności funkcji związanych z bezpieczeństwem. Zaprezentowano modele probabilistyczne systemów E/E/PE wykorzystywane przy ilościowej weryfikacji SIL, zbudowane z użyciem techniki drzew niezdatności i schematów blokowych niezawodności. Metody weryfikacji SIL systemów E/E/PE zaproponowane w normach PN-EN 61508, PN-EN 61511 oraz PN-EN 62061 mają liczne ograniczenia [14, 17, 18, 68, 122, 195, 197, 198]. Przy wykorzystaniu zawartych w nich modeli możliwa jest tylko weryfikacja SIL ograniczonych architektonicznie struktur podsystemów składających się z takich samych elementów.

Ważnym aspektem przy ilościowej weryfikacji SIL jest właściwe uwzględnienie niewykrytych i wykrytych uszkodzeń, które mają wspólną przyczynę. W danym przypadku należy zwrócić szczególną uwagę na współczynnik korekcyjny uzależniony od architektury rozpatrywanego systemu.

Dalsze prace dotyczące procesu weryfikacji SIL powinny się skupić na opracowaniu skutecznych metod uwzględniających w modelach systemów E/E/PE i SIS w czytelny sposób wpływ uszkodzeń spowodowanych wspólną przyczyną i błędów człowieka, ocenę niepewności oraz zagadnienia związane z badaniem wrażliwości. Nie można pominąć tych aspektów w procesie weryfikacji SIL, gdyż uzyskane wyniki mogą być zbyt optymistyczne w stosunku do rzeczywistości.

W rozdziale nie poruszono kwestii uszkodzeń systematycznych oraz weryfikacji poziomów nienaruszalności oprogramowania, skupiono się natomiast na modelowaniu probabilistycznym różnych rozwiązań architektonicznych warstwy sprzętowej systemów E/E/PE (i/lub SIS). Aspekty te nie mogą zostać pominięte w procesie weryfikacji uzyskanego SIL, w danym przypadku jednak nie były przedmiotem prowadzonych analiz.

W przypadku weryfikacji SIL osobnego podejścia wymaga problematyka integrowania koncepcji bezpieczeństwa funkcjonalnego z ochroną informacji (*security*) rozproszonych i skomputeryzowanych systemów sterowania i automatyki zabezpieczeniowej przed możliwymi nieprzyjaznymi działaniami z zewnątrz poprzez sieć lokalną i/lub zewnętrzną, co zostanie szczegółowo omówione w kolejnych rozdziałach niniejszej monografii.

Rozdział 5

WERYFIKACJA SIL SYSTEMU E/E/PE W WARUNKACH NIEPEWNOŚCI

5.1. Wprowadzenie

Poszczególnym poziomom nienaruszalności bezpieczeństwa SIL projektowanego systemu E/E/PE odpowiadają ilościowe kryteria probabilistyczne. W analizie bezpieczeństwa funkcjonalnego kluczowe znaczenie ma określenie SIL dla obiektu (instalacji) podwyższonego ryzyka, a następnie zaprojektowanie takiego systemu zabezpieczeniowego, który spełni te wymagania. Dowód spełnienia przez system zabezpieczeniowy wymagań na określony poziom SIL nazywa się weryfikacją [155, 197, 200, 202].

W aplikacji ProSIL (ProSIL-EAL) zastosowano trzy metody modelowania probabilistycznego systemu E/E/PE: technikę schematów blokowych niezawodności oraz grafów Markowa z zastosowaniem gotowych zależności z normy PN-EN 61508-6; metodę bazującą na technice analizy drzewa niezdatności i schematów blokowych niezawodności z wykorzystaniem cięć minimalnych oraz technikę równań uproszczonych [9, 10, 25, 199, 201, 202].

Model probabilistyczny dowolnego systemu sterowania lub zabezpieczeń można przedstawić z wykorzystaniem schematów blokowych niezawodności RBD, grafów Markowa oraz drzew niezdatności FT (struktura ścieżek lub cięć minimalnych) [6, 79, 196, 198]. W przypadku gdy system rozpatrywany jest z punktu widzenia jego uszkadzalności, wygodnym podejściem jest skorzystanie z metody cięć minimalnych. Biorąc pod uwagę metodę cięć minimalnych, prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez system zabezpieczeniowy można określić na podstawie zależności:

$$PFD(t) \cong \sum_{j=1}^{n} Q_j(t) \cong \sum_{j=1}^{n} \prod_{i \in K_j} q_i(t) \tag{5.1}$$

gdzie: K_j – j-te cięcie minimalne (CM); $Q_i(t)$ – prawdopodobieństwo wystąpienia j-tego cięcia minimalnego w funkcji czasu; n – liczba cięć CM; $q_i(t)$ – prawdopodobieństwo uszkodzenia i-tego podsystemu lub elementu.

Wykorzystując zależność (5.1), można określić przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na przywołanie, zakładając, że poszczególne podsystemy są testowane z interwałem czasowym T_I w celu wykrycia uszkodzeń niebezpiecznych. Średnia częstość występowania uszkodzenia niebezpiecznego na godzinę może być oszacowana na podstawie wzoru:

$$PFH \cong \frac{\sum_{j=1}^{n}(1-\sum_{\substack{i=1 \\ i\neq j}}^{n} Q_j(t))(\sum_{j\in K_j} \frac{Q_j(t)}{q_i(t)}(1-q_i(t))\lambda_i)}{1-\sum_{j=1}^{n}\prod_{i\in K_j} q_i(t)} \tag{5.2}$$

gdzie: λ_i – intensywność uszkodzeń i-tego podsystemu/ elementu

Architekturę sprzętu realizującego funkcję bezpieczeństwa przedstawia się za pomocą schematów blokowych z wyróżnieniem podsystemów i modułów. Korzystając z metody cięć minimalnych, przy określaniu prawdopodobieństwa $PFD(t)$, a następnie wartości PFD_{avg} i PFH można zaproponować dwa podejścia, stanowiące alternatywę dla modeli probabilistycznych podstawowych struktur nadmiarowych wg PN-EN 61508, przedstawionych w rozdziale 4 niniejszej monografii.

Struktura 2 z 3:
I (wg cięć minimalnych (CM))

$$PFD_{avg2z3} \cong 3((1-\beta)\lambda_D)^2(\frac{T_I^2}{3} + T_I \cdot MTTR + MTTR^2) + \beta \cdot \lambda_{DU}(\frac{T_I}{2} + MTTR) \quad (5.3)$$

gdzie: β – udział uszkodzeń niewykrytych, które mają wspólną przyczynę; T_I – interwał przeprowadzania testów okresowych; $MTTR$ – średni czas naprawy; λ_D – intensywność uszkodzeń niebezpiecznych; λ_{DU} – intensywność uszkodzeń niebezpiecznych niewykrywalnych.

$$PFH_{2z3} \cong 6((1-\beta)\lambda_D)^2(\frac{T_I}{2} + MTTR) + \beta \cdot \lambda_{DU} \quad (5.4)$$

II (wg równań uproszczonych)

$$PFD_{avg2z3} \cong 3 \cdot \lambda_D{}^2(\frac{T_I^2}{3} + T_I \cdot MTTR + MTTR^2) + \beta \cdot \lambda_{DU}(\frac{T_I}{2} + MTTR) \quad (5.5)$$

$$PFH_{2z3} \cong 6 \cdot \lambda_D{}^2(\frac{T_I}{2} + MTTR) + \beta \cdot \lambda_{DU} \quad (5.6)$$

Struktura 4 z 6:
II (wg cięć minimalnych (CM))

$$PFD_{avg4z6} \cong 20((1-\beta)\lambda_D)^3[T_I^2(\frac{T_I}{4} + MTTR) + T_I \cdot MTTR(T_I + \frac{3}{2}MTTR) + \\ + MTTR^3] + \beta \cdot \lambda_{DU}(\frac{T_I}{2} + MTTR) \quad (5.7)$$

$$PFH_{4z6} \cong 60((1-\beta)\lambda_D)^3(\frac{T_I}{2} + MTTR)^2 + \beta \cdot \lambda_{DU} \quad (5.8)$$

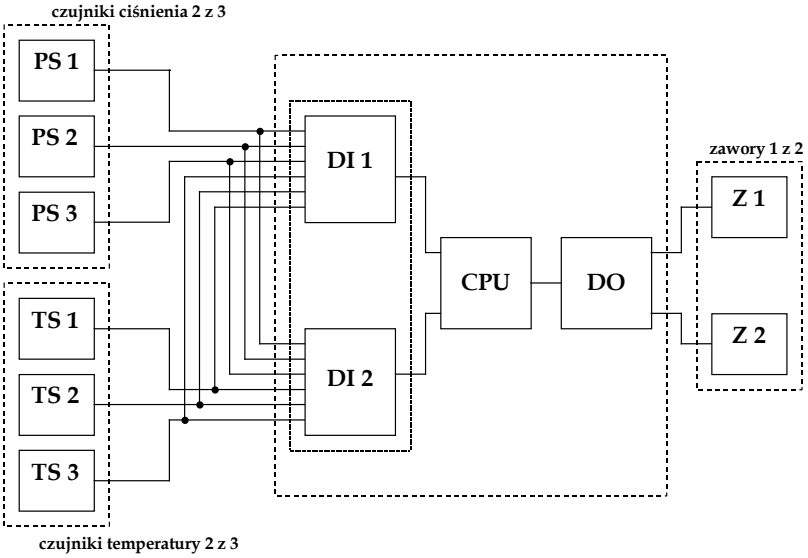
III (wg równań uproszczonych)

$$PFD_{avg4z6} \cong 20 \cdot \lambda_D{}^3[T_I^2(\frac{T_I}{4} + MTTR) + T_I \cdot MTTR(T_I + \frac{3}{4}MTTR) + MTTR^3] + \\ + \beta \cdot \lambda_{DU}(\frac{T_I}{2} + MTTR) \quad (5.9)$$

$$PFH_{4z6} \cong 60 \cdot \lambda_D{}^3(\frac{T_I}{2} + MTTR)^2 + \beta \cdot \lambda_{DU} \quad (5.10)$$

5.2. Modele probabilistyczne struktur złożonych

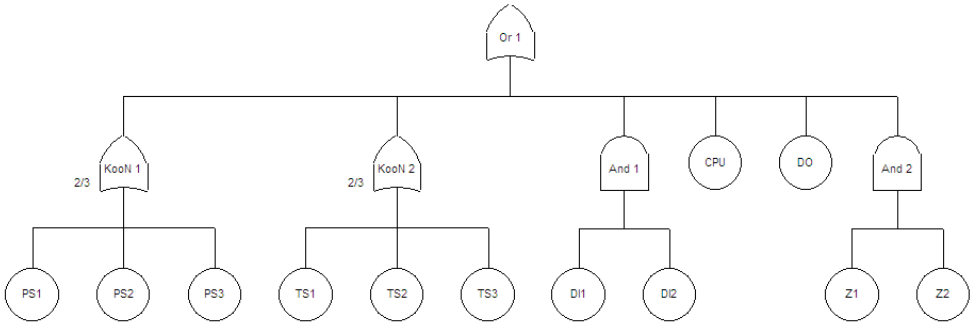
System zabezpieczeniowy (I) ESD, przedstawiony na rys. 5.1, składa się z układu pomiarowego (złożonego z czujników ciśnienia PS w konfiguracji 2 z 3 oraz czujników temperatury TS w konfiguracji 2 z 3), układu przetwarzania danych (w skład którego wchodzą moduły wejść dyskretnych DI w konfiguracji 1 z 2, jednostka centralna CPU i moduł wyjść dyskretnych DO) oraz podsystemu elementów wykonawczych, którymi w danym przykładzie są zawory Z w konfiguracji 1 z 2.



Rys. 5.1. System I – PS i TS (2 z 3), DI (1 z 2), CPU (1 z 1), DO (1 z 1), Z (1 z 2)

Dla systemu z rys. 5.1 istnieje zbiór 10 cięć minimalnych (rys. 5.2 – na podstawie FT):

$$K_1 = \{\text{PS1}, \text{PS2}\}, K_2 = \{\text{PS1}, \text{PS3}\}, K_3 = \{\text{PS2}, \text{PS3}\}, K_4 = \{\text{TS1}, \text{TS2}\}, K_5 = \{\text{TS1}, \text{TS3}\},$$
$$K_6 = \{\text{TS2}, \text{TS3}\}, K_7 = \{\text{DI1}, \text{DI2}\}, K_8 = \{\text{CPU}\}, K_9 = \{\text{DO}\}, K_{10} = \{\text{Z1}, \text{Z2}\}$$



Rys. 5.2. Model FT systemu (E/E/PE) I

Zatem prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa $PFD(t)$ ma postać:

$$PFD(t) \cong q_{PS1}(t) \cdot q_{PS2}(t) + q_{PS1}(t) \cdot q_{PS3}(t) + q_{PS2}(t) \cdot q_{PS3}(t) + q_{TS1}(t) \cdot q_{TS2}(t) + \\ + q_{TS1}(t) \cdot q_{TS3}(t) + q_{TS2}(t) \cdot q_{TS3}(t) + q_{DI1}(t) \cdot q_{DI2}(t) + q_{CPU}(t) + q_{DO}(t) + q_{Z1}(t) \cdot q_{Z2}(t) \quad (5.11)$$

gdzie: $q_{PS1}(t)$ – prawdopodobieństwo uszkodzenia czujnika ciśnienia PS1; $q_{PS2}(t)$ – prawdopodobieństwo uszkodzenia czujnika ciśnienia PS2; $q_{PS3}(t)$ – prawdopodobieństwo uszkodzenia czujnika ciśnienia PS3; $q_{TS1}(t)$ – prawdopodobieństwo uszkodzenia czujnika temperatury TS1; $q_{TS2}(t)$ – prawdopodobieństwo uszkodzenia czujnika temperatury TS2; $q_{TS3}(t)$ – prawdopodobieństwo uszkodzenia czujnika temperatury TS3; $q_{DI1}(t)$ – prawdopodobieństwo uszkodzenia modułu wejść dyskretnych DI1; $q_{DI2}(t)$ – prawdopodobieństwo uszkodzenia modułu DI2; $q_{CPU}(t)$ – prawdopodobieństwo uszkodzenia procesora; $q_{DO}(t)$ – prawdopodobieństwo uszkodzenia modułu wyjść dyskretnych DO; $q_{Z1}(t)$ – prawdopodobieństwo uszkodzenia zaworu Z1, $q_{Z2}(t)$ – prawdopodobieństwo uszkodzenia zaworu Z2.

W przypadku gdy poszczególne podsystemy, czyli układy: pomiarowy, przetwarzania, wykonawczy, składają się z jednakowych elementów, wówczas prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa $PFD(t)$ przedstawia poniższa zależność:

$$PFD(t) \cong 3 \cdot q_{PS}(t)^2 + 3 \cdot q_{TS}(t)^2 + q_{DI}(t)^2 + q_{CPU}(t) + q_{DO}(t) + q_Z(t)^2 \quad (5.12)$$

gdzie: $q_{PS}(t)$ – prawdopodobieństwo uszkodzenia czujnika ciśnienia PS; $q_{TS}(t)$ – prawdopodobieństwo uszkodzenia czujnika temperatury TS; $q_{DI}(t)$ – prawdopodobieństwo uszkodzenia modułu wejść dyskretnych DI; $q_{CPU}(t)$ – prawdopodobieństwo uszkodzenia procesora; $q_{DO}(t)$ – prawdopodobieństwo uszkodzenia modułu wyjść dyskretnych DO; $q_Z(t)$ – prawdopodobieństwo uszkodzenia zaworu Z.

Zatem dla przykładowego systemu zabezpieczeniowego z rys. 5.1 przeciętna wartość prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na żądanie PFD_{avg} wynosi:

$$PFD_{avg} \cong 3((1-\beta_{PS})\lambda_{D^{PS}})^2\left(\frac{T_I^2}{3} + T_I \cdot MTTR_{PS} + MTTR_{PS}^2\right) + \beta_{PS} \cdot \lambda_{DU^{PS}}\left(\frac{T_I}{2} + MTTR_{PS}\right) + \\ + 3((1-\beta_{TS})\lambda_{D^{TS}})^2\left(\frac{T_I^2}{3} + T_I \cdot MTTR_{TS} + MTTR_{TS}^2\right) + \beta_{TS} \cdot \lambda_{DU^{TS}}\left(\frac{T_I}{2} + MTTR_{TS}\right) + \\ + ((1-\beta_{DI})\lambda_{D^{DI}})^2\left(\frac{T_I^2}{3} + T_I \cdot MTTR_{DI} + MTTR_{DI}^2\right) + \beta_{DI} \cdot \lambda_{DU^{DI}}\left(\frac{T_I}{2} + MTTR_{DI}\right) + \\ + \lambda_{DU^{CPU}}\frac{T_I}{2} + \lambda_{D^{CPU}} \cdot MTTR_{CPU} + \lambda_{DU^{DO}}\frac{T_I}{2} + \lambda_{D^{DO}} \cdot MTTR_{DO} + \\ + ((1-\beta_Z)\lambda_{D^Z})^2\left(\frac{T_I^2}{3} + T_I \cdot MTTR_Z + MTTR_Z^2\right) + \beta_Z \cdot \lambda_{DU^Z}\left(\frac{T_I}{2} + MTTR_Z\right) \quad (5.13)$$

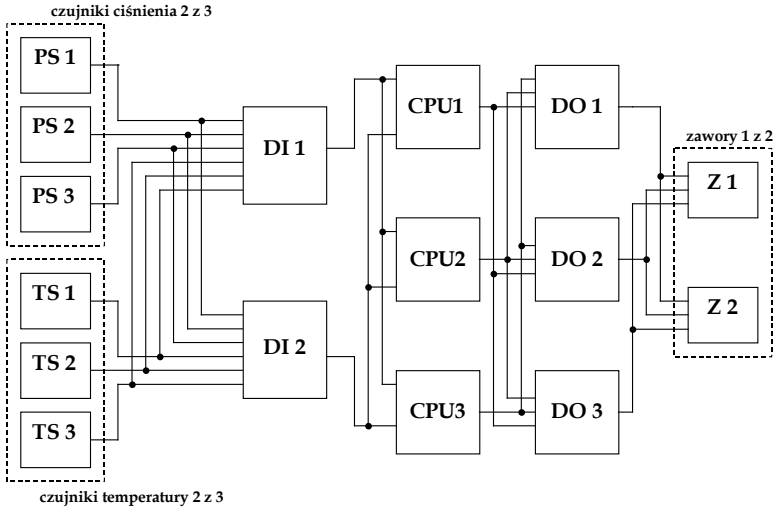
gdzie: β_{PS} – udział uszkodzeń niewykrytych (w układzie czujników ciśnienia PS), które mają wspólną przyczynę; β_{TS} – udział uszkodzeń niewykrytych (w układzie czujników temperatury TS), które mają wspólną przyczynę; β_{DI} – udział uszkodzeń niewykrytych (w układzie modułów wejść dyskretnych DI), które mają wspólną przyczynę; β_Z – udział uszkodzeń niewykrytych (w układzie elementów wykonawczych – zawory Z), które mają wspólną przyczynę; $MTTR_{PS}$ – średni czas naprawy dla czujnika ciśnienia PS; $MTTR_{TS}$ – średni czas naprawy dla czujnika temperatury TS; $MTTR_{DI}$ – średni czas naprawy dla modułu wejść dyskretnych; $MTTR_{CPU}$ – średni czas naprawy dla procesora CPU; $MTTR_{DO}$ – średni czas naprawy dla modułu wyjść dyskretnych; $MTTR_Z$ – średni czas naprawy dla

zaworu Z; T_I – interwał przeprowadzania testów okresowych; λ_{DPS} – intensywność uszkodzeń niebezpiecznych dla czujnika ciśnienia PS; λ_{DTS} – intensywność uszkodzeń niebezpiecznych dla czujnika temperatury TS; λ_{DDI} – intensywność uszkodzeń niebezpiecznych dla modułu wejść dyskretnych DI; λ_{DCPU} – intensywność uszkodzeń niebezpiecznych dla procesora CPU; λ_{DDO} – intensywność uszkodzeń niebezpiecznych dla modułu wyjść dyskretnych DO; λ_{DZ} – intensywność uszkodzeń niebezpiecznych dla zaworu Z; λ_{DUPS} – intensywność uszkodzeń niebezpiecznych niewykrywalnych dla czujnika ciśnienia PS; λ_{DUTS} – intensywność uszkodzeń niebezpiecznych niewykrywalnych dla czujnika temperatury TS; λ_{DUDI} – intensywność uszkodzeń niebezpiecznych niewykrywalnych dla modułu wejść dyskretnych DI; λ_{DUCPU} – intensywność uszkodzeń niebezpiecznych niewykrywalnych dla procesora CPU; λ_{DUDO} – intensywność uszkodzeń niebezpiecznych niewykrywalnych dla modułu DO; λ_{DUZ} – intensywność uszkodzeń niebezpiecznych niewykrywalnych dla zaworu Z.

Średnią częstość występowania uszkodzenia niebezpiecznego na godzinę *PFH* dla pracy ciągłej w danym przypadku opisuje zależność:

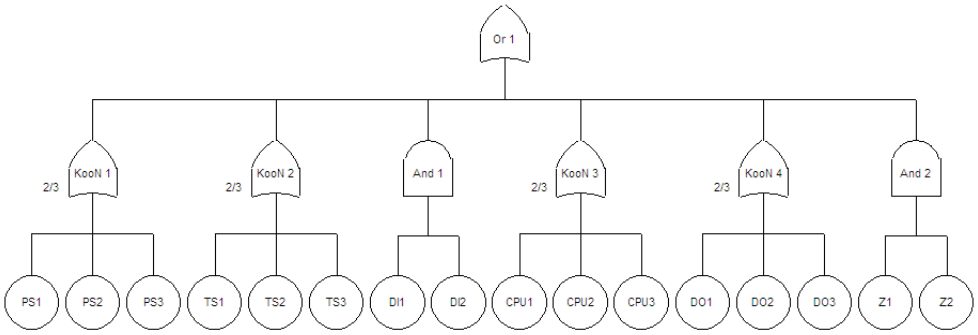
$$\begin{aligned} PFH \cong\ & 6((1-\beta_{PS})\lambda_{D^{PS}})^2(\frac{T_I}{2}+MTTR_{PS})+\beta_{PS}\cdot\lambda_{DU^{PS}}+6((1-\beta_{TS})\lambda_{D^{TS}})^2(\frac{T_I}{2}+MTTR_{TS})+ \\ & +\beta_{TS}\cdot\lambda_{DU^{TS}}+2((1-\beta_{DI})\lambda_{D^{DI}})^2(\frac{T_I}{2}+MTTR_{DI})+\beta_{DI}\cdot\lambda_{DU^{DI}}+\lambda_{DU^{CPU}}+\lambda_{DU^{DO}}+ \\ & +2((1-\beta_Z)\lambda_{D^Z})^2(\frac{T_I}{2}+MTTR_Z)+\beta_Z\cdot\lambda_{DU^Z} \end{aligned} \tag{5.14}$$

System zabezpieczeniowy (II) (rys. 5.3) składa się układu pomiarowego złożonego z czujników ciśnienia PS w konfiguracji 2 z 3 oraz czujników temperatury TS w konfiguracji 2 z 3, elementów wykonawczych, którymi w danym przykładzie są zawory w konfiguracji 1 z 2, oraz układu przetwarzania danych, w skład którego wchodzą: moduły wejść dyskretnych DI w konfiguracji 1 z 2, układ procesorów CPU w konfiguracji 2 z 3 i moduły wyjść dyskretnych DO również w konfiguracji 2 z 3.



Rys. 5.3. System II – PS i TS (2 z 3), DI (1 z 2), CPU (2 z 3), DO (2 z 3), Z (1 z 2)

Dla systemu sterowania/ zabezpieczeniowego z rys. 5.3 istnieje zbiór 14 cięć (rys. 5.4 – na podstawie FT):



Rys. 5.4. Model FT systemu (E/E/PE) II

$$K_1 = \{\text{PS1}, \text{PS2}\}, K_2 = \{\text{PS1}, \text{PS3}\}, K_3 = \{\text{PS2}, \text{PS3}\}, K_4 = \{\text{TS1}, \text{TS2}\}, K_5 = \{\text{TS1}, \text{TS3}\},$$
$$K_6 = \{\text{TS2}, \text{TS3}\}, K_7 = \{\text{DI1}, \text{DI2}\}, K_8 = \{\text{CPU1}, \text{CPU2}\}, K_9 = \{\text{CPU1}, \text{CPU3}\},$$
$$K_{10} = \{\text{CPU2}, \text{CPU3}\}, K_{11} = \{\text{DO1}, \text{DO2}\}, K_{12} = \{\text{DO1}, \text{DO2}\}, K_{13} = \{\text{DO2}, \text{DO3}\}, K_{14} = \{\text{Z1}, \text{Z2}\}$$

Przy założeniu, że rozpatrywany system zabezpieczeniowy/ sterowania składa się z różnych elementów, zależność na prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa $PFD(t)$ ma postać:

$$\begin{aligned} PFD(t) \cong\ & q_{\text{PS1}}(t) \cdot q_{\text{PS2}}(t) + q_{\text{PS1}}(t) \cdot q_{\text{PS3}}(t) + q_{\text{PS2}}(t) \cdot q_{\text{PS3}}(t) + q_{\text{TS1}}(t) \cdot q_{\text{TS2}}(t) + \\ & + q_{\text{TS1}}(t) \cdot q_{\text{TS3}}(t) + q_{\text{TS2}}(t) \cdot q_{\text{TS3}}(t) + q_{\text{DI1}}(t) \cdot q_{\text{DI2}}(t) + q_{\text{CPU1}}(t) \cdot q_{\text{CPU2}}(t) + q_{\text{CPU1}}(t) \cdot q_{\text{CPU3}}(t) + \\ & + q_{\text{CPU2}}(t) \cdot q_{\text{CPU3}}(t) + q_{\text{DO1}}(t) \cdot q_{\text{DO2}}(t) + q_{\text{DO1}}(t) \cdot q_{\text{DO3}}(t) + q_{\text{DO2}}(t) \cdot q_{\text{DO3}}(t) + q_{\text{Z1}}(t) \cdot q_{\text{Z2}}(t) \end{aligned} \quad (5.15)$$

gdzie: $q_{\text{CPU1}}(t)$ – prawdopodobieństwo uszkodzenia procesora CPU1; $q_{\text{CPU2}}(t)$ – prawdopodobieństwo uszkodzenia procesora CPU2; $q_{\text{CPU3}}(t)$ – prawdopodobieństwo uszkodzenia procesora CPU3; $q_{\text{DO1}}(t)$ – prawdopodobieństwo uszkodzenia modułu wyjść dyskretnych DO1; $q_{\text{DO2}}(t)$ – prawdopodobieństwo uszkodzenia modułu wyjść dyskretnych DO2; $q_{\text{DO3}}(t)$ – prawdopodobieństwo uszkodzenia modułu wyjść dyskretnych DO3.

W przypadku gdy poszczególne podsystemy systemu składają się z jednakowych elementów, wówczas prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa $PFD(t)$ przez system II można przedstawić następująco:

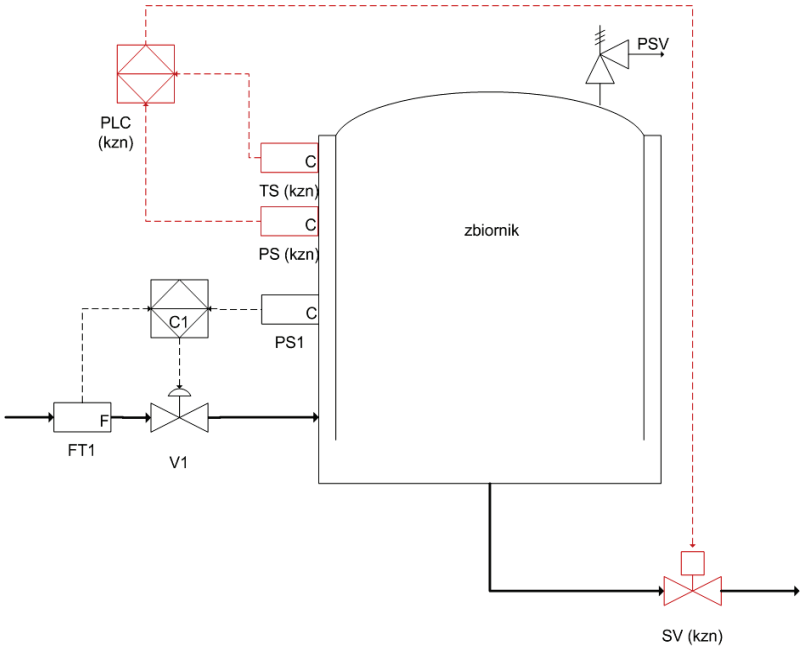
$$PFD(t) \approx 3 \cdot q_{\text{PS}}(t)^2 + 3 \cdot q_{\text{TS}}(t)^2 + q_{\text{DI}}(t)^2 + 3 \cdot q_{\text{CPU}}(t)^2 + 3 \cdot q_{\text{DO}}(t)^2 + q_{\text{Z}}(t)^2 \quad (5.16)$$

Wykorzystując zależność na prawdopodobieństwo niewypełnienia przez system zabezpieczeniowy funkcji bezpieczeństwa $PFD(t)$, można określić przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie PFD_{avg} oraz średnią częstość występowania uszkodzenia niebezpiecznego na godzinę PFH. Wartości te posłużą następnie do weryfikacji poziomu SIL systemu na podstawie kryteriów probabilistycznych bezpieczeństwa funkcjonalnego.

Modele probabilistyczne prostych systemów sterowania i zabezpieczeniowych są skomplikowane. Charakteryzują się znaczną liczbą parametrów, które mają różny wpływ na wynik końcowy, takich jak wartości prawdopodobieństw PFD_{avg} oraz PFH. Należy

zatem zidentyfikować wpływ cięć minimalnych oraz parametrów poszczególnych elementów modelowanych systemów na wynik końcowy, co znacznie uprości postać modeli probabilistycznych analizowanych systemów.

Przed zaprojektowaniem systemu zabezpieczeniowego ESD dla obiektu/ instalacji należy przeprowadzić ocenę ryzyka. Do oceny ryzyka obiektu można wykorzystać analizy niezawodności, takie jak metoda drzew niezdatności FTA, lub analizę rodzajów skutków i krytyczności uszkodzeń FMECA. Na podstawie oceny ryzyka przeprowadzonej dla obiektu uzyskuje się informacje dotyczące wymagań stawianych zabezpieczeniom. Z oceny ryzyka przeprowadzonej dla obiektu wynika, jakim poziomem SIL musi się cechować układ zabezpieczeń. Należy zatem dobrać system zabezpieczeniowy o odpowiedniej architekturze. Podsystem PLC (*k* z *n*) przedstawiony na rys. 5.5 składa się z modułów wejść DI (*k* z *n*), jednostki centralnej CPU (*k* z *n*) oraz modułów wyjść DO (*k* z *n*).



Rys. 5.5. Zbiornik ciśnieniowy wraz z systemami BPCS i ESD

Przykładowe struktury systemu zabezpieczeń dla obiektu podwyższonego ryzyka przedstawiono na rys. 5.1 i 5.3. Układ zabezpieczeniowy składa się ze: sterowników PLC o nieznanej architekturze (*k* z *n*), przy czym każdy sterownik składa się z jednostki centralnej CPU (*k* z *n*) modułów wejść I (dyskretnych DI lub analogowych AI) (*k* z *n*) oraz modułów wyjść O (dyskretnych DO lub analogowych AO) o strukturze (*k* z *n*), czujników o nieznanej strukturze S (*k* z *n*), elementów wykonawczych A (*k* z *n*). Przed wyznaczeniem poziomu SIL dla systemu zabezpieczeniowego nie jest znana warstwa strukturalna jego podsystemów. Poziom SIL zależy od architektury systemu zabezpieczeniowego. Jeżeli uzyskane wartości PFD_{avg} lub *PFH* dla rozpatrywanego systemu zabezpieczeniowego są mniejsze niż PFD_{avg} lub *PFH* wynikające z oceny ryzyka, wówczas można przyjąć taki system zabezpieczeniowy jako spełniający wymagania i zainstalować go w obiekcie.

W danym przypadku analizie zostaną poddane struktury przykładowych systemów SIS, których schematy przedstawiono na rys. 5.1 (system I) i rys. 5.3 (system II). Wymagania stawiane dla układu zabezpieczeniowego są na poziomie nienaruszalności bezpieczeństwa SIL3.

Wartości PFD_{avg} i PFH dla systemu zabezpieczeniowego zostały wyznaczone z wykorzystaniem danych niezawodnościowych zestawionych w tablicy 5.1.

Tablica 5.1

Dane niezawodnościowe dla elementów systemu zabezpieczeniowego

	PS	TS	DI	CPU	DO	SV
λ [h^{-1}]	$4\cdot10^{-6}$	$2\cdot10^{-6}$	$1{,}09\cdot10^{-6}$	$2{,}08\cdot10^{-6}$	$6{,}21\cdot10^{-7}$	$1{,}3\cdot10^{-6}$
FS [%]	50	50	50	50	50	50
λ_D [h^{-1}]	$2\cdot10^{-6}$	$1\cdot10^{-6}$	$5{,}46\cdot10^{-7}$	$1{,}04\cdot10^{-6}$	$3{,}1\cdot10^{-7}$	$6{,}5\cdot10^{-7}$
λ_S [h^{-1}]	$2\cdot10^{-6}$	$1\cdot10^{-6}$	$5{,}46\cdot10^{-7}$	$1{,}04\cdot10^{-6}$	$3{,}1\cdot10^{-7}$	$6{,}5\cdot10^{-7}$
DC [%]	90	90	90	90	90	90
λ_{DD} [h^{-1}]	$1{,}8\cdot10^{-6}$	$9\cdot10^{-7}$	$4{,}91\cdot10^{-7}$	$9{,}38\cdot10^{-7}$	$2{,}79\cdot10^{-7}$	$5{,}85\cdot10^{-7}$
λ_{DU} [h^{-1}]	$2\cdot10^{-7}$	$1\cdot10^{-7}$	$5{,}46\cdot10^{-8}$	$1{,}04\cdot10^{-7}$	$3{,}1\cdot10^{-8}$	$6{,}5\cdot10^{-8}$
$MTTR$ [h]	8	8	8	8	8	8
T_I [rok]	10	10	10	10	10	10
β	0,02	0,02	0,02	0,02	0,02	0,02

W tablicy 5.2 zestawiono wartości PFD_{avg} i PFH dla poszczególnych podsystemów oraz dla całego systemu, uzyskane na podstawie przeprowadzonych obliczeń z wykorzystaniem danych z tablicy 5.1.

Tablica 5.2

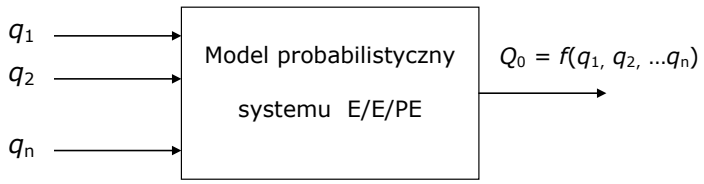
Wyniki uzyskane dla różnych struktur systemu E/E/PE

	PS	TS	DI	CPU	DO	SV
$PFD_{avg\ 1z1}$	$8{,}78\cdot10^{-3}$	$4{,}39\cdot10^{-3}$	$2{,}39\cdot10^{-3}$	$4{,}57\cdot10^{-3}$	$1{,}36\cdot10^{-3}$	$2{,}85\cdot10^{-3}$
PFH_{1z1}	$2\cdot10^{-7}$	$1\cdot10^{-7}$	$5{,}46\cdot10^{-8}$	$1{,}04\cdot10^{-7}$	$3{,}1\cdot10^{-8}$	$6{,}5\cdot10^{-8}$
$PFD_{avg\ 1z2}$	$2{,}76\cdot10^{-4}$	$1{,}13\cdot10^{-4}$	**$5{,}53\cdot10^{-5}$**	$1{,}19\cdot10^{-4}$	$2{,}96\cdot10^{-5}$	**$6{,}76\cdot10^{-5}$**
PFH_{1z2}	$5{,}63\cdot10^{-8}$	$1{,}96\cdot10^{-8}$	**$8{,}56\cdot10^{-9}$**	$2{,}08\cdot10^{-8}$	$4{,}24\cdot10^{-9}$	**$1{,}08\cdot10^{-8}$**
$PFD_{avg\ 2z3}$	**$4{,}77\cdot10^{-4}$**	**$1{,}63\cdot10^{-4}$**	$7{,}03\cdot10^{-5}$	**$1{,}73\cdot10^{-4}$**	**$3{,}45\cdot10^{-5}$**	$8{,}88\cdot10^{-5}$
PFH_{2z3}	**$1{,}25\cdot10^{-7}$**	**$3{,}67\cdot10^{-8}$**	$1{,}37\cdot10^{-8}$	**$3{,}94\cdot10^{-8}$**	**$5{,}89\cdot10^{-9}$**	$1{,}8\cdot10^{-8}$
SIL_{elem}	3	3	4	3	4	4
PFD_{avgSYS}	**$9{,}70\cdot10^{-4}$**					
PFH_{SYS}	**$1{,}14\cdot10^{-7}$**					
SIL_{SYS}	**3**					

Poszukiwaną strukturę systemu zabezpieczeniowego zrealizowanego na bazie sterowników programowalnych, spełniającą wymagania dla poziomu nienaruszalności bezpieczeństwa SIL3, przedstawiono na rys. 5.3 (system II). Wartość PFD_{avg} uzyskana metodą analityczną dla tej struktury wynosi $9{,}7 \cdot 10^{-4}$ (tabl. 5.2) co odpowiada poziomowi nienaruszalności bezpieczeństwa SIL3. Dla struktury przedstawionej na rys. 5.1 (system I) wartość PFD_{avg} uzyskana metodą analityczną wynosi $2{,}41 \cdot 10^{-3}$, co odpowiada SIL2, zatem w tym przypadku założenia nie zostały spełnione. Należy zwrócić uwagę, że uzyskane wyniki są punktowe (konkretna liczba bez podania zakresu niepewności) i dla systemu II są bliskie wartościom kryterialnym odpowiadającym SIL2.

5.3. Propozycja analizy wrażliwości modelu probabilistycznego systemu E/E/PE

Do zbadania wrażliwości modelu probabilistycznego systemu sterowania lub zabezpieczeniowego, czyli wpływu poszczególnych elementów systemu na postać tego modelu, można zastosować zmodyfikowane pojęcie elastyczności cząstkowej funkcji wielu zmiennych. Na rys. 5.6 przedstawiono schemat poglądowy modelu probabilistycznego systemu E/E/PE składającego się z n elementów.



Rys. 5.6. Schemat poglądowy modelu probabilistycznego systemu E/E/PE [17, 155]

Powstaje pytanie, jak zmieni się procentowo wartość Q_0 w wyniku procentowej zmiany A i-tego elementu modelu probabilistycznego systemu E/E/PE. Dla funkcji wielu zmiennych $Q_0 = f(q_1, q_2, \ldots q_n)$ stanowiącej model probabilistyczny systemu E/E/PE można zdefiniować wrażliwość:

$$MS_{q_i}^{WR} \cong \frac{q_i \cdot A_i}{f(q_1, q_2, ...q_n)} \cdot \frac{\partial f(q_1, q_2, ...q_n)}{\partial q_i} \tag{5.17}$$

gdzie: i = 1, 2, …, n – kolejny i-ty element rozpatrywanego systemu; A_i – procentowa zmiana wartości *i-tego* elementu; q_i – prawdopodobieństwo uszkodzenia *i-tego* elementu.

Wrażliwość $MS_{q_i}^{WR}$ podaje w przybliżeniu procentowy przyrost wartości funkcji $Q_0 = f(q_1, q_2, \ldots, q_n)$, gdy odpowiedni parametr q_i ulegnie zmianie o A_i procent.

W ramach przykładu niech dany będzie podsystem o architekturze 2 z 3, wówczas:

$$Q_0(t) \cong PFD(t) = q_1(t) \cdot q_2(t) + q_1(t) \cdot q_3(t) + q_2(t) \cdot q_3(t) \tag{5.18}$$

gdzie: $q_1(t)$ – prawdopodobieństwo uszkodzenia pierwszego elementu; $q_2(t)$ – prawdopodobieństwo uszkodzenia drugiego elementu; $q_3(t)$ – prawdopodobieństwo uszkodzenia trzeciego elementu.

Zakładając, że $q_i(t) \Rightarrow q_i$ dla określonej chwili czasowej *t*:

$$Q_0 \cong q_1 \cdot q_2 + q_1 \cdot q_3 + q_2 \cdot q_3 \tag{5.19}$$

Korzystając z zależności (5.17) określającej wrażliwość $MS_{q_i}^{\mathrm{WR}}$:

$$MS_{q_1}^{\mathrm{WR}} \cong \frac{q_1 \cdot A_1}{q_1 \cdot q_2 + q_1 \cdot q_3 + q_2 \cdot q_3} \cdot (q_2 + q_3) \tag{5.20}$$

$$MS_{q_2}^{\mathrm{WR}} \cong \frac{q_2 \cdot A_2}{q_1 \cdot q_2 + q_1 \cdot q_3 + q_2 \cdot q_3} \cdot (q_1 + q_3) \tag{5.21}$$

$$MS_{q_3}^{\mathrm{WR}} \cong \frac{q_3 \cdot A_3}{q_1 \cdot q_2 + q_1 \cdot q_3 + q_2 \cdot q_3} \cdot (q_1 + q_2) \tag{5.22}$$

Prawdopodobieństwo uszkodzenia *i*-tego elementu systemu E/E/PE jest funkcją wielu zmiennych $q_i = f(\lambda_i, \beta_i, MTTR_i, DC_i, T_{1i})$. Każdy parametr modelu probabilistycznego ma wpływ na wartość prawdopodobieństwa uszkodzenia pojedynczego *i*-tego elementu systemu E/E/PE. Na wyznaczone wartości końcowe prawdopodobieństw PFD_{avg} oraz *PFH* dla systemu mają wpływ poszczególne parametry modeli pojedynczych podsystemów, w szczególności udział uszkodzeń niewykrytych, które mają wspólną przyczynę β. Badanie wrażliwości modelu probabilistycznego umożliwia oszacowanie granic niepewności dla wynikowych prawdopodobieństw na podstawie niepewności związanej z parametrami przyjętymi w modelach probabilistycznych podsystemów.

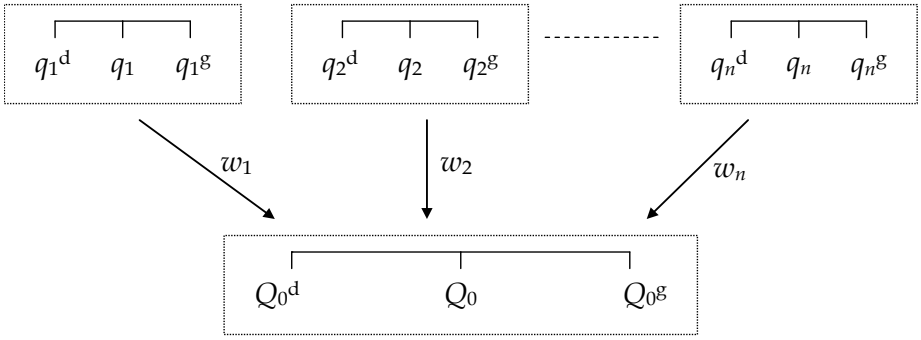
Znając wrażliwość $MS_{q_i}^{\mathrm{WR}}$, a więc względną procentową zmianę wartości funkcji $Q_0 = f(q_1, q_2, \ldots, q_n)$, na procentową zmianę wartości *A i*-tego elementu q_i będącego częścią składową modelu probabilistycznego, można określić przyrost bezwzględny ΔQ_{0qi} wartości funkcji dla tej zmiany.

Całkowity przyrost bezwzględny ΔQ_0 równy jest w przybliżeniu sumie *n* cząstkowych przyrostów bezwzględnych [155, 198]:

$$\Delta Q_0 \cong \sum_{i=1}^{n} \Delta Q_{0q_i} \approx \sum_{i=1}^{n} MS_{q_i}^{\mathrm{WR}} \cdot f(q_1, q_2, \ldots q_n) \approx \sum_{i=1}^{n} q_i \cdot A_i \cdot \frac{\partial f(q_1, q_2, \ldots q_n)}{\partial q_i} \approx \sum_{i=1}^{n} \Delta q_i \cdot w_i \tag{5.23}$$

gdzie: ΔQ_{0qi} – *i-ty* cząstkowy przyrost bezwzględny; $MS_{q_i}^{\mathrm{WR}}$ – wrażliwość modelu probabilistycznego na zmianę wartości prawdopodobieństwa uszkodzenia *i*-tego elementu; q_i – prawdopodobieństwo uszkodzenia *i-tego* elementu; A_i – procentowa zmiana wartości *i-tego* elementu; Δq_i – przyrost bezwzględny prawdopodobieństwa uszkodzenia *i-tego* elementu; w_i – wskaźnik wagowy.

Wykorzystując zależność (5.23), można określić dolną oraz górną granicę zmian wartości Q_0 [Q_0^{d}, Q_0^{g}] na podstawie zmian wartości poszczególnych elementów. Sytuację opisaną zależnością (5.23) ilustruje graficznie rys. 5.7.



Rys. 5.7. Wpływ zmian prawdopodobieństw pojedynczych elementów na zmianę wartości prawdopodobieństwa całego systemu

Ponieważ prawdopodobieństwo uszkodzenia *i*-tego elementu systemu E/E/PE jest funkcją wielu zmiennych $q_i = f(\lambda_i, \beta_i, MTTR_i, DC_i, T_{1i})$, zatem dolna i górna granica dla q_i [q_i^{d}, q_i^{g}] jest uzależniona od niepewności określenia poszczególnych parametrów stanowiących składowe tej funkcji. Zatem badając wrażliwość modelu probabilistycznego systemu E/E/PE, można określić wpływ zmian parametrów modelu na zmiany prawdopodobieństw poszczególnych elementów. Znając zmiany prawdopodobieństw poszczególnych elementów systemu E/E/PE, można określić zmiany wartości prawdopodobieństw PFD_{avg} [$PFD_{\mathrm{avg}}^{\mathrm{d}}$, $PFD_{\mathrm{avg}}^{\mathrm{g}}$] oraz PFH [PFH^{d}, PFH^{g}], a zatem oszacować dla nich przedział niepewności [155, 197, 198].

5.4. Uwzględnienie niepewności w procesie weryfikacji SIL

Wartości PFD_{avg} oraz PFH uzyskane na podstawie oszacowań analitycznych mają charakter punktowy. Zdarza się, że znajdują się blisko dolnej lub górnej granicy przedziału dyskretnego odpowiadającego poziomowi nienaruszalności bezpieczeństwa SIL. Przy weryfikacji SIL użytecznym parametrem jest wskaźnik różnicowy w_{R} niosący informację dotyczącą położenia punktowych wartości PFD_{avg} oraz PFH w przedziale kryterialnym. Wskaźnik różnicowy definiuje się jako różnicę pomiędzy wskaźnikami kryterialnymi dla dolnej i górnej granicy przedziału kryterialnego prawdopodobieństwa, odpowiadającego danemu poziomowi nienaruszalności bezpieczeństwa SIL:

$$w_{\mathrm{R}} = \mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{\mathrm{avg}}) - \mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{\mathrm{avg}}) \tag{5.24}$$

gdzie: $\mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{\mathrm{avg}})$ – dolny wskaźnik kryterialny dla dolnej granicy przedziału kryterialnego $P_{\mathrm{CR}}^{\mathrm{d}}$ odpowiadającego danemu poziomowi nienaruszalności bezpieczeństwa SIL (tablica 2.1), od wartości punktowej (środkowej) PFD_{avg} przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie; $\mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{avg})$ – górny wskaźnik kryterialny dla górnej granicy przedziału kryterialnego $P_{\mathrm{CR}}^{\mathrm{g}}$ odpowiadającego danemu poziomowi nienaruszalności bezpieczeństwa SIL (tablica 2.1), od wartości punktowej (środkowej) PFD_{avg} przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie.

W przypadku uwzględnienia przedziału niepewności przy wyznaczaniu wartości PFD_{avg} (lub PFH) należy uwzględnić dwa dodatkowe wskaźniki różnicowe, dla dolnej i górnej granicy wartości tych prawdopodobieństw; wówczas otrzymujemy następujące wartości: PFD_{avg} [$PFD_{\text{avg}}{}^{\text{d}}$, $PFD_{\text{avg}}{}^{\text{g}}$] (lub PFH [PFH^{d}, PFH^{g}]), dla których wskaźnik różnicowy dolny ma postać:

$$w_{\text{R}}^{\text{d}} = \mu_{\text{SIL}}^{\text{d}}(PFD_{\text{avg}}^{\text{d}}) - \mu_{\text{SIL}}^{\text{g}}(PFD_{\text{avg}}^{\text{d}}) \tag{5.25}$$

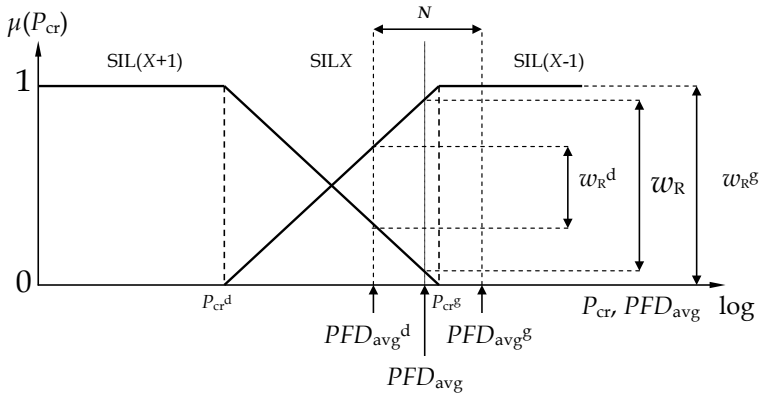
gdzie: $\mu_{\text{SIL}}^{\text{d}}(PFD_{\text{avg}}^{\text{d}})$ – dolny wskaźnik kryterialny dla dolnej granicy przedziału kryterialnego $P_{\text{CR}}{}^{\text{d}}$ odpowiadającego danemu poziomowi nienaruszalności bezpieczeństwa SIL (tablica 2.1), od wartości dolnej granicy $PFD_{\text{avg}}{}^{\text{d}}$ przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie; $\mu_{\text{SIL}}^{\text{g}}(PFD_{\text{avg}}^{\text{d}})$ – górny wskaźnik kryterialny dla górnej granicy przedziału kryterialnego $P_{\text{CR}}{}^{\text{g}}$ odpowiadającego danemu SIL, od wartości dolnej granicy $PFD_{\text{avg}}{}^{\text{d}}$ przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie.

Wskaźnik różnicowy górny opisuje poniższa zależność:

$$w_{\text{R}}^{\text{g}} = \mu_{\text{SIL}}^{\text{d}}(PFD_{\text{avg}}^{\text{g}}) - \mu_{\text{SIL}}^{\text{g}}(PFD_{\text{avg}}^{\text{g}}) \tag{5.26}$$

gdzie: $\mu_{\text{SIL}}^{\text{d}}(PFD_{\text{avg}}^{\text{g}})$ – dolny wskaźnik kryterialny dla dolnej granicy przedziału kryterialnego $P_{\text{CR}}{}^{\text{d}}$ odpowiadającego danemu SIL, od wartości górnej granicy $PFD_{\text{avg}}{}^{\text{g}}$ przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie; $\mu_{\text{SIL}}^{\text{g}}(PFD_{\text{avg}}^{\text{g}})$ – górny wskaźnik kryterialny dla górnej granicy przedziału kryterialnego $P_{\text{CR}}{}^{\text{g}}$ odpowiadającego danemu SIL, od wartości górnej granicy $PFD_{\text{avg}}{}^{\text{g}}$ przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie.

Na rys. 5.8 przedstawiono ogólny przypadek weryfikacji SIL na podstawie oszacowanej wartości PFD_{avg} (lub PFH) z uwzględnieniem przedziałów niepewności.



Rys. 5.8. Weryfikacja SIL z uwzględnieniem niepewności wyników otrzymanych z modelu probabilistycznego

Zaproponowana metoda, wykorzystująca wskaźniki różnicowe, jest pomocna w efektywnej weryfikacji wymaganego poziomu SIL systemów E/E/PE z uwzględnieniem

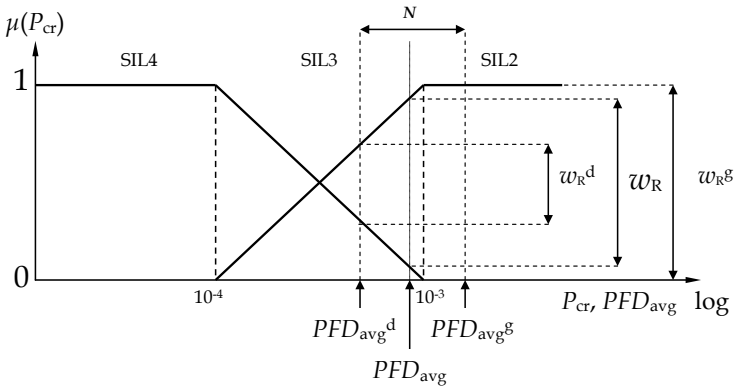
wyników analizy wrażliwości i/lub oszacowanych przedziałów niepewności uzyskanych z opracowanych modeli probabilistycznych, na podstawie systemu dziesięciu reguł:

$$
\begin{aligned}
&\text{I. } w_{\mathrm{R}} < 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow EF = 1\\
&\text{II. } w_{\mathrm{R}} = 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow EF = 1\\
&\text{III. } w_{R} > 0 \Rightarrow \mathrm{SIL}X+ \Leftrightarrow EF = 1\\
&\text{IV. } w_{\mathrm{R}}^{\mathrm{d}} < 0 \wedge w_{\mathrm{R}} < 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} = -1 \Rightarrow \mathrm{SIL}(X-1)+\\
&\text{V. } w_{\mathrm{R}}^{\mathrm{d}} < 0 \wedge w_{\mathrm{R}} < 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} = -1 \Rightarrow \mathrm{SIL}(X-1)\\
&\text{VI. } w_{\mathrm{R}}^{\mathrm{d}} < 0 \wedge w_{\mathrm{R}} < 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X\\
&\text{VII. } w_{\mathrm{R}}^{\mathrm{d}} > 0 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X\\
&\text{VIII. } w_{\mathrm{R}}^{\mathrm{d}} = 1 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X+\\
&\text{IX. } w_{\mathrm{R}}^{\mathrm{d}} > 0 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} \geq 0 \Rightarrow \mathrm{SIL}X+\\
&\text{X. } w_{\mathrm{R}}^{\mathrm{d}} = 1 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow EF \geq 3
\end{aligned}
\tag{5.27}
$$

gdzie: w_{R} – wskaźnik różnicowy; $w_{\mathrm{R}}^{\mathrm{d}}$ – wskaźnik różnicowy dolny; $w_{\mathrm{R}}^{\mathrm{g}}$ – wskaźnik różnicowy górny; EF (*error factor*) – wskaźnik błędu; SILX – poziom nienaruszalności bezpieczeństwa X.

W systemie wnioskowania należy uwzględnić rodzaj wykorzystywanych modeli probabilistycznych – norma PN-EN 61508 (graf Markowa), cięcia minimalne (technika analizy drzewa niezdatności FT, technika schematów blokowych niezawodności RBD) oraz modele bazujące na technice równań uproszczonych [25].

Wykorzystując przedstawione powyżej podejście, można dokonać weryfikacji określonego poziomu SIL dla punktowej wartości PFD_{avg} uzyskanej dla przykładowego systemu II (rys. 5.3) z podrozdziału 5.2 (rys. 5.9).



Rys. 5.9. Weryfikacja SIL3 systemu II dla punktowej wartości $PFD_{\mathrm{avg}} = 9{,}7 \cdot 10^{-4}$ oraz $PFD_{\mathrm{avg}}{}^{\mathrm{d}} = 6{,}47 \cdot 10^{-4}$; $PFD_{\mathrm{avg}}{}^{\mathrm{g}} = 1{,}46 \cdot 10^{-3}$ dla $EF = 1{,}5$

$$w_{\mathrm{R}}^{\mathrm{d}} = \mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{\mathrm{avg}}{}^{\mathrm{d}}) - \mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{\mathrm{avg}}{}^{\mathrm{d}}) = 0,38 - 0,72 = -0,34 \Rightarrow w_{\mathrm{R}}^{\mathrm{d}} < 0$$
$$w_{\mathrm{R}} = \mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{\mathrm{avg}}) - \mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{\mathrm{avg}}) = 0,13 - 0,87 = -0,74 \Rightarrow w_{\mathrm{R}} < 0 \quad \rightarrow \mathrm{SIL2+} \tag{5.28}$$
$$w_{\mathrm{R}}^{\mathrm{g}} = \mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{\mathrm{avg}}{}^{\mathrm{g}}) - \mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{\mathrm{avg}}{}^{\mathrm{g}}) = 0 - 1 \Rightarrow w_{\mathrm{R}}^{\mathrm{g}} = -1$$

Na podstawie IV reguły → SIL2+

Punktowa wartość przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na żądanie mieści się w przedziale odpowiadającym poziomowi nienaruszalności bezpieczeństwa SIL3. Jednak po uwzględnieniu niepewności, na podstawie reguły IV, system II (rys. 5.3) spełnia wymagania SIL2+. Powyższy przypadek pokazuje, że wartość $PFD_{\mathrm{avg}} = 9{,}7 \cdot 10^{-4}$, otrzymana dla systemu II, odpowiada poziomowi SIL3, jest ona jednak bliska kryteriom probabilistycznym dla poziomu SIL2.

5.5. Miary ważności modeli probabilistycznych

Wykorzystując miary ważności, modele probabilistyczne można uprościć do niezbędnego minimum, eliminując z nich elementy wywierające najmniejszy wpływ na końcową wartość określanych prawdopodobieństw. W bardzo złożonych systemach sterowania i zabezpieczeń, w których każdy podsystem składa się ze znacznej liczby elementów, uwzględnienie wrażliwości, czyli wpływu poszczególnych elementów na zachowanie się modelu probabilistycznego, staje się koniecznością. Wrażliwość, czyli wpływ poszczególnych elementów systemu na wynik końcowy, a więc w danym przypadku wartość prawdopodobieństwa, można ustalić poprzez stosowanie miar ważności w modelowaniu (przed zbudowaniem końcowego modelu probabilistycznego systemu) i ocenie bezpieczeństwa funkcjonalnego.

Do zbadania wrażliwości modelu probabilistycznego systemu sterowania lub zabezpieczeniowego, czyli wpływu poszczególnych elementów systemu na postać tego modelu, można zastosować następujące miary [6, 25, 79, 198]:

— ważności Birnbauma $I^{\mathrm{B}}(i|t)$;
— krytyczności $I^{\mathrm{CR}}(i|t)$;
— ważności Vesely'ego–Fussella $I^{\mathrm{VF}}(i|t)$.

Miarę ważności Birnbauma $I^{B}(i|t)$ opisuje zależność:

$$I^{\mathrm{B}}(i|t) = \frac{\partial Q_0(t)}{\partial q_i(t)} \Rightarrow I^{\mathrm{B}}(i|t) = \frac{\partial PFD(t)}{\partial PFD_i(t)} \tag{5.29}$$

gdzie: $i = 1, 2, \ldots, n$ – kolejny, i-ty element rozpatrywanego systemu; $PFD(t)$ – prawdopodobieństwo niewypełnienia przez rozpatrywany system funkcji bezpieczeństwa na rzadkie przywołanie; $PFD_i(t)$ – prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa przez i-ty element rozpatrywanego systemu.

Miarę krytyczności $I^{\mathrm{CR}}(i|t)$ można przedstawić w następującej postaci:

$$I^{\mathrm{CR}}(i|t) = \frac{I^{\mathrm{B}}(i|t) \cdot q_i(t)}{Q_0(t)} \tag{5.30}$$

gdzie: $i = 1, 2, ..., n$ – kolejny, i-ty element rozpatrywanego systemu; $I^{B}(i|t)$ – miara ważności Birnbauma; $q_i(t)$ – prawdopodobieństwo uszkodzenia i-tego elementu rozpatrywanego systemu; $Q_0(t)$ – prawdopodobieństwo uszkodzenia rozpatrywanego systemu.

Wykorzystując zależność (5.29), miarę krytyczności można przedstawić jako:

$$I^{\mathrm{CR}}(i|t) = \frac{\dfrac{\partial Q_0(t)}{\partial q_i(t)} q_i(t)}{Q_0(t)} = \frac{\partial Q_0(t) \cdot q_i(t)}{\partial q_i(t) \cdot Q_0(t)} \tag{5.31}$$

Miarą ważności Vesely'ego–Fussella $I^{\mathrm{VF}}(i|t)$ i-tego elementu jest prawdopodobieństwo, że wystąpiło przynajmniej jedno cięcie minimalne zawierające i-ty element modelowanego systemu. Miarę ważności probabilistycznej Vesely'ego–Fussella $I^{\mathrm{VF}}(i|t)$ przedstawia zależność:

$$I^{\mathrm{VF}}(i|t) \cong \frac{1 - \prod_{j=1}^{k_i} (1 - Q_j^i(t))}{Q_0(t)} \tag{5.32}$$

którą można uprościć do postaci:

$$I^{\mathrm{VF}}(i|t) \cong \frac{\sum_{j=1}^{k_i} Q_j^i(t)}{Q_0(t)} = \frac{\sum_{j=1}^{k_j} \prod_{l \in K_j^i} q_l(t)}{Q_0(t)} \tag{5.33}$$

Postać (5.33) stanowi górną granicę miary ważności Vesely'ego–Fussella (5.32), tzn.:

$$I^{\mathrm{VF}}(i|t) \cong \frac{1 - \prod_{j=1}^{k_i} (1 - Q_j^i(t))}{Q_0(t)} \le \frac{\sum_{j=1}^{k_i} Q_j^i(t)}{Q_0(t)} = \frac{\sum_{j=1}^{k_j} \prod_{l \in K_j^i} q_l(t)}{Q_0(t)} \tag{5.34}$$

gdzie: $i = 1, 2, \ldots, n$ – kolejny, i-ty element rozpatrywanego systemu; $j = 1, 2, \ldots, k_i$ – kolejne, j-te cięcie minimalne dla rozpatrywanego systemu; K_j^i – *j-te* cięcie minimalne systemu zawierające *i-ty* element.

Im większa jest wartość miary ważności $I^{\mathrm{VF}}(i|t)$, tym większy wpływ wywiera i-ty element rozpatrywanego systemu na jego model probabilistyczny, przy czym $I^{\mathrm{VF}}(i|t) \in \langle 0,1 \rangle$.

Niech dany będzie układ o strukturze 2 z 4 (oczywiście rozpatrywany układ składa się z czterech różnych elementów). Bazując na czterech cięciach minimalnych dla układu o danej strukturze, prawdopodobieństwo niesprawności można przedstawić w postaci równania:

$$Q_0(t) \cong PFD(t) \cong q_1(t) \cdot q_2(t) \cdot q_3(t) + q_1(t) \cdot q_2(t) \cdot q_4(t) + q_1(t) \cdot q_3(t) \cdot q_4(t) + q_2(t) \cdot q_3(t) \cdot q_4(t) \tag{5.35}$$

gdzie: $PFD(t)$ – prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa; $q_1(t)$ – prawdopodobieństwo uszkodzenia pierwszego elementu; $q_2(t)$ – prawdopodobieństwo uszkodzenia drugiego elementu; $q_3(t)$ – prawdopodobieństwo uszkodzenia trzeciego elementu; $q_4(t)$ – prawdopodobieństwo uszkodzenia czwartego elementu.

Wykorzystując zależność (5.35), można wyznaczyć miary ważności dla poszczególnych elementów:

$$I^{\mathrm{VF}}(1|t) \cong \frac{Q_1^1(t)+Q_2^1(t)+Q_3^1(t)}{Q_0(t)} = \frac{q_1(t)\cdot q_2(t)\cdot q_3(t)+q_1(t)\cdot q_2(t)\cdot q_4(t)+q_1(t)\cdot q_3(t)\cdot q_4(t)}{q_1(t)\cdot q_2(t)\cdot q_3(t)+q_1(t)\cdot q_2(t)\cdot q_4(t)+q_1(t)\cdot q_3(t)\cdot q_4(t)+q_2(t)\cdot q_3(t)\cdot q_4(t)} \tag{5.36}$$

gdzie: $Q_1^1(t)$ – prawdopodobieństwo wystąpienia pierwszego cięcia zawierającego pierwszy element; $Q_2^1(t)$ – prawdopodobieństwo wystąpienia drugiego cięcia zawierającego pierwszy element; $Q_3^1(t)$ – prawdopodobieństwo wystąpienia trzeciego cięcia zawierającego pierwszy element; $Q_0(t)$ – prawdopodobieństwo niesprawności struktury 2 z 4.

$$I^{\mathrm{VF}}(2|t) \cong \frac{Q_1^2(t)+Q_2^2(t)+Q_3^2(t)}{Q_0(t)} = \frac{q_1(t)\cdot q_2(t)\cdot q_3(t)+q_1(t)\cdot q_2(t)\cdot q_4(t)+q_2(t)\cdot q_3(t)\cdot q_4(t)}{q_1(t)\cdot q_2(t)\cdot q_3(t)+q_1(t)\cdot q_2(t)\cdot q_4(t)+q_1(t)\cdot q_3(t)\cdot q_4(t)+q_2(t)\cdot q_3(t)\cdot q_4(t)} \tag{5.37}$$

gdzie: $Q_1^2(t)$ – prawdopodobieństwo wystąpienia pierwszego cięcia zawierającego drugi element; $Q_2^2(t)$ – prawdopodobieństwo wystąpienia drugiego cięcia zawierającego drugi element; $Q_3^2(t)$ – prawdopodobieństwo wystąpienia trzeciego cięcia zawierającego drugi element.

$$I^{\mathrm{VF}}(3|t) \cong \frac{Q_1^3(t)+Q_2^3(t)+Q_3^3(t)}{Q_0(t)} = \frac{q_1(t)\cdot q_2(t)\cdot q_3(t)+q_1(t)\cdot q_3(t)\cdot q_4(t)+q_2(t)\cdot q_3(t)\cdot q_4(t)}{q_1(t)\cdot q_2(t)\cdot q_3(t)+q_1(t)\cdot q_2(t)\cdot q_4(t)+q_1(t)\cdot q_3(t)\cdot q_4(t)+q_2(t)\cdot q_3(t)\cdot q_4(t)} \tag{5.38}$$

gdzie: $Q_1^3(t)$ – prawdopodobieństwo wystąpienia pierwszego cięcia zawierającego trzeci element; $Q_2^3(t)$ – prawdopodobieństwo wystąpienia drugiego cięcia zawierającego trzeci element; $Q_3^3(t)$ – prawdopodobieństwo wystąpienia trzeciego cięcia zawierającego trzeci element.

$$I^{\mathrm{VF}}(4|t) \cong \frac{Q_1^4(t)+Q_2^4(t)+Q_3^4(t)}{Q_0(t)} = \frac{q_1(t)\cdot q_2(t)\cdot q_4(t)+q_1(t)\cdot q_3(t)\cdot q_4(t)+q_2(t)\cdot q_3(t)\cdot q_4(t)}{q_1(t)\cdot q_2(t)\cdot q_3(t)+q_1(t)\cdot q_2(t)\cdot q_4(t)+q_1(t)\cdot q_3(t)\cdot q_4(t)+q_2(t)\cdot q_3(t)\cdot q_4(t)} \tag{5.39}$$

gdzie: $Q_1^4(t)$ – prawdopodobieństwo wystąpienia pierwszego cięcia zawierającego czwarty element; $Q_2^4(t)$ – prawdopodobieństwo wystąpienia drugiego cięcia zawierającego czwarty element; $Q_3^4(t)$ – prawdopodobieństwo wystąpienia trzeciego cięcia zawierającego czwarty element.

Jeżeli na podstawie powyższych równań spełniona zostałaby poniższa nierówność:

$$I^{\mathrm{VF}}(2|t) \le I^{\mathrm{VF}}(1|t) \le I^{\mathrm{VF}}(4|t) \le I^{\mathrm{VF}}(3|t) \tag{5.40}$$

wówczas można stwierdzić, że największy wpływ na model probabilistyczny rozpatrywanego systemu ma element trzeci o prawdopodobieństwie uszkodzenia $q_3(t)$, natomiast najmniejszy wpływ – element drugi.

Przedstawione zależności oraz uzyskane „hipotetycznie" wyniki znajdują zastosowanie, gdy znana jest wartość prawdopodobieństwa uszkodzenia każdego elementu systemu i wartość ta nie jest uzależniona od rygorów czasowych, np. dla elementu pierwszego $q_1(t) \Rightarrow q_1$, gdzie $q_1 \in \langle 0,1 \rangle$.

Przy założeniu takiego samego czasu t dla całego systemu, a więc jednakowego dla wszystkich elementów, zależności (5.36)–(5.39) można przedstawić w następujący sposób:

$$I^{\mathrm{VF}}(1|t) \cong \frac{(\lambda_1\cdot\lambda_2\cdot\lambda_3+\lambda_1\cdot\lambda_2\cdot\lambda_4+\lambda_1\cdot\lambda_3\cdot\lambda_4)t^3}{(\lambda_1\cdot\lambda_2\cdot\lambda_3+\lambda_1\cdot\lambda_2\cdot\lambda_4+\lambda_1\cdot\lambda_3\cdot\lambda_4+\lambda_2\cdot\lambda_3\cdot\lambda_4)t^3} = \frac{(\lambda_1\cdot\lambda_2\cdot\lambda_3+\lambda_1\cdot\lambda_2\cdot\lambda_4+\lambda_1\cdot\lambda_3\cdot\lambda_4)}{(\lambda_1\cdot\lambda_2\cdot\lambda_3+\lambda_1\cdot\lambda_2\cdot\lambda_4+\lambda_1\cdot\lambda_3\cdot\lambda_4+\lambda_2\cdot\lambda_3\cdot\lambda_4)} \tag{5.41}$$

gdzie: λ_1 – intensywność uszkodzeń elementu pierwszego; λ_2 – intensywność uszkodzeń elementu drugiego; λ_3 – intensywność uszkodzeń elementu trzeciego; λ_4 – intensywność uszkodzeń elementu czwartego; t – czas.

$$I^{\mathrm{VF}}(2|t) \cong \frac{(\lambda_1 \cdot \lambda_2 \cdot \lambda_3 + \lambda_1 \cdot \lambda_2 \cdot \lambda_4 + \lambda_2 \cdot \lambda_3 \cdot \lambda_4)}{(\lambda_1 \cdot \lambda_2 \cdot \lambda_3 + \lambda_1 \cdot \lambda_2 \cdot \lambda_4 + \lambda_1 \cdot \lambda_3 \cdot \lambda_4 + \lambda_2 \cdot \lambda_3 \cdot \lambda_4)} \tag{5.42}$$

$$I^{\mathrm{VF}}(3|t) \cong \frac{(\lambda_1 \cdot \lambda_2 \cdot \lambda_3 + \lambda_1 \cdot \lambda_3 \cdot \lambda_4 + \lambda_2 \cdot \lambda_3 \cdot \lambda_4)}{(\lambda_1 \cdot \lambda_2 \cdot \lambda_3 + \lambda_1 \cdot \lambda_2 \cdot \lambda_4 + \lambda_1 \cdot \lambda_3 \cdot \lambda_4 + \lambda_2 \cdot \lambda_3 \cdot \lambda_4)} \tag{5.43}$$

$$I^{\mathrm{VF}}(4|t) \cong \frac{(\lambda_1 \cdot \lambda_2 \cdot \lambda_4 + \lambda_1 \cdot \lambda_3 \cdot \lambda_4 + \lambda_2 \cdot \lambda_3 \cdot \lambda_4)}{(\lambda_1 \cdot \lambda_2 \cdot \lambda_3 + \lambda_1 \cdot \lambda_2 \cdot \lambda_4 + \lambda_1 \cdot \lambda_3 \cdot \lambda_4 + \lambda_2 \cdot \lambda_3 \cdot \lambda_4)} \tag{5.44}$$

Jeżeli na podstawie powyższych zależności spełniona zostałaby nierówność (5.40), wówczas można stwierdzić, że największy wpływ na model probabilistyczny rozpatrywanego systemu ma element trzeci o intensywności uszkodzeń λ_3 natomiast najmniejszy – element o intensywności uszkodzeń λ_2.

Sytuacja przedstawiona powyżej stanowi jednak nadal dość szczególny przypadek o bardzo uproszczonych założeniach. Każdy element systemu może być naprawialny lub nienaprawialny. Natomiast średni czas naprawy *MTTR* każdego elementu może być różny, np. $MTTR_1 \neq MTTR_2 \neq MTTR_3 \neq MTTR_4$. W takiej sytuacji określenie miar ważności może się okazać trudne w realizacji, tym bardziej że średni czas naprawy (w zależności od jego wartości) będzie miał znaczny wpływ na postać wynikową miary ważności, a zatem analiza wrażliwości modelu probabilistycznego będzie skomplikowana. Przy założeniu, że czas między testami okresowymi jest stały i wynosi T_I, prawdopodobieństwo uszkodzenia *i*-tego elementu systemu określa zależność $q_i(t) = \lambda_i \cdot t_{Ci}$, gdzie $t_{Ci} = t + MTTR_i$ jest ekwiwalentem czasowym; wówczas prawdopodobieństwo uszkodzenia rozpatrywanej struktury wynosi:

$$\begin{aligned}
&Q_0(t) \cong PFD(t) = q_1(t) \cdot q_2(t) \cdot q_3(t) + q_1(t) \cdot q_2(t) \cdot q_4(t) + q_1(t) \cdot q_3(t) \cdot q_4(t) + q_2(t) \cdot q_3(t) \cdot q_4(t) = \\
&= \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} = \\
&= \lambda_1(t + MTTR_1)\lambda_2(t + MTTR_2)\lambda_3(t + MTTR_3) + \lambda_1(t + MTTR_1)\lambda_2(t + MTTR_2)\lambda_4(t + MTTR_4) + \\
&+ MTTR_2)\lambda_4(t + MTTR_4) + \lambda_1(t + MTTR_1)\lambda_3(t + MTTR_3)\lambda_4(t + MTTR_4) + \\
&+ \lambda_2(t + MTTR_2)\lambda_3(t + MTTR_3)\lambda_4(t + MTTR_4)
\end{aligned} \tag{5.45}$$

gdzie: λ_1 – intensywność uszkodzeń elementu pierwszego; λ_2 – intensywność uszkodzeń elementu drugiego; λ_3 – intensywność uszkodzeń elementu trzeciego; λ_4 – intensywność uszkodzeń elementu czwartego; t – czas; $MTTR_1$ – średni czas naprawy pierwszego elementu; $MTTR_2$ – średni czas naprawy drugiego elementu; $MTTR_3$ – średni czas naprawy trzeciego elementu; $MTTR_4$ – średni czas naprawy czwartego elementu; t_{C1} – ekwiwalent czasowy dla elementu pierwszego; t_{C2} – ekwiwalent czasowy dla elementu drugiego; t_{C3} – ekwiwalent czasowy dla elementu trzeciego; t_{C4} – ekwiwalent czasowy dla elementu czwartego.

Przy uwzględnieniu wzoru (5.45) miary ważności określone zależnościami (5.36)–(5.39) będą miały postać:

$$\begin{aligned}
&I^{\mathrm{VF}}(1|t) \approx \frac{Q_1^1(t) + Q_2^1(t) + Q_3^1(t)}{Q_0(t)} = \\
&= \frac{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}}{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}}
\end{aligned} \tag{5.46}$$

gdzie: λ_1 – intensywność uszkodzeń elementu pierwszego; λ_2 – intensywność uszkodzeń elementu drugiego; λ_3 – intensywność uszkodzeń elementu trzeciego; λ_4 – intensywność uszkodzeń elementu czwartego; t – czas; $MTTR_1$ – średni czas naprawy pierwszego elementu; $MTTR_2$ – średni czas naprawy drugiego elementu; $MTTR_3$ – średni czas naprawy trzeciego elementu; $MTTR_4$ – średni czas naprawy czwartego elementu; $t_{C1} = t + MTTR_1$ – ekwiwalent czasowy dla elementu pierwszego; $t_{C2} = t + MTTR_2$ – ekwiwalent czasowy dla elementu drugiego; t_{C3} – ekwiwalent czasowy dla elementu trzeciego; t_{C4} – ekwiwalent czasowy dla elementu czwartego.

$$I^{\mathrm{VF}}(2|t) \approx \frac{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}}{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}} \tag{5.47}$$

$$I^{\mathrm{VF}}(3|t) \approx \frac{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}}{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}} \tag{5.48}$$

$$I^{\mathrm{VF}}(4|t) \approx \frac{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}}{\lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} + \lambda_1 \cdot t_{C1} \cdot \lambda_2 \cdot t_{C2} \cdot \lambda_4 \cdot t_{C4} + \lambda_1 \cdot t_{C1} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4} + \lambda_2 \cdot t_{C2} \cdot \lambda_3 \cdot t_{C3} \cdot \lambda_4 \cdot t_{C4}} \tag{5.49}$$

Jeżeli na podstawie powyższych zależności spełniona zostałaby nierówność (5.40), wówczas można stwierdzić, że największy wpływ na model probabilistyczny rozpatrywanego systemu ma element trzeci o intensywności uszkodzeń λ_3 i średnim czasie naprawy $MTTR_3$, natomiast najmniejszy – element o intensywności uszkodzeń λ_2 i średnim czasie naprawy $MTTR_2$.

W przypadku bardziej złożonych układów, w których o prawdopodobieństwie uszkodzenia pojedynczego elementu systemu decyduje wiele parametrów, wyznaczenie miar ważności, a tym samym redukcja modelu probabilistycznego do prostszej postaci są skomplikowane. W dalszych analizach podczas konstrukcji modeli probabilistycznych systemów sterowania i zabezpieczeniowych spośród trzech proponowanych miar ważności parametrów rozpatrywanych systemów wykorzystywana będzie miara ważności Vesely'ego–Fussella $I^{\mathrm{VF}}(i|t)$.

5.6. Podsumowanie

Poziomy nienaruszalności bezpieczeństwa SIL systemów realizujących funkcje bezpieczeństwa są weryfikowane na podstawie punktowych wartości przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie PFD_{avg} oraz prawdopodobieństwa występowania uszkodzenia niebezpiecznego na godzinę PFH względem przedziałów kryterialnych prawdopodobieństw odpowiadających poszczególnym poziomom dla struktur ograniczonych architektonicznie. Przedstawione w normach bezpieczeństwa funkcjonalnego metody dotyczące obliczania wartości prawdopodobieństw nie uwzględniają oceny niepewności uzyskanych wyników oraz badania wrażliwości modeli probabilistycznych wykorzystywanych w obliczeniach. W niniejszej monografii zaproponowano metody wykorzystujące technikę cięć minimalnych i równań uproszczonych, przydatne w weryfikacji SIL systemów sterowania i zabezpieczeń w odniesieniu do punktowych wartości prawdopodobieństw. Metody te pozwalają na modelowanie systemów E/E/PE o dowolnej konfiguracji, niekoniecznie składających się z jednakowych elementów [192, 195–198, 202–204].

Biorąc pod uwagę opinie ekspertów dotyczące występowania problemu oceny niepewności w oszacowaniach probabilistycznych i brak odpowiednich propozycji dotyczą-

cych zagadnień uwzględnienia niepewności w normach PN-EN 61508 i PN-EN 61511, istotne jest opracowanie i wdrożenie metody pozwalającej na porównywanie wynikowych punktowych i/lub przedziałowych miar probabilistycznych uzyskanych dla analizowanych struktur systemów sterowania i zabezpieczeń z przedziałami kryterialnymi, które byłyby rozszerzeniem podejścia proponowanego w tych normach. Ponadto zaproponowana metoda badania wrażliwości modeli probabilistycznych systemów E/E/PE pozwala na uwzględnienie w modelowaniu tylko tych parametrów, które mają największy wpływ na wartość wynikową prawdopodobieństwa. Takie podejście pozwala na znacznie szybsze uzyskanie końcowej oceny dotyczącej bezpieczeństwa funkcjonalnego analizowanego systemu. Ocena niepewności jest reprezentowana za pomocą rozkładu probabilistycznego z konwersją przedziałową quasi-rozmytą.

Zaproponowana metoda oceny wartości punktowych prawdopodobieństw z uwzględnieniem dolnej i górnej granicy na podstawie techniki wskaźników różnicowych zostanie wykorzystana w integracji bezpieczeństwa funkcjonalnego i ochrony informacji w procesie weryfikacji SIL przy uwzględnieniu wpływu cyberzagrożeń. Problematyka uwzględnienia w modelowaniu probabilistycznym systemów zintegrowanej koncepcji bezpieczeństwa funkcjonalnego i ochrony informacji zostanie przedstawiona w kolejnych rozdziałach niniejszej monografii.

Rozdział 6

OKREŚLANIE WYMAGANEGO SIL DLA FUNKCJI BEZPIECZEŃSTWA Z UWZGLĘDNIENIEM ASPEKTÓW OCHRONY INFORMACJI

6.1. Wprowadzenie

Dokument normatywny PN-EN 61508 [161] oraz norma branżowa PN-EN 61511 [162] dla przemysłu procesowego wprowadzają podejście opierające się na analizie ryzyka w celu określenia wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla funkcji bezpieczeństwa, podając przy tym pewne przykłady metod wykorzystywanych do jego określania. Koncepcja ta odnosi się zarówno do określenia wymaganej redukcji ryzyka związanej z rozpatrywanym zdarzeniem awaryjnym, jak i do wymagań technicznych stawianych systemowi, który będzie implementować określone funkcje związane z bezpieczeństwem. Oba wymienione dokumenty dostarczają również informacji ogólnych na temat podstawowych koncepcji ryzyka oraz powiązania ryzyka z poziomem nienaruszalności bezpieczeństwa, wraz z przedstawieniem modelu ryzyka wykorzystywanego w procesie określania wymaganego SIL. Widać coraz większą świadomość konieczności włączenia ochrony informacji w systemach technicznych do analiz bezpieczeństwa obiektów przemysłowych.

W wymienionych powyżej dokumentach normatywnych zagadnienie związane z ochroną informacji zostało przedstawione jako jeden z punktów, które należy rozpatrywać w ramach analiz bezpieczeństwa funkcjonalnego. Nie zostały jednak zaprezentowane metody, które w usystematyzowany sposób pomogłyby przeprowadzić analizy bezpieczeństwa funkcjonalnego z uwzględnieniem aspektów ochrony informacji. Dlatego w niniejszej monografii proponuje się metodykę, która łączy ze sobą klasyfikację systemów z punktu widzenia ich podatności na zagrożenia związane ściśle z lukami bezpieczeństwa ochrony informacji oraz pewne wytyczne stosowania danych o określonym poziomie ochrony informacji z metodą oceny ryzyka systemów technicznych. W rezultacie poprzez zdiagnozowanie posiadania niewystarczających środków ochrony informacji w systemie sterowania BPCS wymagane może być zwiększenie wymagań dotyczących poziomu nienaruszalności bezpieczeństwa SIL analizowanych funkcji związanych z bezpieczeństwem. Są one wprowadzane do systemu w celu zredukowania ryzyka pracy systemu technicznego do poziomu przynajmniej tolerowanego i wymagają przeprowadzenia dokładnej analizy ryzyka, obejmującej proces identyfikacji zdarzeń awaryjnych oraz zagrożeń, jak również przyporządkowanie wymagań bezpieczeństwa (w tym SIL) do tych funkcji.

6.2. Nowoczesne systemy techniczne i ich podatności

Z perspektywy analizy bezpieczeństwa funkcjonalnego system techniczny jest rozumiany jako uporządkowany zbiór elementów o określonym poziomie złożoności, które pracując w określonym otoczeniu i warunkach środowiskowych, realizują zdefiniowane

funkcje (w tym funkcje bezpieczeństwa, np. SIF). Według PN-IEC 60300-3-9 [170] w skład systemu technicznego mogą wchodzić m.in. takie elementy, jak:
— wyposażenie i infrastruktura techniczna;
— personel;
— procedury;
— materiały;
— energia;
— osprzęt sieciowy i komputerowy wraz z oprogramowaniem.

W większości działających zakładów przemysłowych wykorzystuje się infrastrukturę techniczną zawierającą automatyczne systemy sterowania. Gwarantuje to m.in. zachowanie jakości i ciągłości produkcji, jak również zwiększenie wydajności pracy zakładu. Jednym z ważnych czynników, które także wynikają z zastosowania takiej technologii, jest zminimalizowanie koniecznych przy produkcji prac wykonywanych ręcznie przez obsługę, co znacznie redukuje możliwość popełnienia błędów przez człowieka oraz poprawia bezpieczeństwo operacji. Biorąc pod uwagę system sterowania pracujący w przemyśle, głównie procesowym, można w nim wyodrębnić: podstawowy system pomiarów i sterowania BPCS (*basic process control system*) oraz system związany z bezpieczeństwem SRS (*safety-related system*) lub wykonany w technologii E/E/PE system zabezpieczeń SIS (*safety instrumented system*). System BPCS pełni funkcję typowego automatycznego systemu sterowania, dbającego o poprawny przebieg funkcji produkcyjnych. Natomiast system bezpieczeństwa SIS jest projektowany w sposób gwarantujący wypełnianie określonych funkcji bezpieczeństwa. Oba systemy często korzystają z podobnych rozwiązań technologicznych, choć odpowiednio wysoki stopień bezpieczeństwa systemu zabezpieczającego można osiągnąć głównie poprzez stosowanie niezawodnych, certyfikowanych urządzeń automatyki zabezpieczeniowej i/lub architektury redundantnej. Coraz częściej dąży się jednak do tego, aby oba systemy BPCS i SIS działały w oparciu o wspólne elementy [24]. Zintegrowany system BPCS i SIS znacznie zmniejsza koszty instalacji systemu sterowania i automatyki zabezpieczeniowej ale z drugiej strony wprowadza czynnik zwiększający jego zawodność [131]. Stąd zalecenia, zawarte w dokumentach normatywnych dotyczących systemów zabezpieczeń, aby architektura obu systemów była niezależna [131, 161, 162].

Elementy wchodzące w skład systemu sterowania lub zabezpieczeń mogą być rozmieszczone w różnych miejscach zakładu przemysłowego, czasem w lokalizacjach od siebie znacznie oddalonych. W takim przypadku mamy do czynienia z rozproszonym systemem sterowania DCS (*distributed control system*). W dużych zakładach przemysłowych, ze względu na ich rozległość, jest to wręcz rozwiązanie nieuniknione i znacznie ułatwiające zarządzanie takim systemem. Z drugiej strony powoduje to powstanie dodatkowych źródeł zagrożeń w systemie, związanych z szeroko rozumianą ochroną informacji tego typu infrastruktury. Architektura takich systemów wymusza stosowanie zaawansowanych rozwiązań sieciowych oraz informatycznych [4, 49, 209]. Często jest ona oparta na różnego rodzaju systemach komunikacji (rys. 2.4). Oprócz niewątpliwych walorów ułatwionej obsługi tego typu systemów pojawiają się także nowe problemy natury technicznej, organizacyjnej oraz – przede wszystkim – dotyczące bezpieczeństwa danych, np. procesowych, statystycznych itp. [130]. W związku z możliwością utraty integralności danych czy też nieuprawnionego dostępu do informacji w analizach bezpieczeństwa należy zatem brać pod uwagę także nowe czynniki ryzyka związane z tym zagadnieniem [17].

6.3. Zagadnienia bezpieczeństwa transmisji danych

Kanały komunikacyjne mogą być również narażone na intencyjne działanie osób trzecich, próbujących zakłócić działanie systemu. Projektując rozproszony system automatyki, należy więc rozważyć możliwe ataki na sieć komunikacyjną i zabezpieczyć się przed nimi. Podstawowe rodzaje zagrożeń bezpieczeństwa transmisji danych to: podsłuchiwanie, modyfikacja danych, podstawienie danych i ataki na dostępność danych.

Podsłuchiwanie (*sniffing*) jest formą ataku biernego [100], w którym zagrożona jest poufność przesyłanych danych. Atakujący, poprzez dołączenie się do sieci w trybie nasłuchu, może rejestrować wszystkie dane przekazywane przez określony segment sieci. Atakujący nie modyfikuje ani nie wprowadza danych do sieci, dlatego atak tego typu jest bardzo trudny do wykrycia. Obrona polega najczęściej na wprowadzeniu mechanizmów zapewnienia poufności danych, opartych na algorytmach szyfrowania. Wprawdzie w przypadku zastosowań przemysłowych poprzez sieć przekazywane są głównie informacje pomiarowe i sterujące, nieprzedstawiające przeważnie większej wartości dla atakującego, szyfrowanie może być jednak potrzebne do zapewnienia realizacji innych wymagań bezpieczeństwa, takich jak aktualność czy autentyczność danych.

Modyfikacja danych stanowi z kolei formę ataku aktywnego, w którym atakujący przechwytuje dane, modyfikuje je i ponownie wprowadza do sieci. Modyfikacja może mieć na celu wprowadzenie w błąd operatora, aktywowanie określonego obwodu sterowania, uzyskanie dostępu do zasobów itp. W systemach przemysłowych, opartych głównie na sieciach lokalnych, ta forma ataku jest trudna do przeprowadzania, gdyż wymaga od intruza fizycznego włączenia się w tor przesyłania danych pomiędzy nadawcą i odbiorcą. Niemniej jest prawdopodobna i należy się przed nią zabezpieczyć, wprowadzając mechanizmy zapewniające integralność i autentyczność danych. Mechanizmy te powinny uniemożliwiać zmodyfikowanie przesyłanych danych bez zauważenia tego przez odbiorcę. Najpopularniejszym rozwiązaniem zapewniającym integralność danych jest stosowanie tzw. funkcji skrótu. Pozwalają one na obliczenie swoistego podpisu elektronicznego w postaci sekwencji bitów dołączanej do wysyłanej wiadomości, zależnej od liczby i wartości wysyłanych bajtów danych. Odbiorca może wyliczyć tę wartość według tego samego algorytmu i porównać z dołączonym podpisem. Podczas wyliczania funkcji skrótu uwzględnia się najczęściej dodatkowy ciąg danych, tzw. klucz, znany tylko uprawnionym stronom. Uniemożliwia to osobie nieuprawnionej zmodyfikowanie i ponowne podpisanie zmodyfikowanych danych, nawet wtedy, gdy zna ona algorytm wyliczania skrótu.

Podstawienie danych jest formą ataku, w którym atakujący wprowadza do sieci dane, podszywając się często pod innego uprawnionego nadawcę. Ponieważ przed wprowadzeniem własnych danych przeważnie chronią opisywane wcześniej mechanizmy zapewnienia integralności i autentyczności danych, to do tego typu ataku są często wykorzystywane zarejestrowane wcześniej oryginalne dane innego nadawcy. W ten sposób atakujący może próbować np. zmienić stan sterowanego obiektu za pomocą zarejestrowanej wcześniej sekwencji danych sterujących, bez konieczności jakiejkolwiek ich modyfikacji. Do ochrony przed tego typu atakami służą mechanizmy zapewnienia aktualności (świeżości) przesyłanych danych. Najczęściej sprowadzają się one do użycia tzw. stempla czasu lub odpowiedniej sekwencji numeracji wiadomości w połączeniu z mechanizmem zapewnienia integralności danych.

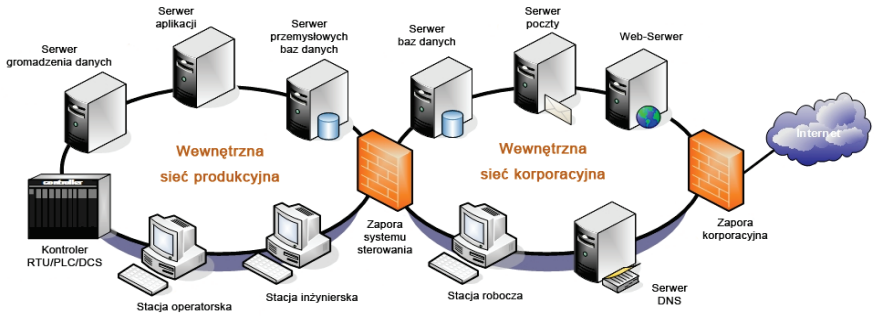
Ataki na dostępność danych stanowią najczęstszą i najtrudniejszą do obrony formę ataków. Są to ataki aktywne, których celem jest zakłócenie pracy sieci, tak aby zablokować możliwość normalnego przekazywania danych. Atak tego rodzaju można zrealizować na bardzo wiele sposobów, takich jak: fizyczne uszkodzenie (np. zwarcie lub przecięcie) ma-

gistrali, generowanie bardzo dużego ruchu blokującego dostęp do magistrali innym węzłom, modyfikowanie przesyłanych danych powodujące ich niszczenie lub wprowadzanie do sieci specjalnie spreparowanych danych, których przetwarzanie przeciąża węzły, do których są kierowane. W typowych lokalnych sieciach przemysłowych zapobieganie tego typu atakom jest bardzo trudne do zrealizowania w inny sposób niż uniemożliwienie fizycznego dostępu do sieci osobom nieupoważnionym. Częściowym rozwiązaniem tego problemu jest wprowadzenie mechanizmów monitorowania stanu sieci, pozwalających na wykrycie obecności tego typu ataków i zlokalizowanie ich miejsca. W sieciach bardziej rozbudowanych, zawierających programowalne przełączniki i routery, istnieją dodatkowe możliwości ochrony lub przynajmniej ograniczania skutków ataku, dzięki możliwości separacji podsieci i filtrowania przesyłanych pomiędzy nimi danych.

Najskuteczniejszy i najczęściej wykorzystywany sposób zabezpieczenia sieci przemysłowej przed atakami polega na jej **izolowaniu** od innych sieci i ochronie przed fizycznym dostępem osób niepowołanych. W przypadku sieci polowych, stosowanych na najniższym poziomie struktury systemu automatyki i zabezpieczeń, jest to przeważnie możliwe do wykonania, gdyż sieci te obejmują zwykle niewielki obszar, pokrywający się z obszarem sterowanego obiektu technologicznego, który sam w sobie jest chroniony.

Trudniejsze jest izolowanie sieci zarządzania, która integruje sterowniki z systemami SCADA i może być łączona z siecią biurową przedsiębiorstwa lub nawet z sieciami publicznymi w celu umożliwienia wybranym osobom dostępu do danych procesowych i informacji o zdarzeniach. W takim przypadku izolowanie sieci wymaga użycia tzw. zapór ogniowych, czyli specjalizowanych bramek i routerów filtrujących ruch międzysieciowy.

Na rys. 6.1 przedstawiono koncepcję pracy dwóch różnych sieci – korporacyjnej oraz przemysłowej, które tworzą tzw. strefy.



Rys. 6.1. Funkcjonowanie dwóch różnych rodzajów sieci (stref) w obiekcie technicznym [207]

Główną rolą sieci korporacyjnej jest umożliwienie przesyłania dużych ilości danych pomiędzy poszczególnymi elementami takiego systemu, czyli najczęściej komputerami poszczególnych pracowników biurowych. Główna rola sieci przemysłowej polega z kolei na zapewnieniu ciągłego i bezawaryjnego przesyłu danych w ogólnie pojmowanym procesie automatyzacji. W pewnych obiektach technicznych może istnieć punkt styku obu tych „światów", dzięki czemu pewne dane z sieci przemysłowej mogą być dostępne w sieci administracyjnej i na odwrót. Z punktu widzenia ochrony informacji stwarza to możliwość ingerencji w funkcjonowanie jednej z nich z zewnątrz, co dotyczy przede wszystkim możliwości celowej działalności, np. sabotażu na systemie sterowania zainstalowanego w omawianym obiekcie. Dlatego dobre rozpoznanie istoty tego problemu może się przy-

czynić do zastosowania odpowiednich środków zaradczych, które zminimalizują ryzyko związane z możliwymi zagrożeniami. W dokumencie [207] zaproponowano klasyfikację opisanych powyżej stref sieciowych na cztery główne architektury rozproszonych systemów technicznych.

W pierwszym przypadku strefy związane z sieciami korporacyjnymi oraz przemysłowymi są połączone ze sobą przy pomocy tzw. firewalla (zapory ogniowej), czyli rozwiązania, które ma na celu chronić przed nieautoryzowanym dostępem do sieci przemysłowej. W praktyce oznacza to zainstalowanie specjalnych rozwiązań sprzętowych oraz programowych i odpowiednie ich skonfigurowanie przez odpowiednio przygotowane do tego zadania kadry. Sieć korporacyjna również ma swoje zabezpieczenie w postaci zapory ogniowej po stronie dostępu tej sieci do Internetu. Rozwiązania stosowane przy tego typu architekturze sieciowej mogą być bardzo różne. Zarządzanie siecią korporacyjną, a co za tym idzie – również odpowiednia dbałość o poprawne funkcjonowanie zaszytych w niej zabezpieczeń, często są realizowane przez odrębną grupę osób niż w sieci przemysłowej.

Kolejna architektura sieciowa odnosi się do innego spotykanego rozwiązania, jakim jest wydzielenie sieci przemysłowej z działającej i istniejącej sieci korporacyjnej. Można powiedzieć, że powstaje wtedy tzw. strefa zdemilitaryzowana DMZ (*demilitarized zone*), do której dostęp odbywa się na zasadach z góry określonych przez politykę bezpieczeństwa danego obiektu technicznego. W strukturze takiej występuje jedna zapora ogniowa, pełniąca podwójną funkcję – ochrony dostępu do zasobów sieci korporacyjnej oraz zabezpieczenia kluczowych aspektów związanych z ochroną informacji i dostępu do sieci przemysłowej. W takim rozwiązaniu o poprawność funkcjonowania oraz konfiguracji takich zabezpieczeń dba jeden zespół techników, najczęściej informatyków zajmujących się zarządzaniem wszystkimi sieciami dostępnymi w obiekcie.

W dużych, rozległych obiektach technicznych zachodzi czasem potrzeba zastosowania pewnej infrastruktury, która już funkcjonuje, aby „przedłużyć" pole oddziaływania strefy przemysłowej. Wiele zdecentralizowanych systemów sterowania może się dzięki temu komunikować między sobą, jednocześnie nie powodując wzrostu kosztów inwestycji w te systemy. Rozwiązanie takie powoduje jednak konieczność rozbudowy tego rodzaju architektury o dodatkowe elementy związane z zabezpieczeniami, m.in. o dodatkowe zapory ogniowe oddzielające sieć korporacyjną od podsieci przemysłowych.

Ostatnią zaproponowaną architekturą jest rozwiązanie dotyczące umiejscowienia wspólnego punktu dostępu do danych – najczęściej danych procesowych z obiektu i systemów sterowania w nim pracujących – we wspólnej strefie zdemilitaryzowanej. Dostęp do niej może zostać przypisany zarówno osobom pracującym w strefie administracyjnej, jak i elementom systemu przemysłowego. Rozwiązanie to ma niewątpliwą zaletę związaną z usunięciem bezpośredniego połączenia pomiędzy dwiema omawianymi strefami.

Mimo że w wymienionych rozwiązaniach mogą być stosowane różnego rodzaju zabezpieczenia, od najprostszych po najbardziej wyrafinowane, zawsze istnieją takie punkty w systemie, które determinują istnienie podatności tego systemu na występowanie różnego rodzaju zagrożeń. W związku z tym warto w tym miejscu zawrzeć bardzo ważną informację, że jedynie całkowite odseparowanie obu opisanych stref może wyeliminować zagrożenia związane z nieautoryzowanym dostępem do sieci przemysłowej z zewnątrz tej strefy. Dotyczy to oczywiście wyłącznie zagrożeń opartych na działaniach wykorzystujących połączenia sieciowe, ponieważ w systemie nadal mogą istnieć podatności związane z działaniem osób na terenie strefy przemysłowej. Jest to jednak już odrębne zagadnienie, które nie zostało omówione w niniejszej monografii.

Znając podstawowy podział systemów na ich architektury, można się skupić na strefie przemysłowej i strukturach, które mogą być w niej wykorzystywane. Należy pamiętać, że w przypadku łączenia sieci skuteczność ochrony zależy od skuteczności działania zapór ogniowych i zastosowanych w nich zabezpieczeń. Niedostateczna ochrona może być wynikiem zastosowania nieodpowiednich metod zabezpieczeń, błędów konfiguracyjnych, jak również ukrytych błędów oprogramowania zapór ogniowych, dlatego też elementy te powinny być przedmiotem odpowiedniej oceny skuteczności zabezpieczeń.

Niekiedy nie można zastosować fizycznej ochrony medium komunikacyjnego. Ten problem występuje najczęściej w instalacjach rozległych, takich jak systemy elektroenergetyczne, hydrotechniczne czy rozproszone systemy automatyki budynków. Dotyczy to również sieci bezprzewodowych, których zasięg nie jest w pełni kontrolowany. W takich sytuacjach konieczne jest wdrożenie odpowiednich mechanizmów kryptograficznych na poziomie protokołów transmisji danych. Do zabezpieczenia informacji wykorzystuje się najczęściej algorytmy szyfrowania z kluczem symetrycznym, algorytmy szyfrowania z kluczem niesymetrycznym oraz funkcje skrótu umożliwiające zabezpieczenie informacji przed nieautoryzowaną modyfikacją.

Szyfrowanie z kluczem symetrycznym jest jednym z najefektywniejszych sposobów zapewnienia poufności przesyłanych danych. Do szyfrowania i deszyfrowania danych wykorzystuje się ten sam klucz, który powinien być znany jedynie nadawcy i odbiorcy informacji. Obecnie najpopularniejszymi algorytmami szyfrowania symetrycznego są algorytmy 3DES [5, 143] oraz nowszy AES [142]. Zaletę tego typu algorytmów stanowi stosunkowo krótki w porównaniu z algorytmami niesymetrycznymi czas potrzebny do zaszyfrowania/ odszyfrowania danych. Niestety, w przypadku wielu nadawców/ odbiorców danych występują problemy związane z zarządzaniem kluczami. Jeżeli klucz jest wspólny, rośnie ryzyko jego ujawnienia, ponadto każdy nadawca informacji może odczytać informację nadaną przez inny węzeł. Jeżeli zaś klucze są niezależne dla każdej pary komunikujących się węzłów, to pojawiają się problemy związane z przechowywaniem dużej liczby kluczy.

Szyfrowanie z kluczem niesymetrycznym opiera się na wykorzystaniu dwóch rodzajów kluczy. Pierwszy z nich, nazywany kluczem publicznym, może być powszechnie znany i pozwala każdemu nadawcy poufnej informacji na jej zaszyfrowanie. Drugi, nazywany kluczem prywatnym, znany jest tylko odbiorcy i jest niezbędny do odczytania informacji. Szyfrowanie z kluczem niesymetrycznym może być również wykorzystywane do generacji podpisów cyfrowych. Przykładami popularnych algorytmów niesymetrycznych są RSA [183] i DSA [144]. Wadą algorytmów szyfrowania niesymetrycznego jest dużo dłuższy czas przetwarzania danych w porównaniu z algorytmami symetrycznymi. Dlatego w wielu praktycznych rozwiązaniach szyfrowanie niesymetryczne wykorzystuje się jedynie do ustalenia i bezpiecznego przekazania klucza symetrycznego, który jest wykorzystywany w dalszej transmisji danych.

Funkcje skrótu to funkcje jednokierunkowe, które pozwalają na generowanie krótkich i łatwych do weryfikacji sygnatur dla dowolnie dużych zbiorów danych. Sygnatury te, dołączane do wiadomości, których dotyczą, umożliwiają wykrycie przypadkowych lub celowo wprowadzonych modyfikacji danych. Dzięki nim możliwe jest też uniknięcie przechowywania wrażliwych danych, takich jak np. login i hasło, i zastąpienie ich skrótem, który jest porównywany z podobnym skrótem obliczanym na podstawie danych wprowadzanych przez logującego się użytkownika. Często stosowane funkcje skrótu to SHA [181], MD5 [179] oraz bazująca na nich metoda HMAC [180], umożliwiająca zapewnienie integralności i autentyczności zabezpieczonych w ten sposób danych.

W celu jednoczesnego zapewnienia integralności, poufności i aktualności danych zwykle stosuje się hybrydę kilku różnych metod kryptograficznych. Przykładami takich kompleksowych metod są protokoły IPsec [125] oraz TSL [182], bardzo często wykorzystywane w sieci Internet, oraz WPA [138], stosowane do ochrony sieci bezprzewodowych Wi-Fi [40, 153].

6.4. Ochrona informacji z punktu widzenia analiz bezpieczeństwa funkcjonalnego

Analiza ryzyka odnosząca się do zagadnień ochrony informacji wiąże się z kilkoma podstawowymi etapami, mającymi swoje odpowiedniki w analizie bezpieczeństwa funkcjonalnego. Pierwszym etapem, od którego należy rozpocząć analizę systemu technicznego pod względem ochrony, jest identyfikacja zasobów, które są cenne dla przedsiębiorstwa i których utrata wiązałaby się z możliwymi do oszacowania stratami. Zasobami takimi mogą być zarówno środki trwałe w postaci aktywów i pasywów firmy, takie jak np. infrastruktura, sprzęt, oprogramowanie itp., jak i środki trudniejsze do policzenia i wyceny, jak np. dane, informacje, wiedza pracowników itp. Jeśli założy się, że wymienione powyżej zasoby są cenne, powinno się je chronić przez odpowiednio dobrane zabezpieczenia. Kolejne kroki w analizie ochrony to identyfikacja zagrożeń przypisanych do każdego zasobu oraz analiza podatności systemu na te zagrożenia. Na tym etapie należy przewidzieć, jakie są przyczyny (źródła) wystąpienia zidentyfikowanego zagrożenia oraz jak dane zagrożenie może wpłynąć na analizowany zasób.

W nawiązaniu do teorii ochrony informacji można stwierdzić, że straty związane z tego typu zagrożeniami można sklasyfikować w trzech kategoriach [171]:

— utrata jawności;
— utrata integralności;
— utrata dostępności danych, informacji itp.

Po zidentyfikowaniu podatności zasobów oraz zagrożeń z nimi związanych należy przejść do etapu oceny ryzyka. Na tym etapie konieczne staje się oszacowanie skutków wystąpienia zagrożenia, jak również prawdopodobieństwa jego zajścia. Na podstawie informacji, jak często dany zasób może być narażony na określone zagrożenie, oraz sklasyfikowania skutków jego wystąpienia można określić wymagania, jakie będą stawiane systemowi ochrony. Może on dotyczyć ochrony informacji lub też ochrony dostępu; w obu przypadkach wymagania będą się od siebie różnić, ale ich cel pozostanie ten sam – zniwelować niekorzystne skutki wystąpienia zagrożenia, które wykorzystuje podatność danego zasobu. Po oszacowaniu poziomu ryzyka dla wszystkich zidentyfikowanych zagrożeń pozostaje zaproponować pewne rozwiązania techniczne bądź organizacyjne, które będą miały na celu zredukowanie występującego ryzyka do poziomu akceptowalnego przez dane przedsiębiorstwo.

W tym momencie, jeśli analiza ochrony byłaby traktowana jako osobny, zupełnie odrębny proces, nieskorelowany z analizą bezpieczeństwa funkcjonalnego, jej przebieg, a przede wszystkim wynik byłyby logicznie ukierunkowane na zapewnienie jak najpełniejszego i jak najlepszego zredukowania ryzyka związanego z występowaniem podatności na poszczególne zidentyfikowane zagrożenia w systemie technicznym. Przeciwdziałania zaproponowane w efekcie takiej analizy miałyby na celu sprowadzenie systemu do stanu bezpiecznego z punktu widzenia ochrony, co w praktyce nie zawsze pokrywałoby się z wymaganiami stawianymi systemowi związanemu z bezpieczeństwem funkcjonalnym. Wymagania takie mogłyby się wręcz wzajemnie wykluczać i w efekcie prowadzić do sta-

nów, które w swojej naturze rodziłyby zupełnie nowe niebezpieczne scenariusze, a które nie zostałyby wykryte w przeprowadzanych osobno analizach ochrony, jak również analizach bezpieczeństwa funkcjonalnego. Chcąc nie dopuścić do tego typu sytuacji, należy określić priorytet działań związanych z bezpieczeństwem systemu technicznego (ochrony lub bezpieczeństwa funkcjonalnego). Wynik jednej z wymienionych analiz powinien być dostosowany pod względem wymogów do drugiej z tych analiz. Dzięki temu można by uniknąć błędów logicznych oraz późniejszych problemów wdrożeniowych.

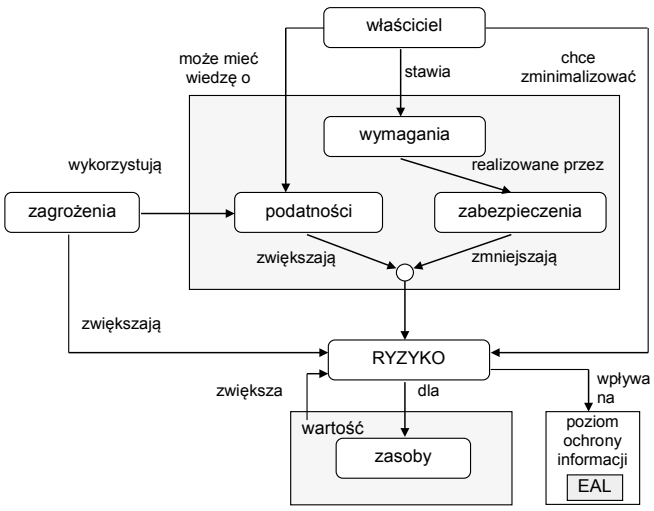
Kolejnym ważnym zagadnieniem związanym z analizami ochrony informacji jest klasyfikacja potencjalnych źródeł wystąpienia szkód w systemie technicznym. Źródła te mogą być związane z czterema kategoriami zagrożeń:

— naturalnymi;
— technicznymi;
— nieumyślnymi działaniami człowieka;
— celowymi działaniami człowieka.

Wszystkie cztery potencjalne źródła zagrożeń powinny być uwzględnione w kompleksowej analizie ochrony informacji, choć najważniejszych źródeł można się dopatrywać w ostatniej kategorii.

Biorąc zatem pod uwagę zagadnienie ochrony informacji, badany system należy oceniać z punktu widzenia zabezpieczenia jego elementów przed wpływem niepożądanych zdarzeń i działań, którymi mogą być, przykładowo, zdarzenia spowodowane przez czynniki naturalne (np. powódź, wyładowania atmosferyczne), przyczyny techniczne (np. zanik zasilania, przegrzanie, zwarcie) lub nieprzyjazne działania człowieka (np. ataki hakerów, wirusy, akty sabotażu) [120]. W takich systemach należy chronić to, co najcenniejsze, czyli m.in.: dane, oprogramowanie, instalacje sieciowe itd., ale również dostęp do różnego rodzaju elementów składowych systemów produkcyjnych itp., których błędne funkcjonowanie mogłoby spowodować często nieprzewidywalne skutki (np. elektrownia jądrowa).

Zagadnienia związane z ochroną informacji w systemach komputerowych przedstawiono w normie ISO/IEC 15408 [93]. Istotę ochrony informacji w takich systemach ilustruje rys. 6.2.



Rys. 6.2. Koncepcja ochrony informacji i relacje [25]

Na rysunku zaprezentowano relacje zachodzące pomiędzy poszczególnymi elementami opisującymi system ochrony informacji. Podobnie jak to ma miejsce w przypadku analiz związanych z bezpieczeństwem funkcjonalnym, ochrona informacji i danych wiąże się ściśle z problematyką zarządzania ryzykiem, obejmującą planowanie oraz utrzymywanie ryzyka na poziomie tolerowanym w cyklu życia, z uwzględnieniem rozpoznawania zagrożeń i stosowania odpowiednich zabezpieczeń.

Na podstawie wymienionego dokumentu wprowadzono pojęcie poziomów uzasadnionego zaufania EAL (*evaluation assurance level*). Poziomy EAL stanowią zbiór wymagań odnoszących się do całkowitego cyklu życia produktu, czyli w tym wypadku systemu informatycznego. Zdefiniowano siedem EAL, przy czym im wyższy poziom, tym mniejsza możliwość wystąpienia negatywnych skutków niekorzystnego zdarzenia, które zależą od podatności systemu.

EAL1 jest poziomem podstawowym i najtańszym w implementacji, potwierdzającym spełnienie podstawowych wymagań ochrony informacji. Poziom EAL7 jest najbardziej rygorystyczny i jednocześnie koszt jego implementacji oraz walidacji jest znacznie wyższy. Aby osiągnąć odpowiedni poziom uzasadnionego zaufania, należy oczywiście spełnić określone wymagania, z których większość odnosi się do dokumentacji i analizy projektu informatycznego, testów funkcjonalności czy też wnikliwych testów poprawnego działania. Im wyższy EAL, tym bardziej szczegółowy charakter powinny mieć dokumentacja, wszelkie analizy i testy. Idea EAL jest w pewnym sensie podobna do idei poziomów nienaruszalności bezpieczeństwa SIL, które są stosowane w ocenie bezpieczeństwa funkcjonalnego. Wymagania dla systemu informatycznego posiadającego odpowiedni EAL zestawiono na podstawie [93] w tablicy 6.1.

Dzięki certyfikatowi określającemu spełnienie przez system informatyczny danego EAL użytkownik ma możliwość stwierdzenia, czy system, którego chce używać, jest wystarczająco bezpieczny w konkretnym zastosowaniu.

Jak wspomniano, rola ochrony różnego typu cennych zasobów przedsiębiorstwa, włączając w to informacje niejawne i inne dane, jest bardzo ważna. Zagadnienie to staje się szczególnie istotne w przypadku systemów zdecentralizowanych, w których wykorzystuje się w znacznej mierze różnego rodzaju środki techniczne, mogące mieć wiele słabych punktów, a przez to sprzyjające występowaniu licznych zagrożeń, których we wcześniejszych analizach zupełnie nie brano pod uwagę.

Tablica 6.1

Poziomy uzasadnionego zaufania EAL [93]

Poziom	Charakterystyka rozwiązania na danym poziomie
EAL1	przetestowany funkcjonalnie
EAL2	przetestowany strukturalnie
EAL3	przetestowany metodycznie i sprawdzony
EAL4	przetestowany, zaprojektowany i zweryfikowany metodycznie
EAL5	zaprojektowany i przetestowany półformalnie
EAL6	przetestowany, zaprojektowany i zweryfikowany półformalnie
EAL7	przetestowany, zaprojektowany i zweryfikowany formalnie

Z każdym z poziomów zaufania powiązany jest również dany zbiór komponentów uzasadnionego zaufania, określony dla poszczególnych klas TOE, które powinny zostać uwzględnione w procesie oceny na danym poziomie. Kompleksowe ujęcie problemów bezpieczeństwa systemów automatyki jest przedmiotem rodziny norm ISA/IEC 62443 [89]. Opisane są w nich zasady tworzenia i wdrażania programu bezpieczeństwa przemysłowych systemów automatyki i sterowania oraz sposób formułowania wymagań dla tego typu systemów. Przedstawione są również możliwe do zastosowania technologie bezpieczeństwa, takie jak: metody uwierzytelniania i autoryzacji użytkowników, konfiguracja zapór ogniowych, sieci wirtualne, metody kryptograficzne oraz monitoring i detekcja zagrożeń.

6.5. Klasyfikacja systemów rozproszonych oraz stopni ochrony informacji

6.5.1. Klasyfikacja systemów rozproszonych

W procesie projektowania i użytkowania programowalnego systemu sterowania i automatyki zabezpieczeniowej, wykorzystującego różne kanały przesyłu informacji, powinny zostać rozpatrzone aspekty bezpieczeństwa funkcjonalnego i ochrony informacji [14, 21, 24, 34, 72, 120, 153, 175, 176, 196]. Integrowanie analiz ochrony informacji i bezpieczeństwa funkcjonalnego wymaga klasyfikacji skomputeryzowanych systemów monitorowania, sterowania i zabezpieczeń.

Mimo stosowania różnego rodzaju zabezpieczeń, od najprostszych po najbardziej wyrafinowane, zawsze mogą istnieć w systemie takie punkty, które zdeterminują jego podatność na występowanie różnego rodzaju zagrożeń. W związku z tym warto w tym miejscu przytoczyć bardzo ważną prawdę, zgodnie z którą jedynie całkowite odseparowanie strefy sieci korporacyjnej/ administracyjnej, jak również sieci rozległej (np. Internet) od części przemysłowej może wyeliminować zagrożenia związane z nieautoryzowanym dostępem do sieci przemysłowej z zewnątrz tej strefy. Dotyczy to oczywiście tylko i wyłącznie zagrożeń opartych na działaniach wykorzystujących połączenia sieciowe, ponieważ w systemie nadal mogą istnieć podatności związane z działaniem osób przebywających na terenie strefy przemysłowej lub – co także jest możliwe w pewnych okolicznościach – także ze strefy korporacyjnej. W szczegółowym określeniu podatności systemu na zagrożenia z zewnątrz pomóc może klasyfikacja systemów oparta na wykorzystywanych kanałach komunikacji.

Proponuje się zatem klasyfikowanie różnego rodzaju wykorzystywanych w praktyce struktur sieci przemysłowych w trzech podstawowych wariantach, które opisano poniżej [17, 24, 120]:

I. systemy zainstalowane w obiektach krytycznych skupionych (np. rafinerie, instalacje chemiczne, obiekty wojskowe), wykorzystujące wyłącznie wewnętrzne kanały przesyłu informacji (np. sieć lokalna);
II. systemy zainstalowane w obiektach krytycznych rozproszonych (np. rurociągi, gazociągi, system energetyczny), w których istnieją wewnętrzne kanały transmisji informacji i mogą być wykorzystywane zewnętrzne kanały przesyłania danych;
III. systemy zainstalowane w obiektach i w systemach infrastruktury krytycznej (np. systemy transportowe – kolej, lotnictwo, transport morski, system ochrony oraz monitoringu w ruchu drogowym), w których wykorzystywane są wyłącznie zewnętrzne kanały transmisji danych.

Proponowana klasyfikacja opiera się na identyfikacji sposobu transmisji danych pomiędzy poszczególnymi elementami systemu monitorowania, sterowania i zabezpieczeń.

Jeżeli ważne dane są przesyłane wyłącznie poprzez sieć wewnętrzną systemu, wówczas rozważany system należy do kategorii I. Jeśli przy transferze danych mogą być wykorzystywane również kanały zewnętrzne (np. stacjonarna sieć telefoniczna, łączność GSM, łączność radiowa lub satelitarna), wówczas system należy do kategorii II. Natomiast w przypadku wyłącznego wykorzystywania zewnętrznych kanałów transmisji danych system zalicza się do kategorii III [14, 120].

Mając zdefiniowane kategorie systemów oraz struktury, w jakich te systemy pracują, można skupić uwagę na zasadniczym problemie, jakim jest integracja zagadnień i analiz bezpieczeństwa funkcjonalnego oraz ochrony informacji. Systemy sterowania oraz automatyki zabezpieczeniowej działają z wykorzystaniem przewodowych bądź też bezprzewodowych kanałów komunikacji. W analizach bezpieczeństwa funkcjonalnego informacje te są prawie zawsze pomijane i nie są brane pod uwagę jako czynniki mogące mieć wpływ na określane wymagania. Standardy bezpieczeństwa funkcjonalnego nie definiują bezpośrednio, w jaki sposób powinno się uwzględniać tę tematykę w analizach bezpieczeństwa funkcjonalnego. Z przeprowadzonej wstępnej analizy wiadomo, że bezpośrednie integrowanie zagadnień ochrony informacji może w tym wypadku nie być rozwiązaniem najbardziej efektywnym. Stąd proponowana metoda integracji tych dwóch różnych zagadnień bazuje na rozwiązaniu, w którym wyniki analizy ochrony informacji, przeprowadzonej dla obiektu technicznego, mogą służyć jako jedne z czynników wpływających na określenie wymaganej redukcji ryzyka dla tego obiektu (stają się zatem czynnikiem ryzyka ujętym w ocenie ryzyka obiektu technicznego). Ma to z kolei bezpośrednie przełożenie na określenie wymaganego poziomu nienaruszalności bezpieczeństwa SIL [14, 15, 18, 20].

6.5.2. Klasyfikacja stopnia ochrony informacji

Główną miarą określającą pewność rozwiązań zastosowanych przy implementacji funkcji bezpieczeństwa jest oczywiście poziom nienaruszalności bezpieczeństwa SIL. Dostępne metody określania tego poziomu oraz sposobność skorzystania z rozwiązań jakościowych, półilościowych oraz ilościowych dają dość elastyczne możliwości analizy problemów o różnych stopniach złożoności. Z punktu widzenia analizy ochrony informacji można stosować zbliżone ideowo poziomy uzasadnionego zaufania EAL. Jednak ich praktyczna implementacja oraz występujące trudności w ich interpretacji sprawiają, że daje się zauważyć trend do ich niewykorzystywania w próbach integracji z bezpieczeństwem funkcjonalnym. Dotyczą one bowiem w zdecydowanej większości pojedynczych rozwiązań technicznych (urządzeń, aplikacji komputerowych itp.), a nie podsystemów czy całych systemów. W związku z tym należy poważnie rozważyć stosowność korzystania z miar EAL na rzecz wartości bardziej ogólnych, będących urzeczywistnieniem realnego poziomu bezpieczeństwa dotyczącego ochrony informacji, a w istocie poziomu związanego z nią ryzyka. W tym kontekście trudno uznać poziom EAL za dobry wyznacznik wymaganej redukcji ryzyka dla systemu technicznego [24].

Dlatego w proponowanej klasyfikacji stopnia ochrony informacji możliwe jest uwzględnienie innych kategoryzacji, które mogą w pewnych przypadkach oddawać rzeczywisty stopień zabezpieczenia systemu technicznego przed ingerencją w jawność, integralność oraz dostępność danych i informacji. Zatem w przedstawionych w dalszej części opracowania tablicach klasyfikacji stopnia ochrony informacji zamiast poziomów uzasadnionego zaufania można wprowadzić inny podział, zgodny z polityką bezpieczeństwa stosowaną w danym przedsiębiorstwie. Mogą to być przykładowo poziomy uzasadnionej ochrony informacji SAL (*security assurance levels*; znane także pod nazwą SL – *security levels*) przedstawione w dokumencie ISA-62443-3-3 [92], które określają stopień zabezpie-

czenia systemu sterowania z perspektywy siedmiu różnych aspektów (poziom ochrony informacji wyrażony za pomocą wektora siedmiu wartości) [92].

Przydatne może być też wykorzystanie metody SeSa, zaproponowanej przez norweską organizację SINTEF. W ramach tej metody analizuje się system z punktu widzenia ochrony informacji systemów sterowania oraz zastosowanych w tym celu pierścieni zabezpieczeniowo-ochronnych w rozproszonej instalacji procesowej, wyposażonej w programowalne systemy: sterowania BPCS i zabezpieczeń SIS [52, 54]. Jak wiadomo, szczególne znaczenie w realizacji funkcji związanych z bezpieczeństwem instalacji procesowej ma przyrządowy system bezpieczeństwa SIS. Pierścienie zabezpieczająco-ochronne takiego systemu powinny zawierać dodatkowo warstwę zero, która polega na fizycznym zabezpieczeniu centralnej sterowni z realizacją funkcji kontroli dostępu osób. W centralnej sterowni przebywa personel operatorski i znajdują się tu kluczowe dla bezpieczeństwa instalacji systemy BPCS i SIS oraz inne systemy sygnalizacyjno-alarmowe, w tym system sygnalizacji pożarowej.

W systemach wydobycia ropy lub gazu oraz niektórych instalacjach przemysłowych istnieje potrzeba zdalnego dostępu do systemu SIS z odpowiednią komunikacją dla przedstawicieli firm wykonujących zakontraktowane usługi w cyklu życia systemu, w tym firm zapewniających serwis oprogramowania poprzez sieć i przeprowadzających okresowe testy wyposażenia. Istnieje zatem konieczność zastosowania odpowiednich środków zabezpieczeniowych, adekwatnych do występujących zagrożeń, np. zabezpieczających przed intencyjnym działaniem hakerów [56–58]. Dlatego w instalacjach dużego ryzyka konieczne może się okazać zastosowanie innych warstw do zabezpieczenia systemów SIS i BPCS.

6.6. Określanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL

Biorąc pod uwagę typową definicję ryzyka, wykorzystywaną w procesie oceny ryzyka, opisującą ryzyko jako kombinację częstości bądź prawdopodobieństwa wystąpienia zdarzenia awaryjnego oraz konsekwencji wystąpienia tego zdarzenia, poniżej zaproponowano uproszczoną metodę określania wymaganego poziomu SIL dla funkcji bezpieczeństwa, z uwzględnieniem aspektów ochrony informacji. Analiza taka bazuje oczywiście na informacji uzyskanej w procesie identyfikacji zagrożeń występujących w systemie technicznym, a także szacowaniu poziomu ryzyka z nimi związanego. Niektóre czynniki ryzyka, brane pod uwagę podczas przeprowadzania tego typu analiz, mają wpływ na oszacowaną wartość częstości bądź prawdopodobieństwa, niektóre zaś – na konsekwencje. Część ryzyka związana z parametrami częstości dotyczy najczęściej zagadnień niezawodności sprzętowej oraz niezawodności i pewności działania człowieka jako elementu systemu technicznego. Czynnik ryzyka związany z komunikacją i przesyłem danych pomiędzy poszczególnymi elementami systemu jest w takim przypadku pomijany. Może się jednak okazać, że w pewnych sytuacjach może on mieć dość znaczny wpływ na rzeczywisty poziom ryzyka analizowanego systemu.

Ryzyko systemu definiuje się jako iloczyn skalarny:

$$R = f \times C \tag{6.1}$$

przy czym częstość występowania scenariusza awaryjnego powodującego określone konsekwencje C jest zależna od wielu czynników, m.in. niezawodności urządzeń technicznych pracujących w analizowanym systemie. Analizując taki system z punktu widzenia ochrony informacji, można wykryć w nim istnienie pewnych podatności, które mogą wpływać na

zwiększenie ryzyka związanego z jego pracą. W większości przypadków będzie to oddziaływać na zwiększenie częstości występowania zdarzenia awaryjnego, zatem zakładając, że współczynnik konsekwencji $C = const$, można powiedzieć, że:

$$f \uparrow \Rightarrow R \uparrow, \text{ gdy podatność systemu } V \text{ będzie } \uparrow$$

Podatność systemu może być mierzalna i wyrażona poprzez poziom ochrony informacji, oczywiście z uwzględnieniem wprowadzonych przeciwdziałań, które mają niwelować tę podatność.

Ryzyko strat ludzkich, środowiskowych i ekonomicznych w analizie bezpieczeństwa funkcjonalnego wyznacza się z uwzględnieniem zidentyfikowanych zagrożeń (*hazards*) środowiskowych i zakłóceń technicznych (zakłócenia wewnętrzne spowodowane uszkodzeniami i/lub błędami człowieka bądź zakłócenia zewnętrzne od instalacji/ systemów współpracujących). W szerszym ujęciu w dopełniającej analizie bezpieczeństwa informacji należy uwzględnić zagrożenia (*threats*) związane z nieprzyjaznymi działaniami intencyjnymi intruzów, znajdujących się wewnątrz lub na zewnątrz danego obiektu, a także z możliwymi w pewnych warunkach działaniami terrorystycznymi.

Miarę ryzyka R_{ij} w okresie rocznym a dla i-tego zagrożenia oraz zdefiniowanego j-tego scenariusza awaryjnego w rozważanym obiekcie/ systemie proponuje się wyznaczać zgodnie z wzorem [9, 116]

$$R_{ij} = f_i \cdot V_{ij} \cdot C_{ij} \tag{6.2}$$

gdzie: f_i – częstość występowania i-tej sytuacji zagrożenia (zdarzenia inicjującego nienormalny stan awaryjny) z powodu intencyjnego działania, a^{-1}; V_{ij} – podatność (*vulnerability*) danego obiektu, wyrażana przez prawdopodobieństwo warunkowe, że wystąpi j-ty poziom skutków, awaryjny dla tej sytuacji zagrożenia; C_{ij} – miara skutku (np. strat ludzkich, środowiskowych lub ekonomicznych) powstałego w wyniku rozważanego zdarzenia awaryjnego; ryzyko ekonomiczne ma wymiar jednostek pieniężnych na rok.

Prawdopodobieństwo warunkowe V_{ij} (podatność) można zmniejszać, stosując odpowiednie rozwiązania techniczne (pierścienie zabezpieczające [108, 117], technologie zabezpieczeń) i organizacyjne (np. programy szkoleniowe, procedury w systemie zarządzania bezpieczeństwem).

Podobnie definiuje się ryzyko w kontekście bezpieczeństwa funkcjonalnego [9, 116]:

$$R_{kj} = f_k \cdot PFD_{kj} \cdot C_{kj} \tag{6.3}$$

gdzie: f_k – częstość występowania k-tej sytuacji zagrożenia (zdarzenia inicjującego stan awaryjny) z powodu zakłóceń wewnętrznych lub zewnętrznych, a^{-1}; PFD_{kj} – prawdopodobieństwo niewypełnienia funkcji na przywołanie przez system zabezpieczeń samodzielny lub warstwowy z wystąpieniem j-tego poziomu skutku; PFD_{kj} wyznacza się na podstawie modeli w nawiązaniu do wymagań normy ogólnej PN-EN 61508 [161] lub normy sektorowej PN-EN 61511 [162].

Na podstawie (6.2) i (6.3), przy założeniu addytywności miar ryzyka, miarę ryzyka zagregowanego, związanego z rozważanym j-tym poziomem skutku, można oszacować z zależności:

$$R_j = \sum_i R_{ij} + \sum_k R_{kj} \tag{6.4}$$

Wyznaczone miary ryzyka można wykorzystać w analizie kosztów i efektów proponowanych rozwiązań systemów zabezpieczeń, w tym warstwowych i pierścieniowych, odpowiednio dla rozwiązań bezpieczeństwa funkcjonalnego i bezpieczeństwa informacji. Należy podkreślić praktyczne znaczenie, ale i wyzwania związane z opracowaniem nowych metod analizy i oceny ryzyka dla celów zintegrowanego zarządzania bezpieczeństwem funkcjonalnym i bezpieczeństwem informacji komputerowych systemów sterowania i zabezpieczeń w warunkach występowania znacznych zwykle niepewności [1, 107, 114].

Tablica 6.2 przedstawia matrycę ryzyka dotyczącego zagadnień ochrony informacji w obiekcie infrastruktury krytycznej. Stopień ryzyka R_{sec} (niski, średni, wysoki lub bardzo wysoki) w danym przypadku jest powiązany z poziomem uzasadnionego zaufania EAL.

Tablica 6.2

Matryca ryzyka dotyczącego zagadnień ochrony informacji w obiekcie infrastruktury krytycznej

Stopień ryzyka R_{sec} oraz powiązany z nim poziom uzasadnionego zaufania EAL		Prawdopodobieństwo i/lub częstość wystąpienia cyberataku			
		niskie	średnie	wysokie	bardzo wysokie
Krytyczność C skutków	katastrofalna	średni R_{sec} EAL3	wysoki R_{sec} EAL5	b. wysoki R_{sec} EAL6	b. wysoki R_{sec} EAL7
	poważna	średni R_{sec} EAL2	średni R_{sec} EAL4	b. wysoki R_{sec} EAL6	b. wysoki R_{sec} EAL6
	średnia	niski R_{sec} EAL1	średni R_{sec} EAL3	wysoki R_{sec} EAL5	wysoki R_{sec} EAL5
	niska	niski R_{sec} EAL1	niski R_{sec} EAL2	średni R_{sec} EAL4	średni R_{sec} EAL4

Tablica 6.3 zawiera natomiast matrycę ryzyka dotyczącego szczególnych zagadnień związanych z cyberbezpieczeństwem przemysłowej sieci komputerowej i jej wpływu na pracę systemu infrastruktury krytycznej. Stopień ryzyka R_{CS} w danym przypadku jest związany z poziomami uzasadnionej ochrony SAL.

Tablica 6.3

Matryca ryzyka dotyczącego zagadnień cyberbezpieczeństwa w obiekcie infrastruktury krytycznej

Stopień ryzyka R_{cs} oraz powiązany z nim poziom uzasadnionej ochrony SAL		Prawdopodobieństwo i/lub częstość wystąpienia cyberataku			
		niskie	średnie	wysokie	bardzo wysokie
Krytyczność C skutków	katastrofalna	średni R_{cs} SAL2	wysoki R_{cs} SAL3	b. wysoki R_{cs} SAL4	b. wysoki R_{cs} SAL4
	poważna	średni R_{cs} SAL2	wysoki R_{cs} SAL3	b. wysoki R_{cs} SAL4	b. wysoki R_{cs} SAL4
	średnia	niski R_{cs} SAL1	średni R_{cs} SAL2	średni R_{cs} SAL2	wysoki R_{cs} SAL3
	niska	niski R_{cs} SAL1	niski R_{cs} SAL1	średni R_{cs} SAL2	wysoki R_{cs} SAL3

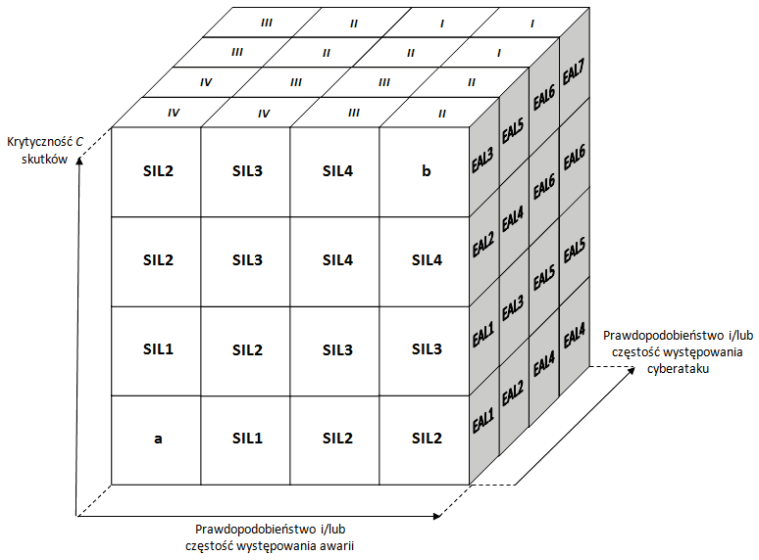
Kolejna tablica (tab. 6.4) przedstawia matrycę ryzyka dotyczącego zagadnień bezpieczeństwa funkcjonalnego. Stopień ryzyka R_{bf} w danym przypadku ma odniesienie w poziomach SIL.

Tablica 6.4

Matryca ryzyka dotyczącego zagadnień bezpieczeństwa funkcjonalnego

Stopień ryzyka R_{bf} oraz powiązany z nim poziom nienaruszalności bezpieczeństwa SIL		Prawdopodobieństwo i/lub częstość wystąpienia awarii			
		niskie	średnie	wysokie	bardzo wysokie
Krytyczność C skutków	katastrofalna	średni R_{bf} SIL2	wysoki R_{bf} SIL3	b. wysoki R_{bf} SIL4	b. wysoki R_{bf} b
	poważna	średni R_{bf} SIL2	wysoki R_{bf} SIL3	b. wysoki R_{bf} SIL4	b. wysoki R_{bf} SIL4
	średnia	niski R_{bf} SIL1	średni R_{bf} SIL2	wysoki R_{bf} SIL3	wysoki R_{bf} SIL3
	niska	b. niski R_{bf} a	niski R_{bf} SIL1	średni R_{bf} SIL2	średni R_{bf} SIL2

Zakładając, że poziomy krytyczności skutków dotyczących bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa są takie same $C_{bf} = C_{cs} = C$, integrację można przedstawić w postaci sześcianu ryzyka (*Risk Cube*). Propozycję integracji zagadnień bezpieczeństwa funkcjonalnego i cyberbezpieczeństwa na etapie analizy ryzyka zaprezentowano na rys. 6.3 oraz 6.4.



Rys. 6.3. Sześcian ryzyka (Risk Cube SIL-SAL)

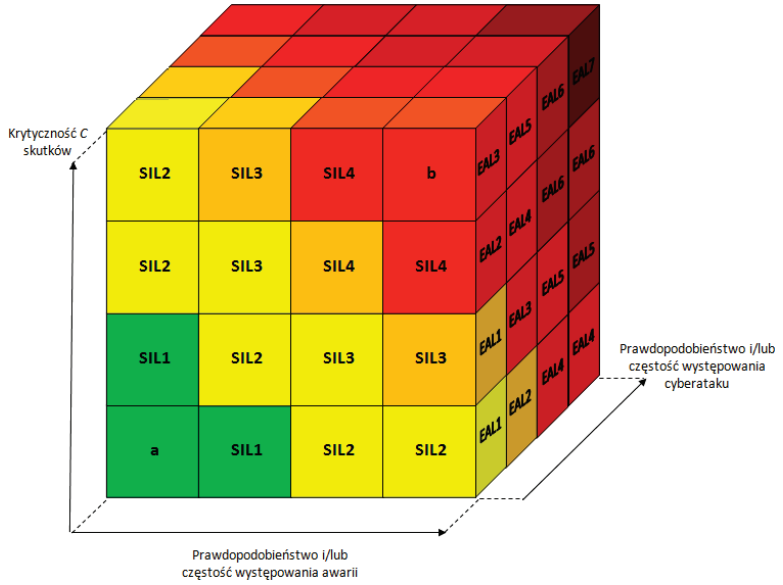
W danym przypadku:

$$R = R_{\text{bf}} + R_{\text{cs}}$$
$$R_{\text{bf}} = C_{\text{bf}} \cdot P_{\text{bf}}(\text{i / lub } F_{\text{bf}}); \quad R_{\text{cs}} = C_{\text{cs}} \cdot P_{\text{cs}}(\text{i / lub } F_{\text{cs}}) \tag{6.5}$$

Zakładając, że: $C_{\text{bf}} = C_{\text{cs}} = C$:

$$R = C \cdot (P_{\text{bf}}(\text{i / lub } F_{\text{bf}}) + P_{\text{cs}} \cdot (\text{i / lub } F_{\text{cs}})) \tag{6.6}$$

gdzie: R – ryzyko; R_{bf} – ryzyko związane z aspektami bezpieczeństwa funkcjonalnego; R_{cs} – ryzyko związane z cyberzagrożeniami; C – krytyczność skutków; C_{bf} – krytyczność skutków związanych z bezpieczeństwem funkcjonalnym; C_{cs} – krytyczność skutków związanych z cyberzagrożeniami; P_{bf} – prawdopodobieństwo wystąpienia awarii; P_{cs} – prawdopodobieństwo wystąpienia cyberataku; F_{bf} – częstość wystąpienia awarii; F_{cs} –częstość wystąpienia cyberataku.



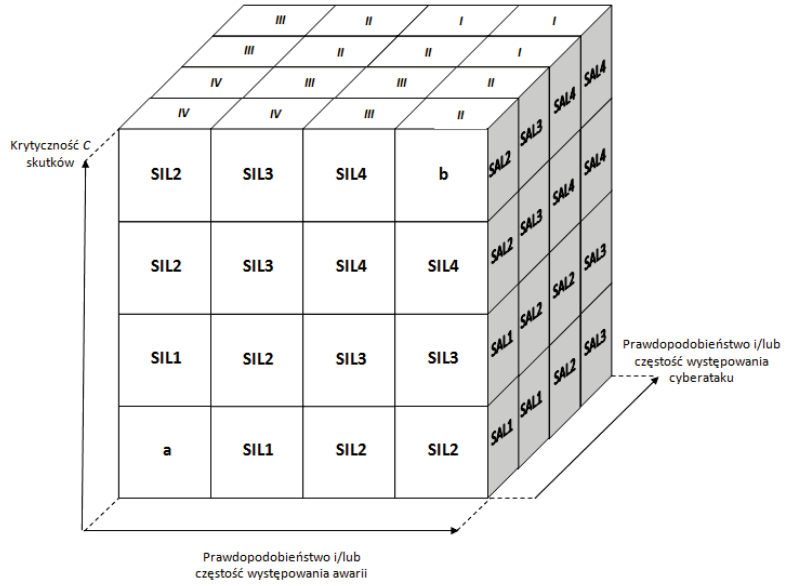
Rys. 6.4. Sześcian ryzyka (Risk Cube SIL-SAL (col))

Analogicznie jak wyżej wygląda sytuacja w przypadku wiązania zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji (wyrażonych przez poziomy uzasadnionego zaufania EAL). Zakładając, że poziomy krytyczności $C_{\text{bf}} = C_{\text{sec}} = C$, zintegrowane podejście zaprezentowano na rys. 6.5 i 6.6 (*Risk Cube* (SIL -> EAL)).

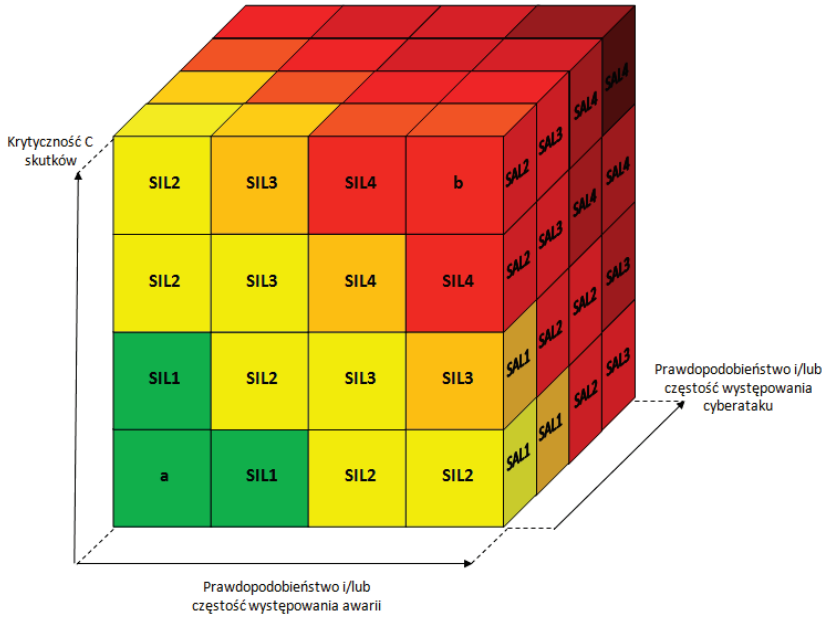
$$R = R_{\text{bf}} + R_{\text{sec}} = C_{\text{bf}} \cdot P_{\text{bf}}(\text{i / lub } F_{\text{bf}}) + C_{\text{sec}} \cdot P_{\text{sec}}(\text{i / lub } F_{\text{sec}}) = C \cdot P(\text{i / lub } F) \tag{6.7}$$

Zakładając, że $C_{\text{bf}} = C_{\text{sec}} = C$:

$$R = C \cdot (P_{\text{bf}}(\text{i / lub } F_{\text{bf}}) + P_{\text{sec}} \cdot (\text{i / lub } F_{\text{sec}})) \tag{6.8}$$



Rys. 6.5. Sześcian ryzyka (Risk Cube SIL-EAL)

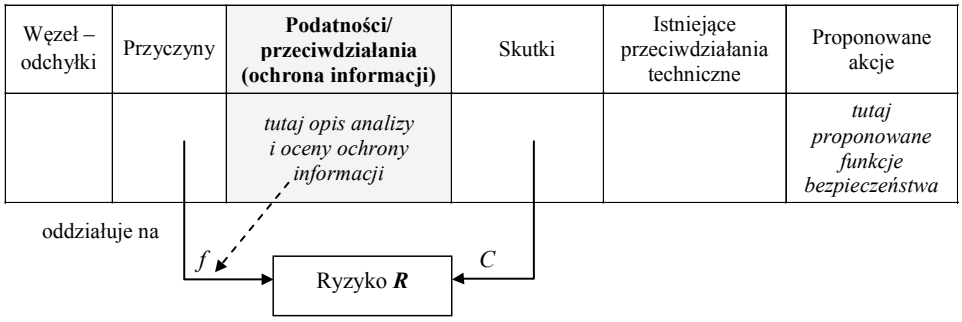


Rys. 6.6. Sześcian ryzyka (Risk Cube SIL-EAL (col))

Wracając do etapu identyfikacji zagrożeń, który ma kluczowe znaczenie z punktu widzenia definiowania funkcji bezpieczeństwa, jakie będą implementowane w systemie technicznym, można stwierdzić, że dla każdego zagrożenia czy też scenariusza awaryjnego opisanego na tym etapie zapisuje się także przyczyny oraz skutki ich wystąpienia. Ochrona informacji, a raczej jej brak w analizowanym obiekcie, jak założono wcześniej, będzie

wpływała na część ryzyka związaną z przyczynami (druga kolumna tabeli przedstawionej na rys. 6.7), gdzie zawarta będzie informacja o poziomie ochrony informacji oraz zwiększeniu częstości występowania opisywanych scenariuszy awaryjnych. Skutki wystąpienia awarii pozostaną te same, chyba że rozważać będziemy działania sabotujące działanie np. barier, procedur postępowania awaryjnego itp. Wiedząc, że ograniczanie przyczyn wystąpienia sytuacji awaryjnych odgrywa kluczową rolę z punktu widzenia bezpieczeństwa obiektu technicznego, ochronę informacji powinno się traktować bardzo poważnie.

Dla metody identyfikacji zagrożeń HAZOP można zaproponować rozszerzenie stosowanej tabeli o kolumnę dotyczącą zidentyfikowanych podatności systemu (np. sieci przemysłowej) oraz zastosowanych środków ochrony informacji. Dane te wpływałyby bezpośrednio na częstość występowania identyfikowanego zagrożenia, kalkulowaną na podstawie zdefiniowanych przyczyn. Propozycję metody identyfikacji zagrożeń HAZOP rozszerzonej o zagadnienia ochrony informacji przedstawiono na rys. 6.7.



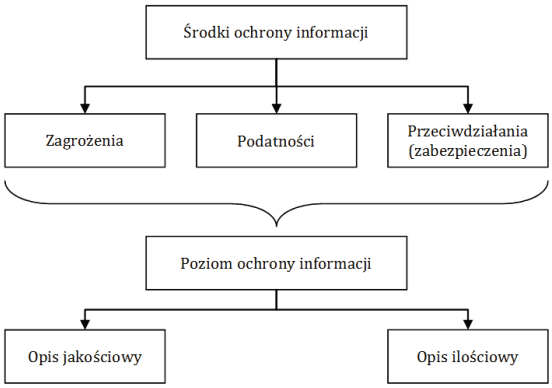
Rys. 6.7. Dodatkowe informacje o poziomie ochrony informacji w analizie HAZOP (CyberHAZOP)

Uwzględnienie w analizie HAZOP aspektów związanych z ochroną informacji stanowi podstawę integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji. Na podstawie analizy HAZOP można wytypować cyberzagrożenia na poziomie założeń koncepcyjnych projektu. Zidentyfikowane cyberzagrożenia mają istotny wpływ na definiowane funkcje bezpieczeństwa realizowane przez system automatyki zabezpieczeniowej. Identyfikację zagrożeń łączącą aspekty bezpieczeństwa funkcjonalnego (lub procesowego) oraz ochrony informacji można określić jako C HAZOP lub CyberHAZOP.

Poziom ochrony informacji, który ma być wykorzystywany w dalszej ocenie ryzyka związanego bezpośrednio z analizą bezpieczeństwa funkcjonalnego, musi być zdefiniowany w sposób umożliwiający jego ujęcie w tych analizach w szybki i prosty sposób (rys. 6.8).

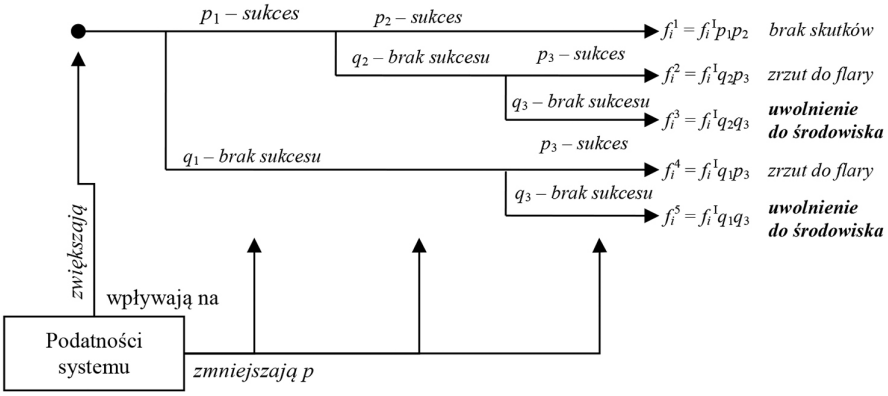
W zależności od metod wykorzystywanych w analizach bezpieczeństwa funkcjonalnego wymagana będzie wartość liczbowa opisująca poziom ochrony informacji lub klasyfikacja jakościowa. Dla wartości liczbowych analiza będzie znacznie bardziej kosztowna i trudniejsza, gdyż trzeba będzie przeprowadzić szereg analiz dotyczących występowania podatności w systemie oraz przypisania im wartości prawdopodobieństw, np. przy użyciu metody drzew ataku AT (*attack trees*) [120, 187].

Rozpatrując scenariusze awaryjne i znając wartości liczbowe przypisane częstościom występowania zdarzeń je inicjujących, jak również wartości prawdopodobieństw zadziałania poszczególnych warstw zabezpieczeń istniejących lub projektowanych, można wykorzystać wartości liczbowe opisujące charakter ochrony informacji w analizowanym systemie i scenariuszu (rys. 6.9).



Rys. 6.8. Określenie poziomu ochrony informacji [24]

Zdarzenie inicjujące	Zabezpieczenie 1	Zabezpieczenie 2	Zabezpieczenie 3	*Częstość/ skutek*
uszkodzenie systemu pomiarowego – zbyt wysokie ciśnienie	*alarm wysokiego ciśnienia*	*odpowiedź operatora*	***funkcja bezpieczeństwa***	
$f_i^{\mathbf{I}}$	P_1	P_2	P_3	

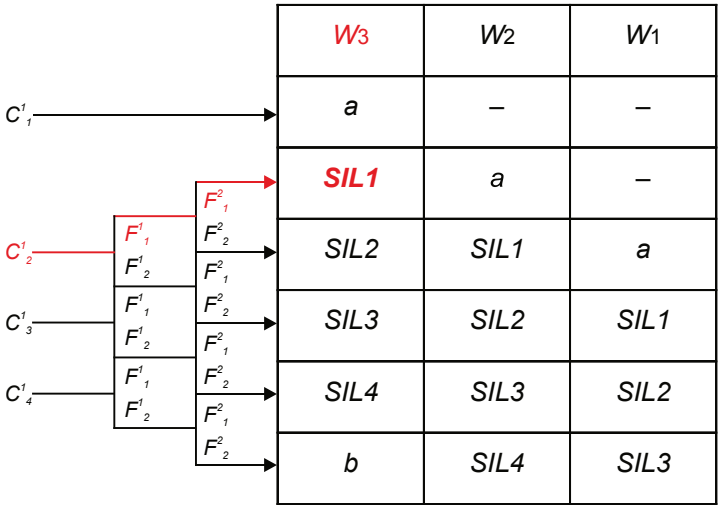


Rys. 6.9. Przykładowe drzewo zdarzeń z określeniem częstości i skutków poszczególnych sekwencji zdarzenia awaryjnego (f_i^1 – częstość występowania zdarzenia inicjującego; p_1 – prawdopodobieństwo zadziałania zabezpieczenia pierwszego; p_2 – prawdopodobieństwo zadziałania zabezpieczenia drugiego; p_3 – prawdopodobieństwo zadziałania zabezpieczenia trzeciego; q_1 – prawdopodobieństwo niezadziałania zabezpieczenia pierwszego; q_2 – prawdopodobieństwo niezadziałania zabezpieczenia drugiego; q_3 – prawdopodobieństwo niezadziałania zabezpieczenia trzeciego; f_i^1 – częstość wystąpienia pierwszego skutku dla *i*-tego zdarzenia inicjującego) [23]

Zdefiniowane w scenariuszu zdarzenia inicjujące posiadają przypisaną im pewną wartość częstości występowania, która wynika bezpośrednio z analiz przeprowadzonych w fazie analizy zagrożeń (np. metodą HAZOP). Zgodnie z założonym kryterium częstość takich zdarzeń może wzrosnąć w zależności od stopnia ochrony informacji (podatności,

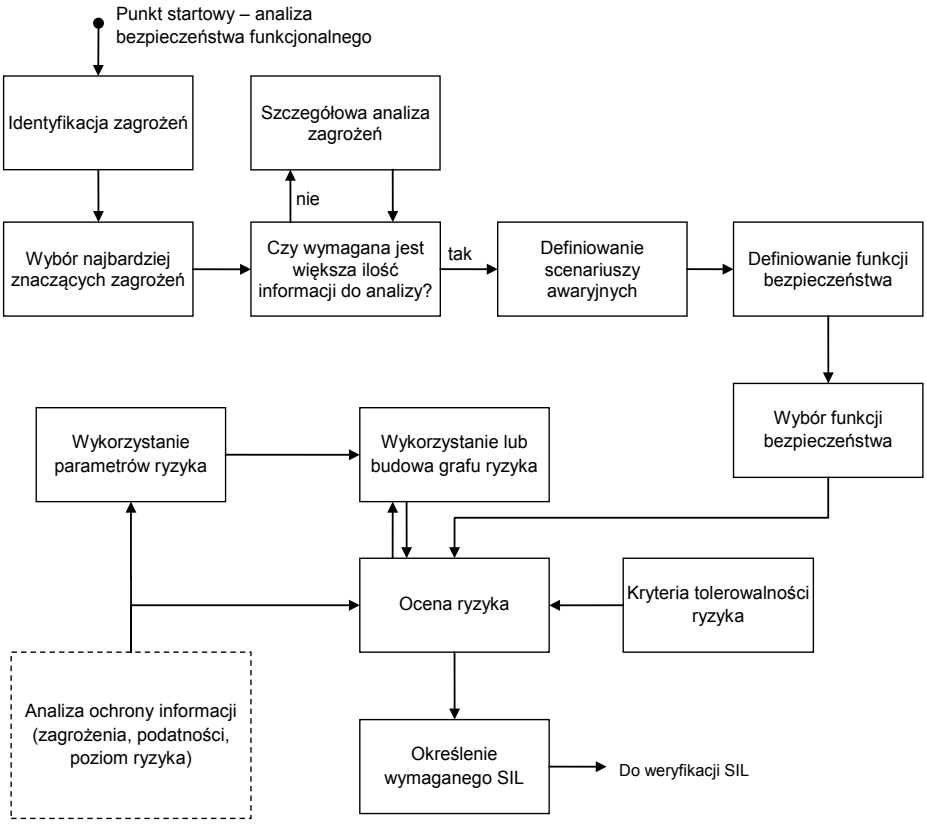
które nie są odpowiednio zabezpieczone). Poprzez analizę ochrony informacji, np. metodą drzew ataku, można oszacować wartość prawdopodobieństwa wystąpienia zagrożenia związanego z podatnościami systemu przypisanymi zdarzeniom inicjującym. W takim przypadku można określić wartość, o jaką zostanie zwiększona częstość zdarzeń inicjujących. Drugim aspektem tego typu analizy jest wpływ ochrony informacji na poprawne działanie poszczególnych analizowanych warstw zabezpieczeniowo-ochronnych. Może się zdarzyć sytuacja, w której istniejące podatności systemu spowodują możliwość ingerencji w funkcjonowanie warstw i ich destrukcję. W takim wypadku stopień ochrony informacji będzie wpływał bezpośrednio na wartości PFD_{avg} przypisane do poszczególnych warstw. Przykładem może tu być działanie warstwy SIS realizującej funkcje bezpieczeństwa. Nieodpowiednia ochrona takiego systemu przed celowym działaniem z zewnątrz (przy jednoczesnym istnieniu poważnych pozwalających na to podatności) spowoduje obniżenie zdolności do wypełnienia funkcji bezpieczeństwa w razie potrzeby, czyli zmniejszenie uzyskanego poziomu nienaruszalności bezpieczeństwa SIL. Sytuację taką opisano szerzej w kolejnym rozdziale. Dlatego konieczna staje się również odpowiednio sprecyzowana analiza poszczególnych warstw zabezpieczeń z punktu widzenia ich podatności na wszelkiego rodzaju zagrożenia związane z ochroną informacji.

W przypadku metod jakościowych, które z pewnością nie dają tak dokładnych wyników jak metody ilościowe i półilościowe, ale umożliwiają szybkie oszacowanie wymagań SIL także dla sytuacji, gdy dane liczbowe nie są znane, zaproponowano rozszerzenie metody grafu ryzyka poprzez dodanie pewnych parametrów ryzyka, odnoszących się do aspektów związanych z ochroną informacji, a raczej wyników przeprowadzonych analiz, mających na celu określenie, jak bezpieczny jest analizowany system pod względem ochrony informacji i dostępu. Proponowana metoda pozwala na uwzględnienie zagadnień ochrony informacji w ocenie ryzyka dla analizy bezpieczeństwa funkcjonalnego. Typowy graf ryzyka składający się z parametrów ryzyka odnoszących się do: konsekwencji (C^1), częstości i czasu przebywania w strefie zagrożenia (F^1), możliwości uniknięcia zagrożenia (F^2) oraz prawdopodobieństwa wystąpienia zagrożenia bez użycia systemu związanego z bezpieczeństwem (W) przedstawiono na rys. 6.10.



Rys. 6.10. Przykładowy graf ryzyka [161]

W odniesieniu do rozszerzonej wersji grafu ryzyka i możliwości jego elastycznego modyfikowania istnieje możliwość dodania pewnych elementów związanych z czynnikiem ryzyka wynikającym z zastosowania bądź niezastosowania rozwiązań redukujących ryzyko wiążące się z zagadnieniami ochrony informacji w systemie technicznym. W praktyce oznacza to, że do grafu ryzyka można dodać parametr opisany za pomocą wyników oceny ryzyka ochrony informacji. Ogólna koncepcja, którą proponuje się w niniejszej monografii, została przedstawiona na rys. 6.11. Zakłada się przy tym, że analiza ochrony informacji jest przeprowadzana niezależnie od analizy bezpieczeństwa funkcjonalnego, a jej wyniki określają, jak bezpieczny jest system pod względem związanych z nią aspektów. Zaprezentowana metoda ma szczególne znaczenie w przypadku analizy różnego rodzaju systemów sterowania i zabezpieczeń działających na bazie architektury rozproszonej, w której wykorzystywane są wszelkie dostępne kanały komunikacyjne. W systemach tego typu mogą istnieć różnego rodzaju podatności, np. takie, które są ściśle związane z wykorzystaniem kanałów komunikacyjnych. Analiza ochrony informacji ma pomóc zidentyfikować takie podatności i jednocześnie zaproponować pewne rozwiązania mające na celu przeciwdziałanie im.



Rys. 6.11. Ogólna koncepcja integrowania zagadnień analizy bezpieczeństwa funkcjonalnego i ochrony informacji [24]

Jeśli weźmie się pod uwagę nadrzędne – jak wspomniano wcześniej – zagadnienia bezpieczeństwa funkcjonalnego, zidentyfikowane podatności takiego systemu, jak również zaimplementowane przeciwdziałania mogą w pewien sposób wpływać na zmierzony i określony poziom ochrony informacji w systemie, ale również na wymagany poziom SIL, który ma być później implementowany przez systemy związane z bezpieczeństwem.

Mając zatem wyniki analizy ochrony informacji dla np. systemu sterowania pracującego w obiekcie technicznym, można je podzielić na kilka podstawowych przedziałów, np. z wykorzystaniem opisu jakościowego. Jeżeli analiza ochrony informacji przebiegałaby zgodnie z [93], dla systemu takiego określono by poziom EAL. Dzięki temu poziom EAL również mógłby zostać uwzględniony w analizie bezpieczeństwa funkcjonalnego. W tablicy 6.5 przedstawiono kategoryzację poziomów ochrony informacji, związanych z poziomami uzasadnionej ochrony EAL oraz parametrem ryzyka wprowadzanym bezpośrednio do grafu.

Tablica 6.5

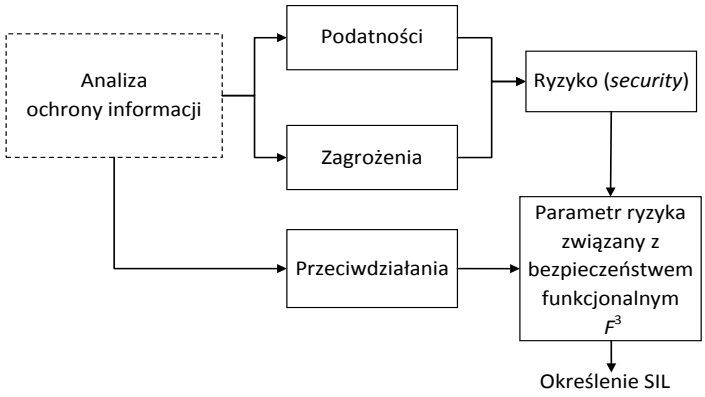
Kategoryzacja poziomów ochrony informacji na podstawie poziomów EAL wg Common Criteria ISO/IEC 15408 [17, 24]

Poziom EAL	Poziom ochrony informacji	Parametr ryzyka i jego kategoria
EAL1	niski	F^3_3
EAL2	niski	F^3_3
EAL3	średni	F^3_2
EAL4	średni	F^3_2
EAL5	wysoki	F^3_1
EAL6	wysoki	F^3_1
EAL7	wysoki	F^3_1

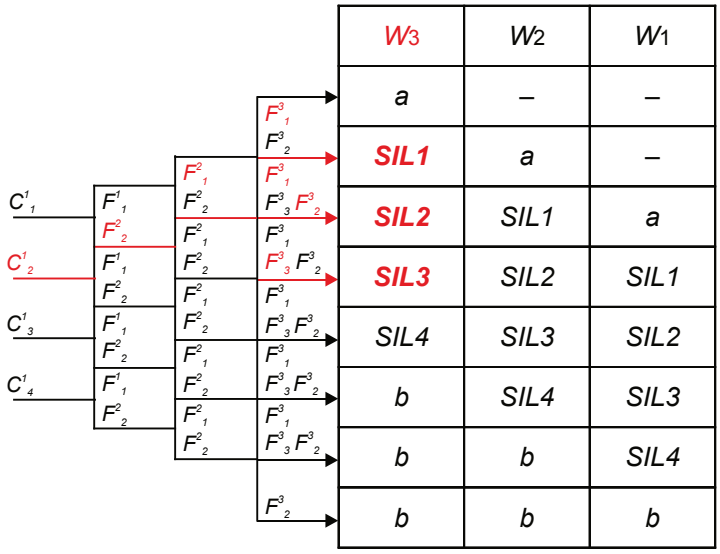
Jak wspomniano, wynik przeprowadzonej analizy ochrony informacji zależy od zidentyfikowanych podatności na zagrożenia w systemie technicznym, tych podatności, które nie były do tej pory uwzględniane w analizach bezpieczeństwa funkcjonalnego. Czynniki związane z opisywanymi podatnościami oraz proponowanymi przeciwdziałaniami, które odpowiadają za określony poziom ochrony informacji, mogą mieć zatem istotny wpływ na dalszy proces oceny ryzyka, związany już z zagadnieniem bezpieczeństwa funkcjonalnego. Ogólną procedurę tego typu przedstawiono na rys. 6.12.

Wykorzystywana w tym kontekście metoda modyfikowalnego grafu ryzyka [13, 24], uwzględniająca dodatkowy parametr ryzyka F^3, została zilustrowana na rys. 6.13. Poprawna kalibracja takiego grafu ma za zadanie zwiększenie wymagań stawianych systemowi E/E/PE, implementującemu funkcję bezpieczeństwa, w przypadku wykrycia zbyt niskiego poziomu ochrony informacji występującego w analizowanym systemie. Oznacza to, że z im mniej bezpiecznym pod względem ochrony informacji systemem ma się do czynienia, tym większe jest prawdopodobieństwo wystąpienia zdarzeń awaryjnych, ponieważ do standardowych przyczyn, związanych z m.in. zawodnym działaniem sprzętu, dochodzą czynniki związane z możliwym celowym działaniem na szkodę takiego systemu ze strony osób trzecich. Sytuacja taka może oczywiście prowadzić do dość poważnych następstw. W takim przypadku częstość lub prawdopodobieństwo wystąpienia zdarzenia awaryjnego są większe. W związku z tym funkcja bezpieczeństwa, która ma za zadanie chronić system, jego

elementy oraz otoczenie poprzez minimalizowanie ryzyka, musi spełniać bardziej rygorystyczne warunki, co wiąże się z nadaniem wyższego wymaganego poziomu nienaruszalności bezpieczeństwa SIL w systemie implementującym taką funkcję.



Rys. 6.12. Czynniki ochrony informacji w analizie bezpieczeństwa funkcjonalnego [17, 24]



W_3	W_2	W_1
a	–	–
SIL1	a	–
SIL2	SIL1	a
SIL3	SIL2	SIL1
SIL4	SIL3	SIL2
b	SIL4	SIL3
b	b	SIL4
b	b	b

Rys. 6.13. Przykładowy graf ryzyka z uwzględnieniem czynnika ochrony informacji

Propozycję przedstawioną powyżej można uznać za konserwatywną i stawiającą bardzo rygorystyczne wymagania. Ponieważ poziomy uzasadnionego zaufania EAL5÷7 są bardzo rzadko możliwe do uzyskania w praktyce, w takiej sytuacji można zmodyfikować założenia przedstawione w tablicy 6.5 i zapisać je w postaci zaprezentowanej w tablicy 6.6.

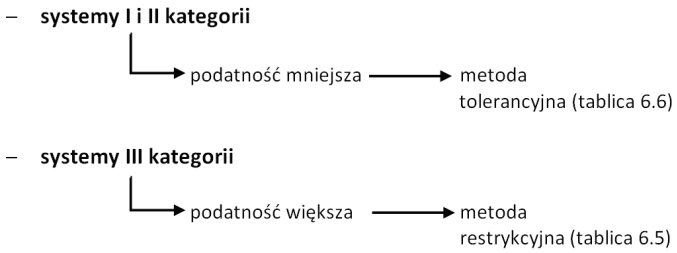
W takim przypadku można się odnieść do przedstawionej wcześniej klasyfikacji systemów technicznych pracujących z wykorzystaniem różnych kanałów komunikacyjnych. Z klasyfikacji tej wynika, że najbardziej narażone na wszelkiego rodzaju podatności są systemy kategorii III, wykorzystujące tylko zewnętrzne kanały przesyłu danych. Dla tych systemów może być uzasadnione bardziej rygorystyczne założenie przy ocenie ryzyka.

Natomiast dla systemów sklasyfikowanych jako I i II kategoria można stosować wersję bardziej tolerancyjną. Podejście to zilustrowano na rys. 6.14.

Tablica 6.6

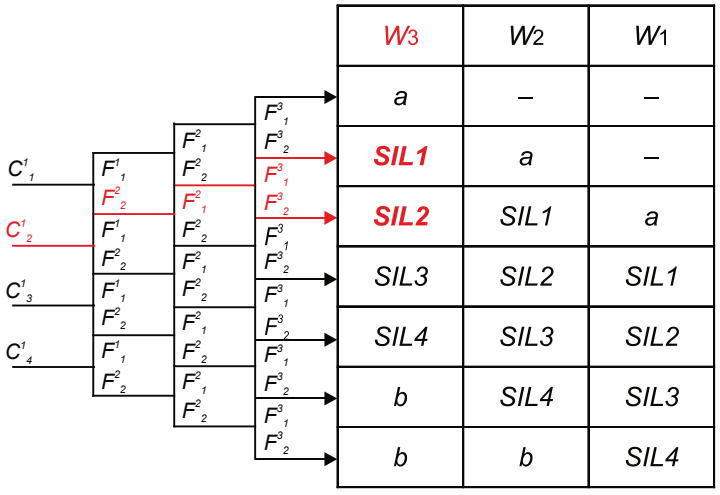
Kategoryzacja poziomów ochrony informacji – mniej rygorystyczna [24]

Poziom EAL	Poziom ochrony informacji	Parametr ryzyka i jego kategoria
EAL1	niezadowalający	F^3_2
EAL2	niezadowalający	F^3_2
EAL3	zadowalający	F^3_1
EAL4	zadowalający	F^3_1



Rys. 6.14. Podejścia w ocenie ryzyka w zależności od kategorii rozpatrywanego systemu

W przypadku zastosowania metody tolerancyjnej graf ryzyka miałby postać jak na rys. 6.15.



Rys. 6.15. Graf ryzyka z uwzględnieniem czynnika ochrony informacji – wersja mniej restrykcyjna

Brak należytej ochrony informacji w analizowanym systemie będzie miał wpływ na zwiększenie wymaganego poziomu SIL dla funkcji bezpieczeństwa, jednak maksymalnie tylko o jedną dekadę.

6.7. Podsumowanie

We współczesnych systemach technicznych wykorzystuje się zarówno wewnętrzne, jak i zewnętrzne kanały transmisji danych. Kanały zewnętrzne umożliwiają zwiększenie funkcjonalności systemu, lecz mogą być źródłem pogorszenia stanu bezpieczeństwa, jeżeli nie zostaną we właściwy sposób zaprojektowane i nie będą odpowiednio eksploatowane. Przy projektowaniu rozproszonych skomputeryzowanych systemów sterowania, zabezpieczeń i monitoringu powinno się zatem uwzględnić wszystkie potencjalne zagrożenia. Są one realne i rzeczywiście mogą się wiązać w praktyce z wieloma niebezpieczeństwami. Aby przeciwdziałać takim zdarzeniom, należy – w ramach poprawnie zarządzanej polityki bezpieczeństwa – dokonać analizy ochrony informacji, a przeprowadzane analizy bezpieczeństwa funkcjonalnego powinny być zintegrowane z aspektami ochrony informacji [24, 187, 202]. W związku z tym zaproponowano metodykę określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL z uwzględnieniem aspektów ochrony informacji.

W niniejszym rozdziale przedstawiono sposób implementacji metod określania wymagań SIL z uwzględnieniem zagadnień ochrony informacji w obiektach przemysłowych. W tym celu wykorzystano opracowane wcześniej podejście metodyczne integracji analizy i oceny bezpieczeństwa funkcjonalnego uwzględniające klasyfikację systemów rozproszonych. Zaproponowaną metodykę zaimplementowano jednocześnie w module określania wymagań bezpieczeństwa funkcjonalnego ProSILen w oprogramowaniu ProSIL-EAL [10, 11, 22]. Komputerowo wspomagana analiza bezpieczeństwa funkcjonalnego pozwala na usystematyzowanie tego procesu w całym cyklu życia bezpieczeństwa systemu technicznego.

Rozdział 7

WERYFIKACJA POZIOMÓW NIENARUSZALNOŚCI BEZPIECZEŃSTWA SIL Z UWZGLĘDNIENIEM ASPEKTÓW OCHRONY INFORMACJI

7.1. Wprowadzenie

Poszczególnym poziomom nienaruszalności bezpieczeństwa SIL projektowanego systemu elektrycznego/ elektronicznego/ programowalnego elektronicznego E/E/PE (BPCS lub SIS) odpowiadają przedziałowe ilościowe kryteria probabilistyczne [161]. Dowód dotyczący spełnienia przez system zabezpieczeń wymagań SIL nazywa się weryfikacją. Model probabilistyczny dowolnego systemu zabezpieczeń SIS można przedstawić za pomocą schematów blokowych niezawodności RBD, grafów Markowa, równań uproszczonych oraz drzew niezdatności FTA [161]. Z punktu widzenia cyklu życia bezpieczeństwa zagadnienia związane z ochroną informacji należy uwzględnić zarówno na etapie określania wymaganych poziomów nienaruszalności bezpieczeństwa SIL dla projektowanych funkcji bezpieczeństwa, jak i ich weryfikacji dla warstwy sprzętowej realizującej te funkcje [21, 24, 58, 98, 176, 196, 212].

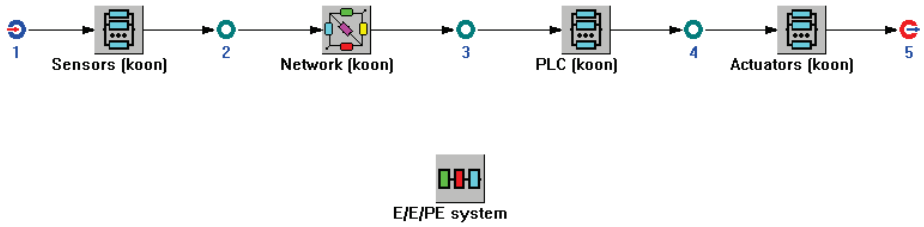
W niniejszym rozdziale zaproponowano wykorzystanie metod (w ramach aktualizacji metodyki analiz bezpieczeństwa funkcjonalnego) weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji, m.in. poprzez wykorzystanie w tym procesie poziomów uzasadnionego zaufania EAL (*evaluation assurance level*) [93], poziomów uzasadnionej ochrony SAL (*security assurance level*) [89] lub przypisanie analizowanemu systemowi stopnia ochrony informacji na podstawie liczby pierścieni zabezpieczeniowo-ochronnych wg metodyki SeSa – SINTEF, wraz z uwzględnieniem klasyfikacji systemów rozproszonych [18, 24, 58, 200]. Integrację zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji zilustrowano na podstawie przykładu zrealizowanego z wykorzystaniem autorskiego prototypowego oprogramowania ProSIL-EAL [24, 176, 200]

7.2. Wpływ infrastruktury sieciowej

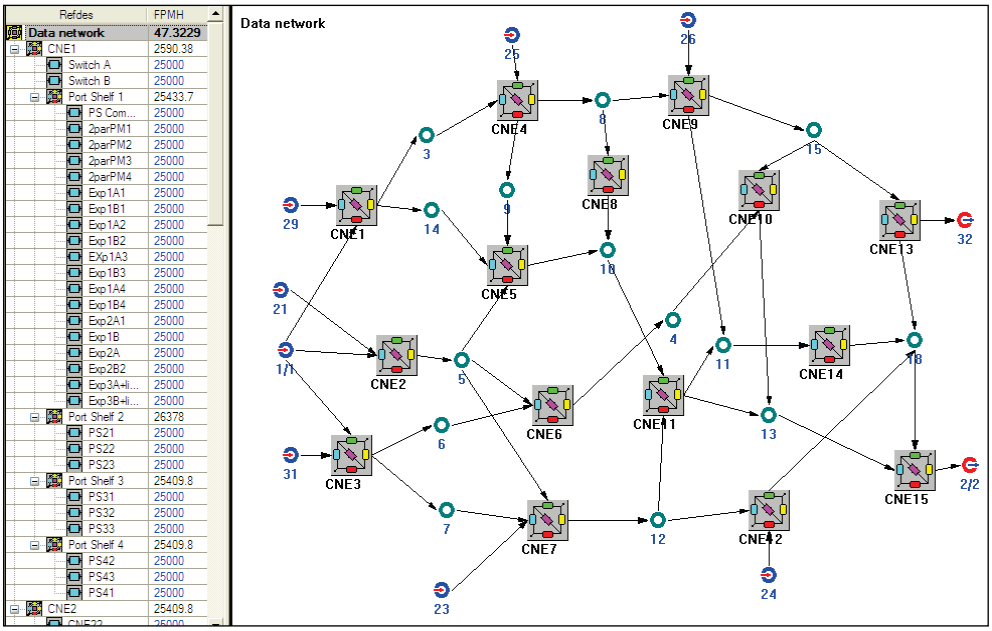
W modelowaniu probabilistycznym rozproszonych systemów sterowania DCS (*distributed control system*) lub automatyki zabezpieczeniowej SIS należy uwzględnić infrastrukturę przemysłowej sieci komputerowej. Budując taki model, można wykorzystać technikę ścieżek, cięć minimalnych lub schematów blokowych niezawodności [24, 200, 201].

Na rys. 7.1 przedstawiono model systemu SIS w postaci schematów blokowych niezawodności RBD.

Blok pomiędzy węzłami 2 i 3 (Network (koon)), reprezentujący model RBD sieci przemysłowej zastosowanej w rozproszonym systemie BPCS lub SIS, może mieć dowolną architekturę wewnętrzną, składającą się z wielu połączonych węzłów i podsystemów (rys. 7.2).



Rys. 7.1. Schemat blokowy niezawodności systemu SIS



Rys. 7.2. Model RBD sieci przemysłowej WAN w konfiguracji siatki (wykorzystanie intranetowej technologii VPN)

Na rys. 7.2 zaprezentowano szczegółowy model RBD typowej sieci komunikacyjnej WAN, stanowiącej zbiór połączonych sieci lokalnych LAN mogących być połączonymi zespołami współpracujących sterowników programowalnych PLC.

Struktury połączeń elementów sieci przemysłowej mogą mieć różne topologie. Topologia fizyczna przemysłowej sieci komputerowej wiąże się ze sposobem realizacji połączeń pomiędzy urządzeniami w sieci. W inny sposób realizowany jest schemat połączeń w sieci lokalnej LAN, a jeszcze w inny w rozległej sieci WAN, której doskonały przykład stanowi sieć Internet, a zwłaszcza wykorzystywane w rozproszonych systemach automatyki przemysłowej (na poziomie BPCS – systemy telemetrii gazociągów, rurociągów oraz sieci energetycznych, sterowanie infrastrukturą autostrad, linii kolejowych, sieciami wodociągowymi i ciepłowniczymi) technologie intranetowe i działające na ich bazie wydzielone wirtualne sieci prywatne VPN (szyfrowane, niejawne tunele komunikacyjne wewnątrz Internetu). Błędy transmisji na poziomie oprogramowania powstają m.in. w ramach topologii logicznej sieci komputerowej, czyli mechanizmów związanych z przekazywaniem informacji przez określoną topologię fizyczną oraz błędów wynikających z nieprawidłowej

konfiguracji urządzeń sieciowych występujących w danej strukturze sieci. Dlatego ich analiza również jest konieczna i uzasadniona [173, 175, 176].

Po uwzględnieniu struktury fizycznej sieci komputerowej w rozproszonym systemie sterowania lub zabezpieczeń prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie można wyznaczyć przy zastosowaniu zależności [24, 120, 175, 176]:

$$PFD_{\text{avgSYS}} \cong PFD_{\text{avgS}} + PFD_{\text{avgNet}} + PFD_{\text{avgPLC}} + PFD_{\text{avgA}} \tag{7.1}$$

gdzie: PFD_{avgSYS} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania systemu E/E/PE (BPCS lub SIS); PFD_{avgS} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa podsystemu pomiarowego; PFD_{avgNet} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa warstwy sieciowej; PFD_{avgPLC} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa sterownika programowalnego; PFD_{avgA} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa podsystemu elementów wykonawczych.

Analogicznie w przypadku pracy ciągłej lub na częste przywołanie do działania średnią częstość wystąpienia uszkodzenia niebezpiecznego na godzinę można określić z zależności:

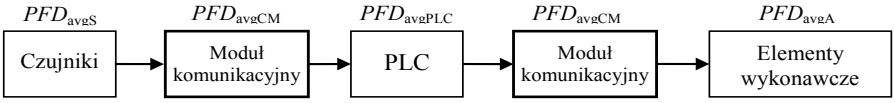
$$PFH_{\text{SYS}} \cong PFH_{\text{S}} + PFH_{\text{Net}} + PFH_{\text{PLC}} + PFH_{\text{A}} \tag{7.2}$$

Z powyższych zależności wynika jednoznacznie, że średnie wartości prawdopodobieństwa i częstości są większe po uwzględnieniu w modelu probabilistycznym topologii sieci komputerowej, a zatem otrzymane wyniki są mniej optymistyczne, co ma istotny wpływ na przebieg weryfikacji poziomów SIL określonych na podstawie analizy ryzyka.

7.3. Uwzględnienie rodzaju pracy modułów komunikacyjnych w systemach E/E/PE i SIS

Norma PN-EN 61508 wprowadza kryteria probabilistyczne dla wyróżnionych rodzajów pracy systemów E/E/PE, które są związane z poziomami nienaruszalności bezpieczeństwa SIL. Dla systemów sterowania i zabezpieczeń pracujących w trybie rzadkiego przywołania do działania kryterium takim jest przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie PFD_{avg}. W przypadku systemów realizujących funkcje bezpieczeństwa w sposób ciągły lub w trybie częstego przywołania do działania kryterium tym jest średnia częstość występowania uszkodzenia niebezpiecznego na godzinę *PFH*. W praktyce spotyka się systemy E/E/PE, w których zaimplementowane są różne funkcje bezpieczeństwa, realizowane zarówno w sposób ciągły, jak i na żądanie. Istnieje problem wyboru kryterium probabilistycznego zarówno przed określeniem wymagań SIL dla takich systemów, jak i w późniejszym procesie weryfikacji ilościowej tych systemów, dlatego też ważną kwestię stanowi uwzględnienie rodzaju pracy modułów komunikacyjnych w systemach BPCS, DCS i SIS [20, 174, 175, 176].

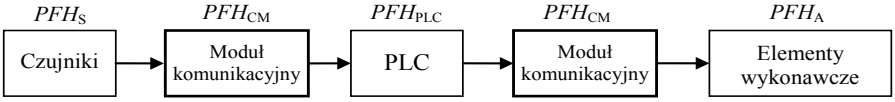
System E/E/PE może realizować kilka funkcji bezpieczeństwa jednocześnie. Funkcje te mogą mieć charakter rzadkiego przywołania, częstego przywołania lub pracy ciągłej. Na rys. 7.3 przedstawiono sytuację, gdy system E/E/PE (SIS) realizuje funkcję bezpieczeństwa w trybie rzadkiego przywołania.



Rys. 7.3. System E/E/PE (SIS) realizujący funkcję bezpieczeństwa w trybie rzadkiego przywołania do działania

W danym przypadku w procesie weryfikacji SIL wykorzystuje się obliczoną z zależności (7.1) wartość przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na żądanie PFD_{avg} dla systemu.

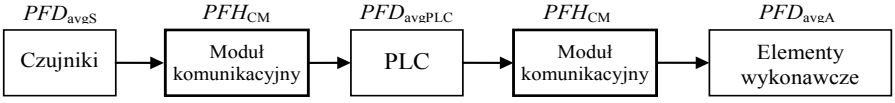
Na rys. 7.4 zaprezentowano sytuację, gdy system E/E/PE (SIS) realizuje funkcję bezpieczeństwa w trybie częstego przywołania do działania lub pracy ciągłej.



Rys. 7.4. System E/E/PE (SIS) realizujący funkcję bezpieczeństwa w trybie pracy ciągłej lub częstego przywołania do działania [20, 175, 176]

W danym przypadku w procesie weryfikacji SIL wykorzystuje się obliczoną z zależności (7.2) wartość *PFH* dla systemu.

W praktyce bywa często, że część sprzętowa podsystemów systemu realizującego funkcje bezpieczeństwa pracuje w sposób ciągły, mimo że realizowana przez ten system funkcja bezpieczeństwa ma charakter rzadkiego przywołania do działania. Przykładem takiej sytuacji może być podsystem modułu komunikacyjnego CM, który najczęściej pracuje w trybie ciągłym (rys. 7.5). W opisanym powyżej przypadku w procesie weryfikacji SIL nie można skorzystać z równań (7.1) i (7.2), gdyż nie można dodać do siebie wartości PFD_{avg} oraz *PFH*.



Rys. 7.5. System E/E/PE (SIS) realizujący funkcję bezpieczeństwa w trybie pracy mieszanej – część modułów pracuje w trybie pracy ciągłej, a część na rzadkie przywołanie [20, 175, 176]

W tej sytuacji jedynym rozwiązaniem jest obliczenie wartości PFD_{avg} oraz *PFH* dla podsystemów systemu E/E/PE lub SIS, przyporządkowanie im SIL na podstawie uzyskanych wyników, a następnie – przy wykorzystaniu metody zwijania schematów blokowych – ustalenie SIL dla całego systemu [20, 175, 176].

7.4. Metodyka weryfikacji SIL z uwzględnieniem aspektów ochrony informacji

7.4.1. Ochrona informacji i cyberzagrożenia w analizach bezpieczeństwa funkcjonalnego

Biorąc pod uwagę fakt, że w złożonych obiektach technicznych wykorzystywane są różnego rodzaju sieci, w tym sieci korporacyjne, inaczej zwane sieciami administracyjnymi, oraz sieci typowo przemysłowe, należy sobie uzmysłowić pewne zagrożenia, jakie wiążą się z ich wspólnym funkcjonowaniem. Oczywiście zadania, jakie stawia się obu rodzajom sieci, są diametralnie różne, zarówno pod względem funkcjonalnym, jak i infrastrukturalnym. Dodatkowo, każda z tych sieci może być zbudowana na bazie innych rozwiązań technicznych i strukturalnych, co dodatkowo komplikuje ewentualne dalsze analizy tych systemów. Coraz częściej spotykane rozwiązania z komunikacją zdalną, bezprzewodową dają realne oszczędności instalacyjne, wprowadzając jednak do systemu nowe zagrożenia, o czym należy pamiętać [40, 41, 43, 78].

Elementy wchodzące w skład systemu sterowania lub zabezpieczeń mogą być rozmieszczone w różnych miejscach, czasem znacznie od siebie oddalonych. W takim przypadku mamy do czynienia z rozproszonym systemem sterowania DCS. W dużych zakładach przemysłowych, ze względu na ich rozległość, jest to wręcz rozwiązanie nieuniknione i znacznie ułatwiające zarządzanie takim systemem. Z drugiej strony powoduje to powstanie dodatkowych źródeł zagrożeń w systemie, związanych z szeroko rozumianą ochroną informacji tego typu infrastruktury. Architektura takich systemów wymusza stosowanie zaawansowanych rozwiązań sieciowych oraz informatycznych. Często jest ona oparta na różnego rodzaju systemach komunikacji.

W rozproszonych systemach sterowania i automatyki zabezpieczeniowej, realizowanych z wykorzystaniem systemów elektrycznych, elektronicznych i programowalnych elektronicznych E/E/PE, wdraża się nowe trendy z branży technologii informacyjnych IT (*information technology*) oraz telekomunikacji (przewodowej i/lub bezprzewodowej). Współczesne sterowniki PLC, na bazie których realizuje się systemy BPCS i SIS, są wyposażone w liczne interfejsy komunikacyjne, np. USB, Ethernet, RS-232 oraz RS-485, oraz protokoły komunikacyjne Modbus, Profibus, ProfiSafe, CanSafe, SafetyBus. Pozwalają na wymianę danych z wykorzystaniem technologii HART, PSTN, ISDN oraz GSM/GPRS. Dzięki tym możliwościom komunikacyjnym sterowników PLC rozproszone systemy BPCS i SIS są bardzo elastyczne. Niestety, z tym rozwojem wiążą się również zagrożenia, których nie można pominąć na etapie projektowania [25, 176].

Norma PN-EN 61508 wprowadza zagadnienia związane z wymaganiami dla tzw. białych i czarnych kanałów komunikacyjnych w ramach systemów E/E/PE (BPCS, DCS lub SIS) realizujących określone funkcje związane z bezpieczeństwem. Jeżeli analizowana infrastruktura krytyczna jest obiektem rozproszonym, w którym stosuje się różne sposoby komunikacji pomiędzy systemami sterowania BPCS i zabezpieczeniowymi SIS, konieczne staje się uwzględnienie problematyki ochrony informacji (wg IEC 62443 oraz PN-EN 61784) oraz określenie rodzaju interfejsu komunikacyjnego. Występowanie białego kanału komunikacyjnego oznacza, że interfejs komunikacyjny łączący systemy BPCS lub SIS został zaprojektowany zgodnie z wymogami zawartymi w PN-EN 61508 i spełnia określone wymagania bezpieczeństwa (SIL1, 2, 3 lub 4). Czarny kanał komunikacyjny występuje wówczas, gdy interfejs komunikacyjny został zaprojektowany zgodnie z wymaganiami IEC 62280 i komunikacja pomiędzy interfejsami nie cechuje się udokumentowanym spełnieniem wymagań związanych z zapewnieniem odpowiedniego poziomu nienaruszalności

bezpieczeństwa SIL wg PN-EN 61508. Przy projektowaniu rozproszonych skomputeryzowanych systemów sterowania, zabezpieczeń, ochrony i monitorowania muszą zostać uwzględnione wszystkie potencjalne zagrożenia wynikające z zastosowania różnych kanałów transmisji danych [42, 43, 152, 153, 161, 162, 176].

W przypadku przemysłowej sieci komputerowej bardzo ważnymi wymaganiami są również zapewnienie odpowiednio wysokiej niezawodności przesyłania danych, skuteczne wykrywanie błędów transmisji oraz możliwość szybkiej lokalizacji potencjalnych uszkodzeń. W celu spełnienia powyższych wymogów przy projektowaniu elementów sieci stosuje się wiele specyficznych rozwiązań na poziomie zarówno sprzętu, jak i oprogramowania [24, 184, 185, 187].

Metody analizy systemów E/E/PE zaproponowane w normach PN-EN 61508 oraz PN-EN 61511 nie uwzględniają problematyki oceny poziomu bezpieczeństwa złożonych struktur sieci komputerowych w zastosowaniach przemysłowych, co w efekcie prowadzi do poważnego uproszczenia rozpatrywanych systemów. W rozproszonych systemach sterowania i automatyki zabezpieczeniowej nie można nie uwzględniać wpływu sieci komputerowej na poziom nienaruszalności bezpieczeństwa SIL. Kanał komunikacyjny pomiędzy dwoma sterownikami należy traktować jako blok sprzętowy z przypisanym mu poziomem nienaruszalności bezpieczeństwa SIL, który trzeba określić na podstawie analizy ryzyka, a następnie zweryfikować i ustalić architekturę sieci, która spełni postawione wymagania. Można tego dokonać, stosując metody jakościowe lub ilościowe. Metody ilościowe są bardziej wiarygodne w przypadku, gdy dysponuje się zestawem danych niezawodnościowych dotyczących poszczególnych elementów składowych. W przypadku braku danych niezawodnościowych można stosować podejście jakościowe, które w tej sytuacji ma jedynie charakter szacunkowy [12, 161, 162, 175, 176].

7.4.2. Poziomy uzasadnionego zaufania EAL wg ISO/IEC 15408 oraz poziom uzasadnionej ochrony SAL wg IEC 62443

Koncepcja zarządzania oraz oceny ryzyka związana z ochroną informacji została zawarta w dokumencie normatywnym ISO/IEC 15408 [93], mającym szczególne znaczenie przy certyfikacji przewidzianych zabezpieczeń. Dokument ten wprowadza pojęcie poziomów uzasadnionego zaufania EAL, które stanowią zbiór wymagań odnoszących się do całkowitego cyklu życia produktu, czyli w tym przypadku systemu informatycznego. Zdefiniowano siedem poziomów EAL, przy czym im wyższy poziom, tym mniejsza możliwość wystąpienia negatywnych skutków niekorzystnego zdarzenia, które zależą od podatności systemu.

EAL1 stanowi poziom podstawowy i najtańszy w implementacji, potwierdzający spełnienie podstawowych wymagań ochrony informacji. Poziom EAL7 jest najbardziej rygorystyczny i jednocześnie koszt jego implementacji oraz walidacji jest znacznie wyższy. Aby osiągnąć odpowiedni poziom EAL, należy oczywiście spełnić określone wymagania, z których większość odnosi się do dokumentacji i analizy projektu informatycznego, testów funkcjonalności czy też wnikliwych testów poprawnego działania. Im wyższy poziom EAL, tym bardziej szczegółowy charakter powinny mieć dokumentacja, wszelkie analizy i testy. Idea poziomów EAL jest w pewnym sensie podobna do idei poziomów nienaruszalności bezpieczeństwa SIL, które są stosowane w ocenie bezpieczeństwa funkcjonalnego [29, 93, 113, 175, 176]. Wymagania dla systemu informatycznego cechującego się odpowiednim poziomem EAL zestawiono na podstawie ISO/IEC 15408 w tablicy 6.1 (rozdział 6) [93].

Dzięki certyfikatowi określającemu spełnienie przez system informatyczny wymogów danego EAL użytkownik ma możliwość stwierdzenia, czy system, którego chce używać, jest wystarczająco bezpieczny w konkretnym zastosowaniu. Jak wspomniano, rola ochrony różnego rodzaju cennych zasobów przedsiębiorstwa, włączając w to informacje niejawne i inne dane, jest bardzo ważna. Zagadnienie to staje się szczególnie widoczne w przypadku systemów zdecentralizowanych, w których wykorzystuje się w znacznej mierze różnego rodzaju środki techniczne, mogące mieć wiele słabych punktów, a przez to sprzyjające występowaniu licznych zagrożeń, których we wcześniejszych analizach zupełnie nie brano pod uwagę.

Z drugiej strony w ogólnej koncepcji bezpieczeństwa systemu technicznego istnieje zagadnienie związane z bezpieczeństwem funkcjonalnym, częściej niż ochrona informacji rozumianym jako jedna z gałęzi ogólnego bezpieczeństwa. Zależy ono przede wszystkim od poprawnego funkcjonowania systemów związanych z bezpieczeństwem, które muszą realizować funkcje bezpieczeństwa zgodnie z postawionymi im wymaganiami. Koncepcja bezpieczeństwa funkcjonalnego została przedstawiona w dokumentach [161, 162] i dotyczy głównie projektowania oraz utrzymywania systemów E/E/PE (elektrycznych, elektronicznych, elektronicznych programowalnych) związanych z bezpieczeństwem. To właśnie te systemy implementują specyficzne funkcje bezpieczeństwa, mające na celu redukowanie ryzyka związanego z pewnymi obiektami technicznymi i – co także ważne – utrzymywanie go na akceptowalnym poziomie.

Norma IEC 62443 wprowadza do zagadnień bezpieczeństwa i ochrony informacji w przemysłowych sieciach komputerowych, obsługujących m.in. rozproszone systemy sterowania, poziomy uzasadnionej ochrony SAL [89, 97, 98]. Poziomy te zostały sklasyfikowane na podobieństwo poziomów nienaruszalności bezpieczeństwa od 1 do 4, przy czym SAL1 jest poziomem odpowiadającym najsłabszym zabezpieczeniom, natomiast SAL4 – najwyższym. W przeciwieństwie do poziomów nienaruszalności bezpieczeństwa, które w zależności od rodzaju pracy (tryb częstego i rzadkiego przywołania do działania funkcji bezpieczeństwa) wiążą się z ilościowymi kryteriami probabilistycznymi odpowiadającymi prawdopodobieństwu PFD_{avg} oraz częstości PFH, które mieszczą się w odpowiednich przedziałach kryterialnych, poziomy SAL są związane z typowymi miarami jakościowymi. Aby skwantyfikować poszczególne miary określające stan ochrony informacji rozpatrywanego systemu informatycznego, będącego częścią infrastruktury przemysłowej, poziom uzasadnionej ochrony SAL przyjmuje się jako siedmioelementowy wektor, którego poszczególne elementy są oceniane jakościowo według określonych procedur.

Propozycję formatu wektora SAL na podstawie IEC 62443 opisuje zależność [89]:

$$SAL = \left\{ AC \quad UC \quad DI \quad DC \quad RDF \quad TRE \quad RA \right\} \tag{7.3}$$

gdzie: *AC* – kontrola dostępu; *UC* – kontrola użytkowania; *DI* – integralność danych; *DC* – poufność danych; *RDF* – ograniczenia przesyłania danych; *TRE* – odpowiedź w czasie na zdarzenie; *RA* – dostępność zasobów.

7.4.3. Przypisanie stopnia ochrony informacji systemom realizującym funkcje bezpieczeństwa

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 SRS (*safety-related*

systems) bazuje na wspomnianej wcześniej identyfikacji zagrożeń oraz analizie i ocenie ryzyka. Integralność systemów w rozumieniu bezpieczeństwa (*safety*) jest weryfikowana za pomocą metod formalnych pod względem zgodności z wymaganiami i kryteriami, np. zawartymi w PN-EN 61511. Z punktu widzenia cyklu życia bezpieczeństwa zagadnienia związane z ochroną informacji należy uwzględnić zarówno na etapie określania wymaganych poziomów SIL dla projektowanych funkcji bezpieczeństwa, jak i ich weryfikacji dla warstwy sprzętowej realizującej te funkcje.

Systemy sterowania oraz automatyki zabezpieczeniowej, jak opisano to we wcześniejszej części niniejszego rozdziału, działają z wykorzystaniem przewodowych bądź też bezprzewodowych kanałów komunikacji. W analizach bezpieczeństwa funkcjonalnego zagadnienia związane z ochroną informacji w systemach sterowania są kluczowe i mają wpływ na określanie wymagań SIL oraz ich weryfikację [12, 176, 196].

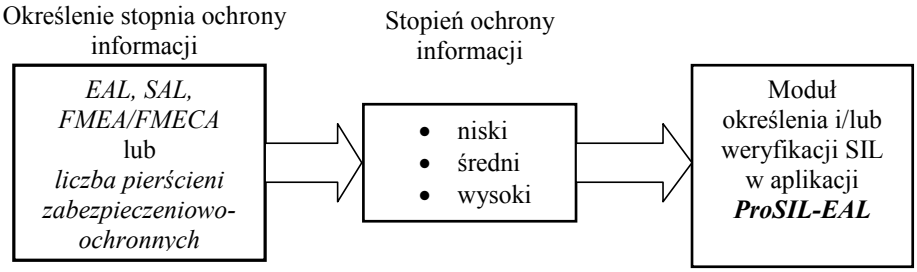
Na podstawie przeprowadzonej wstępnej analizy wiadomo, że bezpośrednie integrowanie zagadnień ochrony informacji w procesie określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL może nie być rozwiązaniem najbardziej efektywnym. Dlatego zaproponowana metoda integracji dwóch różnych zagadnień bazuje na innym rozwiązaniu, w którym wyniki analizy ochrony informacji przeprowadzonej dla obiektu infrastruktury krytycznej mogą służyć jako jedne z czynników wpływających na określenie wymaganej redukcji ryzyka dla tego obiektu. Ma to następnie bezpośrednie przełożenie na określenie wymaganego poziomu SIL, czyli redukcji ryzyka związanego z działaniem takiego obiektu. W takim przypadku analiza bezpieczeństwa funkcjonalnego będzie niezaprzeczalnie odgrywała rolę nadrzędną.

W przypadku weryfikacji SIL powstaje zasadnicze pytanie, w jaki sposób uwzględnić zagadnienia ochrony informacji: czy poprzez integrację SIL i EAL, SIL z SAL, czy też wyznaczając stopień ochrony informacji (niski, średni lub wysoki) w inny sposób, np. przez przeprowadzanie dla każdego prototypowego rozproszonego systemu E/E/PE (BPCS, DCS lub SIS) szczegółowej analizy rodzajów, skutków i krytyczności uszkodzeń FMECA, umożliwiającej zbadanie wpływu infrastruktury sieciowej na brak realizacji funkcji bezpieczeństwa lub powiązanie stopnia ochrony z liczbą pierścieni zabezpieczeniowo-ochronnych (rys. 7.6) [24, 176, 196]. Przykład analizy FMECA przedstawiono w załączniku Z.2 niniejszej monografii.

W systemach rozproszonych mogą istnieć różnego rodzaju podatności, np. takie, które wiążą się ściśle z wykorzystaniem kanałów komunikacyjnych. Analiza ochrony informacji ma pomóc zidentyfikować takie podatności i jednocześnie zaproponować pewne rozwiązania mające na celu przeciwdziałanie im. Jeśli weźmie się pod uwagę nadrzędne, jak wspomniano wcześniej, zagadnienia bezpieczeństwa funkcjonalnego, zidentyfikowane podatności takiego systemu, jak również zaimplementowane przeciwdziałania mogą w pewien sposób wpływać na zmierzony i określony poziom ochrony informacji w systemie, ale również na wymagany poziom SIL, który ma być później implementowany przez systemy związane z bezpieczeństwem.

Mając zatem wyniki analizy ochrony informacji dla np. systemu sterowania pracującego w obiekcie infrastruktury krytycznej, można je podzielić na kilka podstawowych przedziałów, np. z wykorzystaniem opisu jakościowego. Jeżeli analiza ochrony informacji przebiegałaby zgodnie z ISO/IEC 15408 [93], dla takiego systemu określono by EAL. Dzięki temu poziom EAL również mógłby zostać uwzględniony w analizie bezpieczeństwa funkcjonalnego. W rozdziale 6, w tablicy 6.5, przedstawiono kategoryzację poziomów ochrony informacji z wykorzystaniem poziomów uzasadnionego zaufania EAL. W danym przypadku typ i liczba podatności na zagrożenia związane z cyberatakiem mają źródło

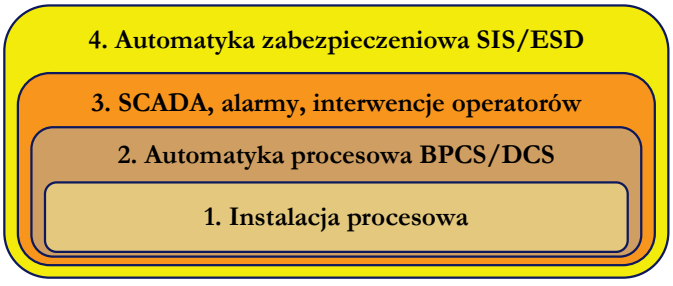
w przedstawionej wcześniej klasyfikacji (podrozdział 6.5.1) na kategorie rozpatrywanych systemów sterowania i zabezpieczeń (I, II i III kategoria).



Rys. 7.6. Przypisanie stopnia ochrony informacji na potrzeby procesu weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji [176, 196, 202, 203]

Czynniki związane z opisywanymi podatnościami oraz proponowanymi przeciwdziałaniami, które odpowiadają za określony poziom ochrony informacji, mogą mieć zatem istotny wpływ na dalszy proces oceny ryzyka, związany już z zagadnieniem bezpieczeństwa funkcjonalnego, a także w znacznym stopniu wpływać na proces weryfikacji SIL [17, 18, 24, 42, 43, 175, 176, 199].

Na rys. 7.7 przedstawiono typowe warstwy zabezpieczeniowo-ochronne związane z programowalnymi systemami sterowania, monitorowania i zabezpieczeń obiektu przemysłowego podwyższonego ryzyka, jakim jest instalacja procesowa. Obiekty przemysłowe podwyższonego ryzyka są obecnie projektowane zgodnie z zasadą obrony w głąb z wyróżnieniem kilku warstw zabezpieczeniowo-ochronnych [3, 162]. Mając na uwadze model warstw zabezpieczeń w typowej instalacji procesowej pokazany na rys. 7.7, można stwierdzić, że najważniejszym systemem z punktu widzenia bezpieczeństwa funkcjonalnego, oczywiście poza samą instalacją procesową, jest system SIS.

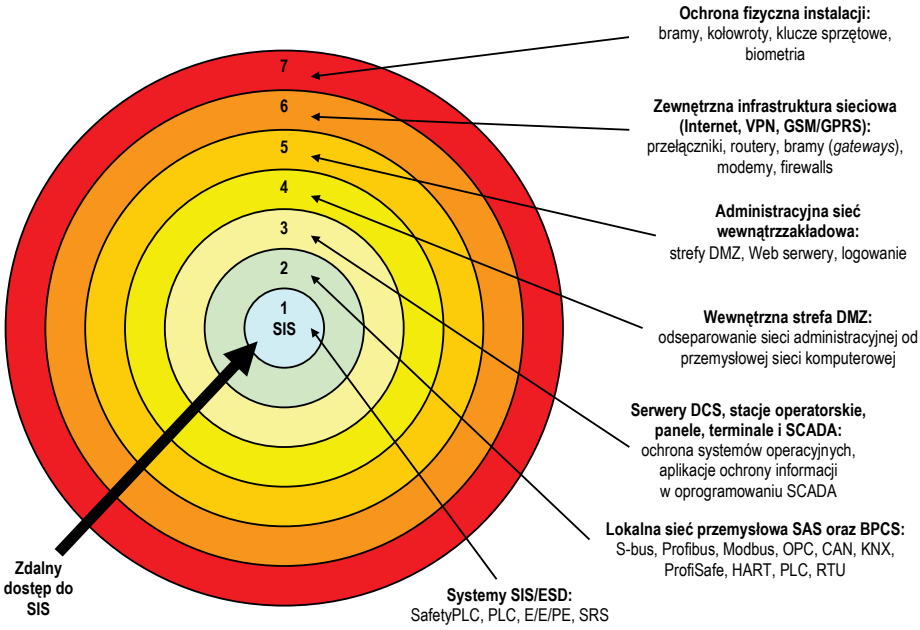


Rys. 7.7. Warstwy zabezpieczeń w instalacji procesowej (na podstawie PN-EN 61511 [162])

Projektowanie tych warstw i systemów związanych z bezpieczeństwem bazuje na wspomnianej wcześniej identyfikacji zagrożeń oraz analizie i ocenie ryzyka. Integralność systemów w rozumieniu bezpieczeństwa (*safety*) jest weryfikowana za pomocą metod formalnych pod względem zgodności z wymaganiami i kryteriami, np. zawartymi w PN-EN 61511 [162].

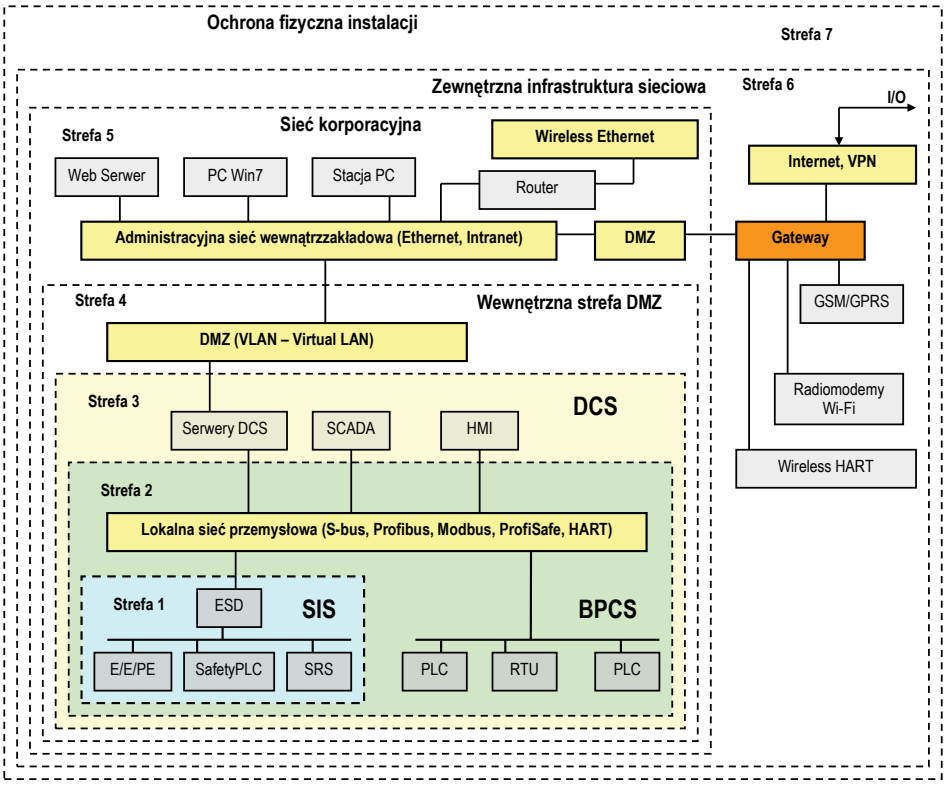
Innym podejściem do wykorzystania integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji w procesie weryfikacji poziomów nienaruszalności SIL jest

wspomniana wcześniej metodyka SeSa (*SecureSafety*), opracowana przez ośrodek badawczy SINTEF [24, 58, 156, 176]. Jest ona przeznaczona dla systemów sterowania i automatyki zabezpieczeniowej stosowanych w przemyśle wydobywczym na morskich platformach wiertniczych, monitorowanych i zarządzanych zdalnie z lądu, poprzez ogólnie dostępne środki komunikacyjne. Podejście to wykorzystuje uwzględnienie pierścieni zabezpieczeniowo-ochronnych w przemysłowych sieciach komputerowych ze szczególnym zwróceniem uwagi na programowalne systemy sterowania i zabezpieczeń (rys. 7.8) [24, 43, 57, 58, 152].



Rys. 7.8. Pierścienie zabezpieczeniowo-ochronne w systemach BPCS, DCS i SIS wyposażonych w przemysłową sieć komputerową [24, 176, 196]

System SIS jest najważniejszy, gdyż jego zadanie polega na wykonywaniu zaprojektowanych i zaimplementowanych funkcji bezpieczeństwa, dla których wcześniej zostały określone wymagania SIL, a następnie wymagania te zostały poddane weryfikacji. Przekładając tę sytuację na język związany ze standardem ISO/IEC 15408, można założyć, że warstwa SIS, z punktu widzenia bezpieczeństwa funkcjonalnego stanowiąca 4. warstwę zabezpieczeń, w danym wypadku staje się zasobem (obiektem) TOE (czyli numerem 1), dla którego bada się stopień i jakość zabezpieczeń. W nawiązaniu do modelu pierścieniowego system SIS staje się zasobem, który chronimy. Stopień ochrony informacji tego systemu będzie tym większy, im więcej będzie pierścieni ochronnych wokół niego (rys. 7.8). Rozpatrywany system sterowania i zabezpieczeń wraz z przemysłową siecią komputerową należy podzielić na obszary (strefy chronione), co zaprezentowano na rys. 7.9 [24, 117, 176, 196].



Rys. 7.9. Przykład przemysłowej sieci komputerowej z uwzględnieniem programowalnych systemów sterowania i zabezpieczeń [24, 196]

Po tak przeprowadzonej dekompozycji można przystąpić do budowy pierścieni zabezpieczeniowo-ochronnych, a następnie wytypować potencjalne zagrożenia oraz ścieżki ataków z zewnątrz (możliwych obecnie w coraz większym zakresie dzięki powszechnie stosowanym w przemysłowych sieciach komputerowych elastycznym sposobom komunikacji z wykorzystaniem technologii: HART (*highway addressable remote transducter*), Bluetooth, WLAN, GSM/GPRS, Trusted Wireless i Wireless HART, a także transmisji wszystkich protokołów ethernetowych IP, Modbus, TCP czy PROFINET z wykorzystaniem Wireless Ethernet na bazie bezprzewodowej komunikacji sieciowej WLAN 802.11 i Bluetooth). Należy cały czas mieć na uwadze, że z punktu widzenia zagadnień bezpieczeństwa funkcjonalnego system SIS zawsze będzie się znajdował w środkowym pierścieniu. Dzięki zobrazowaniu systemu w postaci pierścieni można zaproponować system zabezpieczeń chroniący SIS przed niepożądanym atakiem z zewnątrz poprzez przemysłową sieć komputerową.

Jeśli weźmie się pod uwagę podział rozpatrywanego obiektu na strefy, powstaje kolejne zasadnicze pytanie, w jaki sposób powiązać poziomy EAL z pierścieniami zabezpieczeniowo-ochronnymi i czy stosowanie poziomów uzasadnionego zaufania EAL jest w dalszych rozważaniach właściwe. Jeżeli system ma określony i udokumentowany EAL, wówczas należy tę sytuację wykorzystać i uwzględnić EAL w analizie bezpieczeństwa funkcjonalnego. W przeciwnym wypadku, kiedy EAL nie jest określony,

a znana jest liczba pierścieni zabezpieczeniowo-ochronnych lub wiemy, jaki jest poziom uzasadnionej ochrony SAL, wówczas można jakościowo określić stopień ochrony informacji, tj.: niski, średni bądź wysoki. Jakościowo określony stopień (poziom) ochrony informacji ma związek z poziomami uzasadnionej ochrony SAL i uzasadnionego zaufania EAL (tabl. 6.1, 6.5, rozdział 6), przy czym podstawowy (niski) stopień ochrony informacji odpowiada SAL1, EAL1 i 2 (oraz liczbie pierścieni od 0 do 1), stopień średni odpowiada SAL2 oraz EAL3 i 4 (2 do 4 pierścieni zabezpieczeniowo-ochronnych), a stopień wysoki – SAL3 i 4 oraz EAL5 i 6 (od 5 pierścieni zabezpieczeniowo-ochronnych) (tabl. 7.1). Poziom EAL7 można zarezerwować dla bardzo wysokiego stopnia ochrony informacji, który ze względu na koszty wdrożenia zabezpieczeń niekoniecznie jest wymagany w systemach związanych z instalacjami procesowymi.

7.4.4. Zweryfikowany SIL z uwzględnieniem stopnia ochrony informacji

W procesie weryfikacji poziomy SIL odnoszą się do struktury sprzętowej systemu SIS realizującego konkretne funkcje bezpieczeństwa (np. ochrona reaktora przed eksplozją). Przyjęto, że niepożądane zdarzenia i działania z zewnątrz przy niskim stopniu ochrony informacji (np. EAL1 lub 2) mogą wpływać niekorzystnie na wypełnienie przez system SIS wymagań SIL dla funkcji bezpieczeństwa [24, 176, 196, 200, 204].

W tablicy 7.3 przedstawiono propozycję takiej zależności dla systemów II oraz III kategorii. W nawiasie znajdują się zmodyfikowane poziomy SIL dla systemu III kategorii, gdyż jest on bardziej podatny na działania z zewnątrz (według przyjętej klasyfikacji i podziału rozproszonych systemów E/E/PE na kategorie – podrozdział 6.5.1).

Tablica 7.1

Wynikowe poziomy SIL z uwzględnieniem poziomów EAL, SAL i metodyki SeSa dla systemów II i III kategorii

Ochrona informacji				Weryfikowany SIL dla systemu II (i III) kategorii			
				Bezpieczeństwo funkcjonalne			
EAL	SAL	liczba pierścieni zabezpieczeń	poziom	1	2	3	4
1	1	1	niski	– (–)	SIL1 (–)	SIL2 (1)	SIL3 (2)
2	1	2		– (–)	SIL1 (–)	SIL2 (1)	SIL3 (2)
3	2	3	średni	SIL1 (–)	SIL2 (1)	SIL3 (2)	SIL4 (3)
4	2	4		SIL1 (–)	SIL2 (1)	SIL3 (2)	SIL4 (3)
5	3	5	wysoki	SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
6	4	6		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)
7	4	7		SIL1 (1)	SIL2 (2)	SIL3 (3)	SIL4 (4)

Niski poziom ochrony informacji, zdeterminowany poziomem uzasadnionego zaufania EAL1 lub 2 bądź poziomem uzasadnionej ochrony SAL1 albo liczbą pierścieni zabezpieczeniowo-ochronnych 1, przy weryfikacji określonego poziomu SIL może w rezultacie skutkować jego obniżeniem.

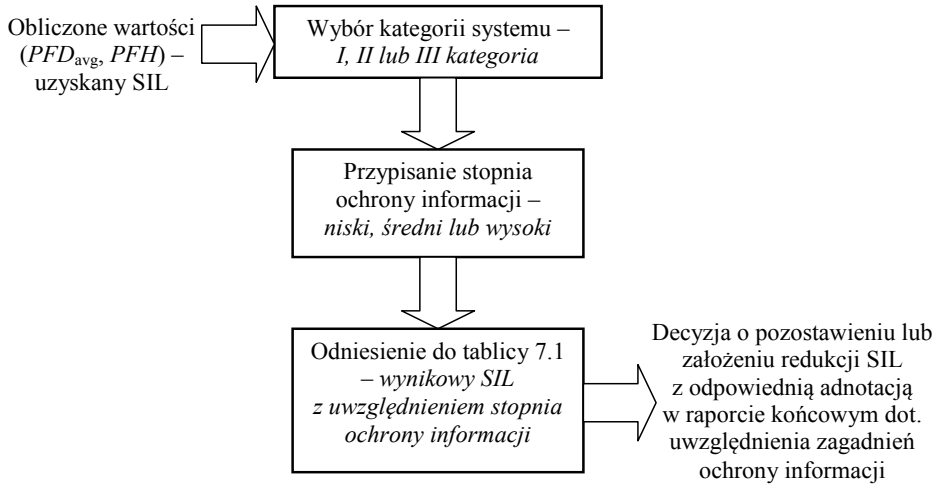
W przypadku weryfikacji SIL powstaje zasadnicze pytanie, czy uwzględnienie zagadnienia ochrony informacji musi się odbywać poprzez integrację SIL i EAL (lub SAL), czy też w inny sposób, np. przy wykorzystaniu przeprowadzania dla każdego prototypowego rozproszonego systemu E/E/PE (BPCS lub SIS) szczegółowej analizy FMECA. Umożliwia ona zbadanie wpływu infrastruktury sieciowej na brak wykonania funkcji bezpieczeństwa. Uwzględnienie zagadnień ochrony informacji poprzez zastosowanie FMEA/FMECA pozwala także zbadać wpływ uszkodzeń infrastruktury sieciowej na tzw. nieuzasadnione zadziałanie systemu BPCS lub SIS, czego nie uzyska się na podstawie EAL i SAL.

7.5. Procedura weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji

W przypadku systemów E/E/PE I kategorii w procesie weryfikacji SIL stosuje się podejście opisane w rozdziale 4 niniejszej monografi. Zagadnienia bezpieczeństwa funkcjonalnego i ochrony informacji traktuje się niezależnie. Z wymaganymi poziomami nienaruszalności bezpieczeństwa SIL związane są część sprzętowa oraz oprogramowanie wbudowane, a także po części oprogramowanie aplikacyjne, które jednocześnie determinuje wymagany poziom EAL dla oprogramowania i całego systemu E/E/PE, który z punktu widzenia ISO/IEC 15408 jest TOE. Aby określić wymagania ochrony informacji dla rozpatrywanego systemu, należy zdefiniować m.in. cel takiej ochrony, czyli TOE, funkcje ochrony informacji, które ma się zrealizować w systemie, oraz wykonywane zadania i ich zagrożenia. Na tej podstawie można określić szereg wymagań, zestawiając je w odpowiednie grupy. Te z kolei, na podstawie normy ISO/IEC 15408 i zawartych w niej kryteriów oceny, determinują odpowiedni poziom EAL, który należy uzyskać przy tworzeniu systemu. Szacowany EAL będzie zależał w głównej mierze od tego, w jakim stopniu wybrane funkcje ochrony informacji będą ograniczać potencjalne straty i jaki będą miały wpływ na pracę oraz wydajność systemu, a także w jakich warunkach system będzie użytkowany [21, 176, 196, 202]. Określenie wymagań EAL dla danych funkcji ochrony informacji według normy ISO/IEC 15408 jest bardzo skomplikowane.

Sytuacja przedstawia się inaczej w przypadku systemów rozproszonych E/E/PE (BPCS lub SIS) należących do II lub III kategorii (podrozdział 6.5.1). Dla warstwy sprzętowej takiego systemu przed uwzględnieniem aspektów ochrony informacji powinno się oszacować – przy wykorzystaniu odpowiednich modeli probabilistycznych – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie PFD_{avg} (i/lub średnią częstość występowania uszkodzenia niebezpiecznego na godzinę *PFH* – w trybie pracy częstej lub ciągłej), co odpowiada przedziałowi kryterialnemu związanemu z uzyskanym poziomem nienaruszalności bezpieczeństwa SIL (tablica 2.1, rozdział 2). Rozpatrywanemu systemowi II lub III kategorii należy w dalszej kolejności przypisać stopień ochrony informacji (np. w postaci poziomu uzasadnionego zaufania EAL – w tym wypadku EAL wiąże się z typem ochrony danych przesyłanych zewnętrznymi kanałami). Następnie należy dokonać odniesienia uzyskanego poziomu SIL do tablicy 7.1.

Schemat procedury weryfikacji SIL z uwzględnieniem aspektów ochrony informacji (przedstawionych w niniejszej monografii) bez wprowadzenia zagadnień niepewności przedstawiono na rys. 7.10 [21, 176, 196, 203, 204].

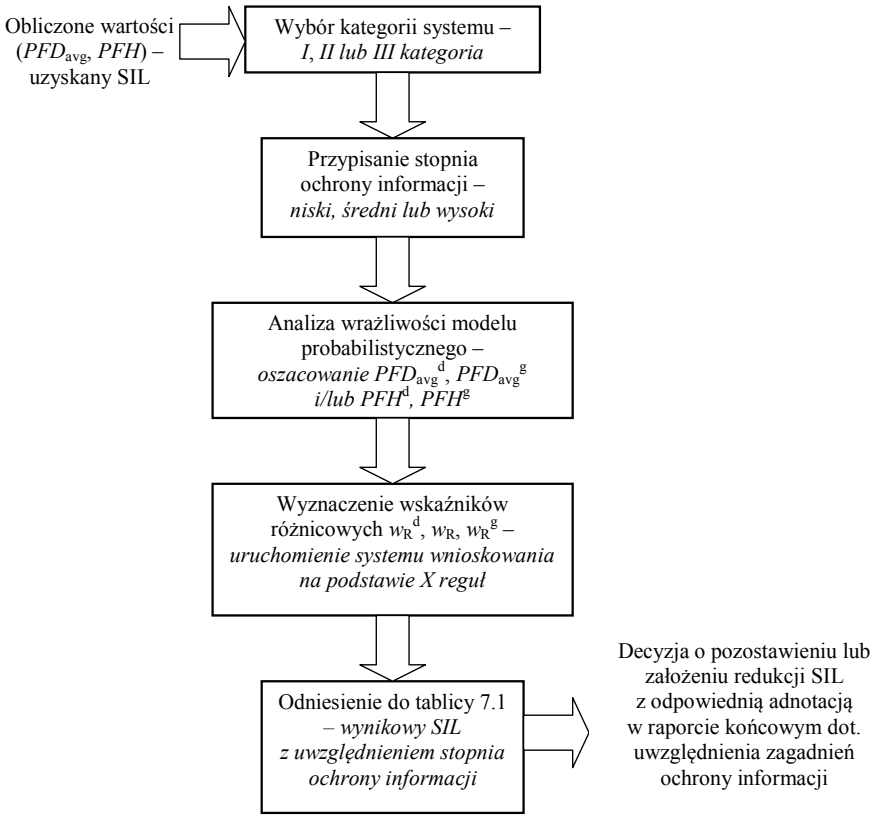


Rys. 7.10. Procedura weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji

W wyniku zestawienia uzyskanego na podstawie modelowania probabilistycznego poziomu nienaruszalności bezpieczeństwa SIL z tablicą 7.1, alokującą go w zależności od stopnia ochrony informacji, podejmuje się decyzję o jego pozostawieniu lub założeniu jego redukcji z odpowiednią adnotacją w raporcie końcowym.

W niniejszej monografii zaproponowano także strukturę systemu regułowego, wiążącego zagadnienia niepewności przy weryfikacji SIL z ochroną informacji poprzez uwzględnienie w procesie decyzyjnym (konkluzjach reguł) stopnia ochrony informacji (np. przy wykorzystaniu poziomów SAL, EAL lub liczby pierścieni zabezpieczeniowo-ochronnych wg SeSa). Przy weryfikacji SIL z uwzględnieniem stopnia ochrony informacji (np. EAL) bardzo istotne jest ustalenie kategorii systemu E/E/PE (BPCS lub SIS). W przypadku systemów II i III kategorii poziomy nienaruszalności bezpieczeństwa SIL odnoszą się do wymagań dla konkretnych funkcji bezpieczeństwa, a stopień ochrony informacji, wyrażony np. poziomem uzasadnionego zaufania EAL – do ochrony informacji całego systemu. Przyjęto, że niepożądane zdarzenia i działania z zewnątrz przy niskim poziomie ochrony informacji EAL mogą wpływać niekorzystnie na wypełnianie przez system funkcji bezpieczeństwa. Niski poziom uzasadnionego zaufania EAL przy weryfikacji uzyskanego poziomu SIL może skutkować jego obniżeniem. Schemat procedury weryfikacji SIL z uwzględnieniem zagadnień niepewności i ochrony informacji przedstawiono na rys. 7.11.

W danym przypadku oprócz dokonania wyboru kategorii systemu i przypisania stopnia ochrony informacji trzeba przeprowadzić analizę wrażliwości modelu probabilistycznego, następnie oszacować przedziały dolne i górne dla przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie PFD_{avg} (PFD_{avg}^{d}, PFD_{avg}^{g}) lub średniej częstości występowania uszkodzenia niebezpiecznego na godzinę PFH (PFH^{d}, PFH^{g}) [15, 25, 155, 175, 176]. W dalszym kroku należy wyznaczyć wskaźniki różnicowe oraz uruchomić system wnioskowania na podstawie zestawu dziesięciu reguł [24, 25, 155, 196] (rozdział 5). Dalsze postępowanie (czyli odniesienie do tablicy 7.1 – zawierającej wynikowe poziomy nienaruszalności bezpieczeństwa SIL z uwzględnieniem stopnia ochrony) jest takie jak w podejściu klasycznym przedstawionym na rys. 7.10 [176, 196].



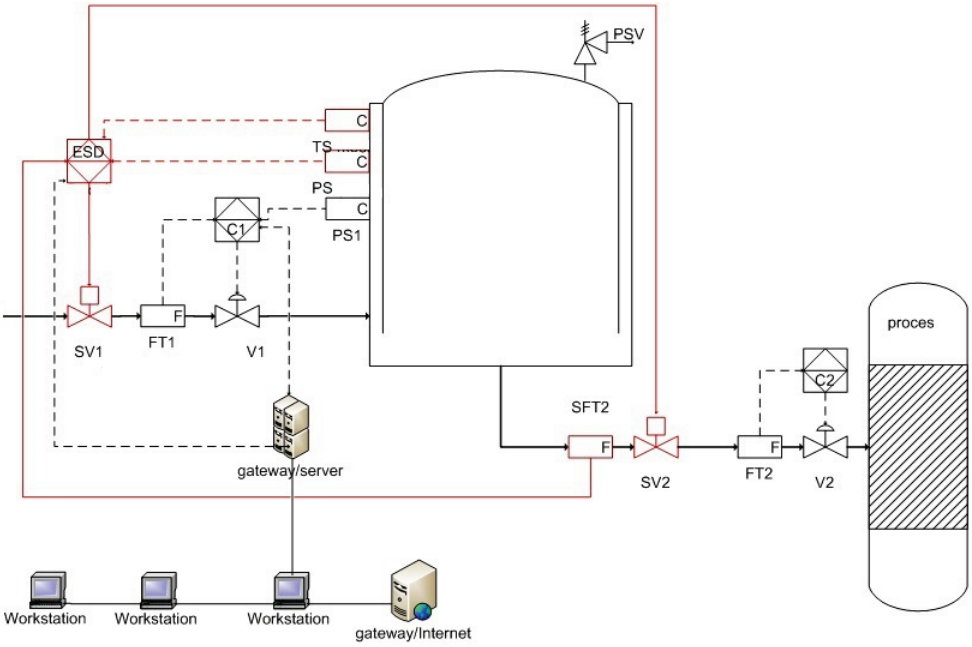
Rys. 7.11. Procedura weryfikacji SIL z uwzględnieniem zagadnień niepewności i aspektów związanych z ochroną informacji

7.6. Przykład weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji w przemysłowej sieci komputerowej

Etap weryfikacji SIL struktury sprzętowej realizującej funkcje bezpieczeństwa opiera się w głównej mierze na modelowaniu probabilistycznym złożonych struktur sprzętowych systemu SIS [4]. Na etapie tym, podobnie jak to ma miejsce przy określaniu wymagań, można uwzględnić zagadnienia ochrony informacji, bazując na przedstawionej wcześniej klasyfikacji systemów BPCS, DCS i SIS w obiektach i systemach infrastruktury krytycznej [188, 190, 200].

Na rys. 7.12 znajduje się schemat P&ID rozpatrywanej instalacji wraz z systemem sterowania i zabezpieczeń [176]. Na podstawie analizy ryzyka z uwzględnieniem zagadnień związanych z ochroną informacji dla systemu SIS określono wymagania SIL3. Rozpatrywany system należy do II kategorii. W danym przypadku system SIS ma potencjalny kontakt z siecią Internet poprzez wewnętrzną przemysłową sieć komputerową, serwer, sieć zewnętrzną oraz bramę. Zastosowanie technologii VPN w ramach Internetu może pozwolić na osiągnięcie niskiego poziomu ochrony informacji (np. EAL2). W nawiązaniu do procedury weryfikacji SIL zilustrowanej na rys. 7.10 na początku przeprowadzania tej czynności

należy zastosować metodę klasyczną. Uzyskane wyniki stanowią pakiet danych wejściowych do uruchomienia procedury z uwzględnieniem aspektów ochrony informacji.



Rys. 7.12. Schemat P&ID instalacji wraz z systemem sterowania BPCS i zabezpieczeń SIS

Weryfikację SIL z uwzględnieniem zagadnień ochrony informacji przeprowadzono przy wykorzystaniu autorskiego oprogramowania ProSIL-EAL, będącego rozbudowaną wersją narzędzia komputerowego ProSIL [200, 201]. W tablicy 7.2 zestawiono dane niezawodnościowe elementów poddanego weryfikacji systemu SIS [70, 157].

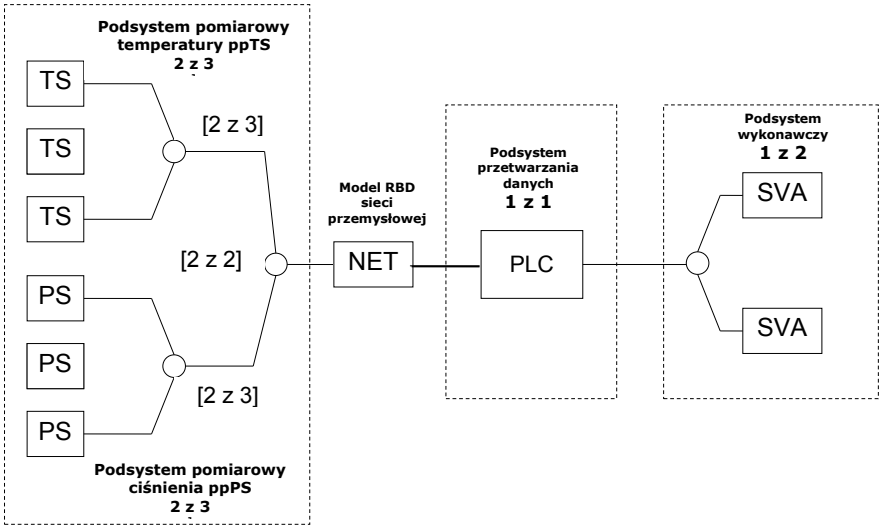
Tablica 7.2

Dane niezawodnościowe dla elementów systemu zabezpieczeniowego

Element	PS	TS	NET	PLC	Safety PLC	SRS	SVA
DC [%]	54	66	99	90	99	99	24
λ_{DU} [1/h]	$3 \cdot 10^{-7}$	$3 \cdot 10^{-6}$	$8{,}5 \cdot 10^{-8}$	$4 \cdot 10^{-6}$	$2{,}2 \cdot 10^{-8}$	$8 \cdot 10^{-8}$	$8 \cdot 10^{-7}$
T_I [h]	8760	8760	8760	8760	8760	8760	8760
β	0,02	0,02	0,01	0,01	0,01	0,01	0,02

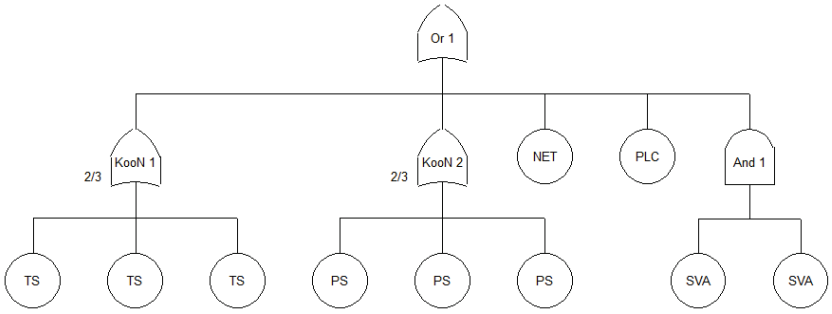
W danym przypadku analizie zostały poddane trzy struktury przykładowego systemu SIS, których schematy przedstawiono, odpowiednio, na rysunkach 7.13 – SIS (I), 7.15 – SIS (II), 7.16 – SIS (III) oraz 7.17 – SIS (IV).

Na rys. 7.13 znajduje się pierwsza struktura sprzętowa systemu SIS (I), która została oparta na układzie sterownika PLC.



Rys. 7.13. Architektura systemu SIS (I) wyposażona w sterownik PLC (matryce detektorów pracują w konfiguracji 2 z 2)

Na rys. 7.14 pokazano drzewo niezdatności systemu SIS (I), na podstawie którego można wyznaczyć cięcia minimalne potrzebne do budowy modelu probabilistycznego.



Rys. 7.14. Model FT systemu SIS (I)

Uwzględniając dane niezawodnościowe zawarte w tablicy 7.2, uzyskano wyniki, które wraz z całościową specyfikacją sprzętową systemu SIS (I) zestawiono w raporcie końcowym znajdującym się w tablicy 7.3.

Tablica 7.3

Raport końcowy weryfikacji SIL dla systemu SIS (I)

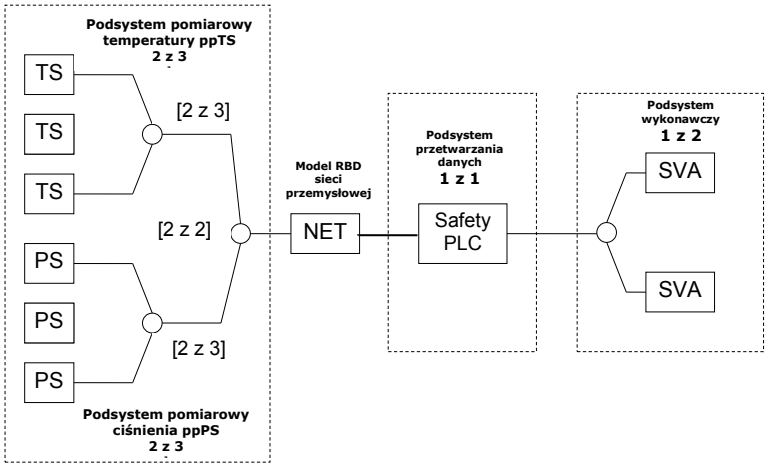
System /podsystem /element		*k* z *n*	β [%]	PFD_{avg}	SIL
SIS (I)	**0**	**–**	**–**	**$1{,}85\cdot10^{-2}$**	**1**
ppTS	**.1**	**2 z 3**	**3**	**$2{,}93\cdot10^{-5}$**	**4**
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2
TS	..2	–	–	$1{,}53\cdot10^{-3}$	2
ppPS	**.1**	**2 z 3**	**3**	**$3{,}11\cdot10^{-5}$**	**4**
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2
PS	..2	–	–	$1{,}58\cdot10^{-3}$	2
NET	**.1**		**–**	**$3{,}72\cdot10^{-4}$**	**3**
ESD	**.1**	**1 z 1**	**–**	**$1{,}8\cdot10^{-2}$**	**1**
PLC	..2	–	–	$1{,}8\cdot10^{-2}$	1
pwSV	**.1**	**1 z 2**	**2**	**$7{,}14\cdot10^{-5}$**	**4**
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2
SVA	..2	–	–	$3{,}5\cdot10^{-3}$	2

$$PFD_{avgSIS(I)} \cong PFD_{avgTS(2z3)} + PFD_{avgPS(2z3)} + PFD_{avgNET} + PFD_{avgPLC} + PFD_{avgSVA(1z2)} \cong$$
$$\cong 2{,}93\cdot10^{-5} + 3{,}11\cdot10^{-5} + 3{,}72\cdot10^{-4} + 1{,}8\cdot10^{-2} + 7{,}14\cdot10^{-5} \cong 1{,}85\cdot10^{-2} \Rightarrow \text{SIL1} \tag{7.4}$$

gdzie: $PFD_{avgSIS(I)}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla systemu SIS (I); $PFD_{avgTS(2z3)}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu pomiaru temperatury ppTS w konfiguracji 2 z 3; $PFD_{avgPS(2z3)}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu pomiaru ciśnienia ppPS w konfiguracji 2 z 3; PFD_{avgNET} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla warstwy sieciowej; PFD_{avgPLC} – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie dla sterownika PLC; $PFD_{avgSVA(1z2)}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania dla podsystemu wykonawczego pwSVA w konfiguracji 1 z 2.

Stąd wynika, że struktura sprzętowa systemu SIS (I) wyposażona w sterownik PLC nie spełnia wymagań SIL3.

Na rys. 7.15 znajduje się kolejna struktura sprzętowa SIS (II), która została oparta na układzie sterownika bezpieczeństwa *safety* PLC.



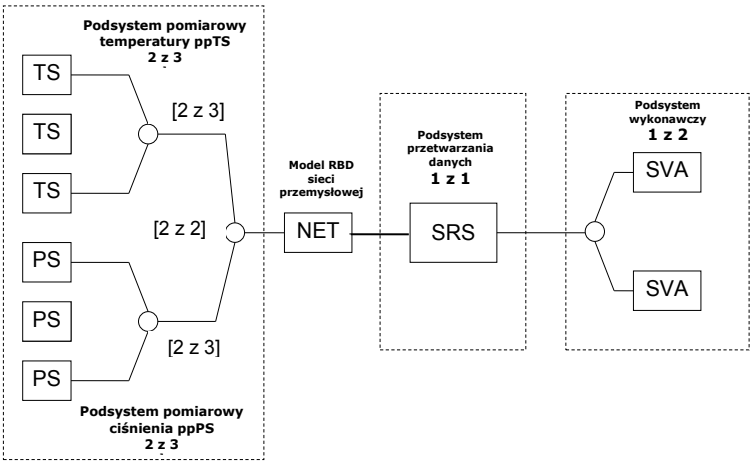
Rys. 7.15. Architektura systemu SIS (II) wyposażona w sterownik safety PLC (matryce detektorów pracują w konfiguracji 2 z 2)

Uwzględniając dane niezawodnościowe zawarte w tablicy 7.2, uzyskano wynik w postaci punktowej wartości prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie:

$$PFD_{\text{avgSIS(II)}} \cong PFD_{\text{avgTS(2z3)}} + PFD_{\text{avgPS(2z3)}} + PFD_{\text{avgNET}} + PFD_{\text{avgSafetyPLC}} + PFD_{\text{avgSVA(1z2)}} \cong$$
$$\cong 2{,}93 \cdot 10^{-5} + 3{,}11 \cdot 10^{-5} + 3{,}72 \cdot 10^{-4} + 9{,}64 \cdot 10^{-5} + 7{,}14 \cdot 10^{-5} \cong 6 \cdot 10^{-4} \Rightarrow \text{SIL3} \tag{7.5}$$

gdzie: $PFD_{\text{avgSIS(II)}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie do działania przez system SIS (II); $PFD_{\text{avgSafetyPLC}}$ – przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie dla sterownika *safety* PLC.

Stąd wynika, że struktura sprzętowa systemu SIS (II) spełnia wymagania SIL3.



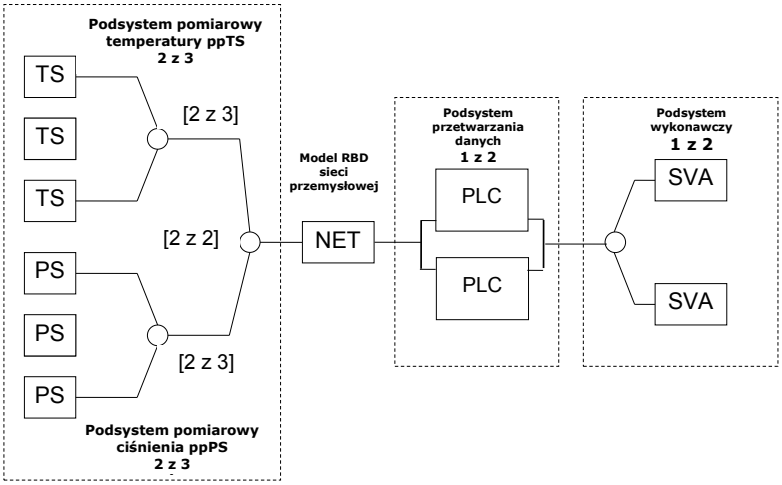
Rys. 7.16. Architektura systemu SIS (III) wyposażona w system SRS

Na rys. 7.16 przedstawiono system SIS (III), przy czym w podsystemie przetwarzania danych zastosowano układ SRS (np. przekaźnik programowalny).

$$PFD_{\text{avgSIS(III)}} \cong PFD_{\text{avgTS(2z3)}} + PFD_{\text{avgPS(2z3)}} + PFD_{\text{avgNET}} + PFD_{\text{avgSRS}} + PFD_{\text{avgSVA(1z2)}} \cong$$
$$\cong 2{,}93 \cdot 10^{-5} + 3{,}11 \cdot 10^{-5} + 3{,}72 \cdot 10^{-4} + 3{,}5 \cdot 10^{-4} + 7{,}14 \cdot 10^{-5} \cong 8{,}54 \cdot 10^{-4} \Rightarrow \text{SIL3} \tag{7.6}$$

System SIS (III) zrealizowany z wykorzystaniem układu SRS w podsystemie przetwarzania danych spełnia wymagania SIL3.

Na rys. 7.17 pokazano system SIS (IV), przy czym w podsystemie przetwarzania danych zastosowano standardowe sterowniki programowalne PLC w redundancji 1 z 2.



Rys. 7.17. Architektura systemu SIS (IV) wyposażona w dwa sterowniki PLC (konfiguracja 1 z 2)

$$PFD_{\text{avgSIS(IV)}} \cong PFD_{\text{avgTS(2z3)}} + PFD_{\text{avgPS(2z3)}} + PFD_{\text{avgNET}} + PFD_{\text{avgPLC(1z2)}} + PFD_{\text{avgSVA(1z2)}} \cong$$
$$\cong 2{,}93 \cdot 10^{-5} + 3{,}11 \cdot 10^{-5} + 3{,}72 \cdot 10^{-4} + 5{,}04 \cdot 10^{-4} + 7{,}14 \cdot 10^{-5} \cong 1{,}01 \cdot 10^{-3} \Rightarrow \text{SIL2} \tag{7.7}$$

Stąd wynika, że struktura sprzętowa systemu SIS (IV) nie spełnia wymagań SIL3.

Weźmy następnie pod uwagę system SIS (III) (rys. 7.16), zrealizowany z wykorzystaniem układu SRS w podsystemie przetwarzania danych, który spełnia wymagania SIL3. Punktowa wartość prawdopodobieństwa $PFD_{\text{avgSIS(III)}} = 8{,}54 \cdot 10^{-4}$, opisana zależnością (7.6), mieści się w przedziale kryterialnym odpowiadającym poziomowi SIL3. Jest to początek procedury weryfikacji SIL z uwzględnieniem zagadnień ochrony informacji, przedstawionej na rys. 7.10.

W danym przypadku rozpatrywany system należy do II kategorii, natomiast poziom ochrony informacji zdeterminowany poziomem uzasadnionego zaufania EAL2 jest niski. Kolejnym krokiem jest „zmapowanie" powyższych informacji do tablicy 7.1, zawierającej wynikowe poziomy nienaruszalności bezpieczeństwa SIL z uwzględnieniem stopnia ochrony informacji i kategorii rozpatrywanego systemu. W danym przypadku weryfikowany poziom nienaruszalności bezpieczeństwa po uwzględnieniu aspektów ochrony informacji ulega redukcji do SIL2. Zestawienie uzyskanych wyników znajduje się w tablicy 7.4.

Tablica 7.4

Raport wynikowy weryfikacji SIL z uwzględnieniem aspektów ochrony informacji dla systemu II kategorii SIS (III) [200]

SIS	Zweryfikowany SIL	
EAL/ stopień ochrony informacji/ SAL	bez ochrony informacji	z ochroną informacji
brak/ brak (podejście klasyczne)	SIL3	–
EAL2/ niski/SAL1	SIL3	SIL2
EAL3/ średni/SAL2	SIL3	SIL3

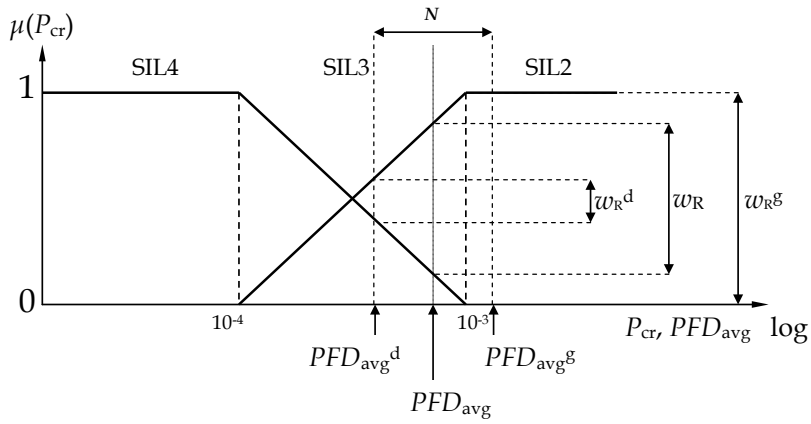
Aby spełnić wymagania kryterialne SIL3 postawione systemowi SIS, należy zwiększyć stopień ochrony informacji systemu SIS (III) do średniego (równy lub większy od EAL3, SAL2 bądź wg SeSa – 2 lub więcej pierścieni zabezpieczeniowo-ochronnych).

Zaprezentowany przykład przedstawia możliwość uwzględnienia zagadnień związanych z ochroną informacji w procesie weryfikacji SIL. Widać, że kluczową rolę w proponowanym postępowaniu (wg tabl. 7.1) odgrywa kategoria rozpatrywanego systemu SIS. W danym przypadku był to system II kategorii. Gdyby system należał do III kategorii (np. działał na bazie sieci Wi-Fi), wówczas uzyskany poziom nienaruszalności bezpieczeństwa SIL zredukowałby się do SIL1 (aby zapewnić spełnienie wymagań SIL3, trzeba by było zapewnić ochronę informacji zdefiniowaną wysokim stopniem – np. EAL5 wg *Common Criteria* [93] lub powyżej 5 pierścieni zabezpieczeniowo-ochronnych wg metodyki SeSa). Wykorzystując podejście przedstawione powyżej, można dokonać weryfikacji SIL dla punktowej wartości PFD_{avg} (lub *PFH*) uzyskanej dla systemu SIS z uwzględnieniem aspektów ochrony informacji.

Wartości PFD_{avg} (lub *PFH*) otrzymane na podstawie oszacowań analitycznych mają charakter punktowy. Zdarza się, że znajdują się blisko dolnej lub górnej granicy przedziału dyskretnego odpowiadającego poziomowi nienaruszalności bezpieczeństwa SIL. Przy weryfikacji SIL użytecznym parametrem jest wskaźnik różnicowy w_R, niosący informację dotyczącą położenia punktowych wartości PFD_{avg} oraz *PFH* w przedziale kryterialnym. Zaproponowana (w rozdziale 5 monografii) metoda wykorzystująca wskaźniki różnicowe jest pomocna w efektywnej weryfikacji wymaganego poziomu SIL systemów E/E/PE z uwzględnieniem wyników analizy wrażliwości i/lub oszacowanych przedziałów niepewności na podstawie systemu wnioskowania opartego na zbiorze dziesięciu reguł. W danym przypadku, weryfikując poziom nienaruszalności bezpieczeństwa SIL, można uwzględnić wpływ zagadnień ochrony informacji poprzez odpowiednie zastosowanie w regułach wnioskowania (7.8) stopnia ochrony informacji (niski, średni lub wysoki), wykorzystując w tym celu np. poziom uzasadnionego zaufania EAL, poziom uzasadnionej ochrony SAL lub liczbę pierścieni zabezpieczeniowo-ochronnych wg metodyki SeSa.

$$
\begin{aligned}
&\text{I. } w_{\mathrm{R}} < 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow \mathrm{EAL} \geq 3; \mathrm{SAL} \geq 2; \text{sredni} \\
&\text{II. } w_{\mathrm{R}} = 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow \mathrm{EAL} \geq 3; \mathrm{SAL} \geq 2; \text{sredni} \\
&\text{III. } w_{\mathrm{R}} > 0 \Rightarrow \mathrm{SIL}X+ \Leftrightarrow \mathrm{EAL} \geq 5; \mathrm{SAL} \geq 3; \text{wysoki} \\
&\text{IV. } w_{\mathrm{R}}^{\mathrm{d}} < 0 \wedge w_{\mathrm{R}} < 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} = -1 \Rightarrow \mathrm{SIL}(X-1)+ \Leftrightarrow \mathrm{EAL} \geq 3; \mathrm{SAL} \geq 2; \text{sredni} \\
&\text{V. } w_{\mathrm{R}}^{\mathrm{d}} < 0 \wedge w_{\mathrm{R}} < 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} = -1 \Rightarrow \mathrm{SIL}(X-1) \Leftrightarrow \mathrm{EAL} < 3; \mathrm{SAL} < 2; \text{niski} \\
&\text{VI. } w_{\mathrm{R}}^{\mathrm{d}} < 0 \wedge w_{\mathrm{R}} < 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow \mathrm{EAL} \geq 5; \mathrm{SAL} \geq 3; \text{wysoki} \\
&\text{VII. } w_{\mathrm{R}}^{\mathrm{d}} > 0 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow \mathrm{EAL} \geq 3; \mathrm{SAL} \geq 2; \text{sredni} \\
&\text{VIII. } w_{\mathrm{R}}^{\mathrm{d}} = 1 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X+ \Leftrightarrow \mathrm{EAL} \geq 5; \mathrm{SAL} \geq 3; \text{wysoki} \\
&\text{IX. } w_{\mathrm{R}}^{\mathrm{d}} > 0 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} \geq 0 \Rightarrow \mathrm{SIL}X+ \Leftrightarrow \mathrm{EAL} \geq 5; \mathrm{SAL} \geq 3; \text{wysoki} \\
&\text{X. } w_{\mathrm{R}}^{\mathrm{d}} = 1 \wedge w_{\mathrm{R}} > 0 \wedge w_{\mathrm{R}}^{\mathrm{g}} < 0 \Rightarrow \mathrm{SIL}X \Leftrightarrow EF \geq 3 \Leftrightarrow \mathrm{EAL} \geq 5; \mathrm{SAL} = 4; \text{wysoki}
\end{aligned}
\tag{7.8}
$$

Wykorzystując podejście przedstawione powyżej, można dokonać weryfikacji uzyskanego poziomu nienaruszalności bezpieczeństwa SIL dla punktowej wartości PFD_{avg}, oszacowanej dla przykładowego systemu SIS realizującego funkcje bezpieczeństwa (rys. 7.17).



Rys. 7.17. Weryfikacja SIL systemu SIS (III) dla punktowej wartości $\mathrm{PFD}_{\mathrm{avg}} = 8{,}54 \cdot 10^{-4}$ oraz $\mathrm{PFD}_{\mathrm{avg}}{}^{\mathrm{d}} = 5{,}69 \cdot 10^{-4}$; $\mathrm{PFD}_{\mathrm{avg}}{}^{\mathrm{g}} = 1{,}28 \cdot 10^{-3}$; EF = 1,5 (przy średnim stopniu ochrony informacji)

Punktowa wartość przeciętnego prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na rzadkie przywołanie mieści się w przedziale odpowiadającym poziomowi nienaruszalności bezpieczeństwa SIL3. Powyższy przypadek pokazuje, że wartość $PFD_{\mathrm{avg}} = 8{,}54 \cdot 10^{-4}$, otrzymana dla systemu SIS, odpowiada poziomowi SIL3, jednak jest ona bliska kryteriom probabilistycznym odpowiadającym SIL2. Poziom uzasadnionego zaufania EAL uzyskany dzięki zastosowanym zabezpieczeniom jest większy od 3. Powstaje pytanie, jaki poziom SIL spełnia rozpatrywana architektura systemu SIS. W danym przypadku przy współczynniku błędu EF = 1,5 dolna granica $PFD_{\mathrm{avg}}{}^{\mathrm{d}} = 5{,}69 \cdot 10^{-4}$, górna odpowiada zaś wartości $PFD_{\mathrm{avg}}{}^{\mathrm{g}} = 1{,}28 \cdot 10^{-3}$. Uwzględniając je w dalszej analizie, można stwierdzić (na podstawie reguły IV), że analizowany system SIS (III) (rys. 7.16), który jest systemem II kategorii, nie spełnia wymagań SIL3, tylko SIL2+.

$$
\begin{aligned}
w_{\mathrm{R}}^{\mathrm{d}} &= \mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{\mathrm{avg}}{}^{\mathrm{d}}) - \mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{\mathrm{avg}}{}^{\mathrm{d}}) = 0,42 - 0.58 = -0,16 \Rightarrow w_{\mathrm{R}}^{\mathrm{d}} < 0 \\
w_{\mathrm{R}} &= \mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{avg}) - \mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{avg}) = 0,14 - 0,86 = -0.72 \Rightarrow w_{\mathrm{R}} < 0 \rightarrow \mathrm{SIL2+} \\
w_{\mathrm{R}}^{\mathrm{g}} &= \mu_{\mathrm{SIL}}^{\mathrm{d}}(PFD_{\mathrm{avg}}{}^{\mathrm{g}}) - \mu_{\mathrm{SIL}}^{\mathrm{g}}(PFD_{\mathrm{avg}}{}^{\mathrm{g}}) = 0 - 1 \Rightarrow w_{\mathrm{R}}^{\mathrm{g}} = -1
\end{aligned}
\tag{7.9}
$$

Zaprezentowany przykład przedstawia możliwość uwzględnienia zagadnień związanych z ochroną informacji w procesie weryfikacji SIL. Widać, że kluczową rolę w proponowanym postępowaniu odgrywa kategoria rozpatrywanego systemu. W danym przypadku był to system II kategorii. Gdyby rozpatrywany system był III kategorii, wówczas otrzymany poziom SIL zredukowałby się do SIL2, a po uwzględnieniu niepewności przy średnim stopniu ochrony informacji (odpowiadającym poziomowi uzasadnionego zaufania EAL3 lub poziomowi uzasadnionej ochrony SAL2) – do SIL1+. Biorąc pod uwagę kategorię systemu, informacje zawarte w tablicy 7.1 oraz system regułowy, można w procesie weryfikacji SIL w warunkach niepewności uwzględnić aspekty ochrony informacji. Aspekty te wiążą się ze stopniem ochrony (niski, średni lub wysoki) reprezentowanym przez poziomy EAL, SAL lub liczbę pierścieni zabezpieczeniowo-ochronnych wg metodyki SeSa. Wykorzystując podejście przedstawione powyżej, można dokonać weryfikacji SIL dla punktowej wartości PFD_{avg} (lub *PFH*) uzyskanej dla systemu SIS, z uwzględnieniem zagadnień cyberbezpieczeństwa w przemysłowej sieci komputerowej.

7.7. Podsumowanie

W niniejszym rozdziale przedstawiono podejście metodyczne w integracji analizy i oceny bezpieczeństwa funkcjonalnego rozproszonych systemów sterowania i zabezpieczeń w obiektach infrastruktury krytycznej w nawiązaniu do wymagań norm PN-EN 61508 i PN-EN 61511 z uwzględnieniem zasad ochrony informacji według ISO/IEC 15408 (poziomy EAL), ochrony informacji w przemysłowych sieciach komputerowych wg IEC 62443 (poziomy SAL) oraz metodyki SeSa SINTEF, na przykładzie procesu weryfikacji SIL.

Zaprezentowano sposób wykorzystania metod weryfikacji poziomów nienaruszalności bezpieczeństwa SIL z uwzględnieniem zagadnień ochrony informacji w przemysłowych sieciach komputerowych. Metody te stanowią aktualizację metodyki zawartej w normach PN-EN 61508 i PN-EN 61511. Omówione metody zostały zaimplementowane w module ProSILer aplikacji komputerowej ProSIL-EAL [10, 11, 13, 22, 196]. W tym celu wykorzystano opracowane wcześniej podejście metodyczne dotyczące integracji analizy i oceny bezpieczeństwa funkcjonalnego rozproszonych systemów sterowania, monitorowania i zabezpieczeń w obiektach infrastruktury krytycznej. Przedstawiona koncepcja integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji uwzględnia klasyfikację systemów rozproszonych na kategorie [175, 176, 196].

Mimo że aspekty związane z analizami bezpieczeństwa funkcjonalnego i ochrony informacji zasadniczo się różnią i dotyczą odrębnych zagadnień (bezpieczeństwo funkcjonalne – automatyka, obszar OT; ochrona informacji – informatyka, technologie informacyjne, obszar IT), uwzględnienie zagadnień ochrony informacji w analizach bezpieczeństwa funkcjonalnego jest możliwe. Metody weryfikacji poziomów nienaruszalności bezpieczeństwa SIL rozważanych architektur sprzętowych (systemów SIS) z uwzględnieniem aspektów ochrony informacji wiążą w odpowiedni sposób kryteria bezpieczeństwa funkcjonalnego ze stopniem ochrony informacji określonym na podstawie poziomów uzasadnionego zaufania

EAL (*Common Criteria*), poziomów uzasadnionej ochrony SAL lub liczby pierścieni zabezpieczeniowo-ochronnych (SeSa) [176, 196].

Przedstawione przykłady wykazały, że z punktu widzenia analiz bezpieczeństwa funkcjonalnego (w procesie weryfikacji poziomów nienaruszalności bezpieczeństwa SIL – sytuacja, gdy system SIS nie jest w pełni odseparowany od przemysłowej sieci komputerowej) można zastosować zbliżone ideowo do poziomów SIL poziomy uzasadnionego zaufania EAL. Ich praktyczna implementacja oraz trudności w ich interpretacji i zrozumieniu sprawiają jednak, że daje się zauważyć trend do ich niewykorzystywania w próbach integracji z bezpieczeństwem funkcjonalnym przy analizach systemów rozproszonych integrowanych przemysłową siecią komputerową [175, 176, 196].

Podejście CC [93] dotyczy w zdecydowanej większości pojedynczych rozwiązań technicznych (urządzeń, aplikacji komputerowych itp.), a nie podsystemów czy całych systemów, natomiast podejście wykorzystujące metodykę SeSa, polegające na określeniu stopnia ochrony informacji poprzez liczbę zastosowanych pierścieni zabezpieczeniowo-ochronnych, zawiera się w tonie metodyki opisanej w normie PN-EN 61511 [162], a nawet technologicznie ją przewyższa [176, 196].

W związku z tym należy poważnie rozważyć stosowność korzystania z miar EAL na rzecz wartości bardziej ogólnych, będących urzeczywistnieniem realnego poziomu bezpieczeństwa związanego z ochroną informacji, a w istocie poziomu związanego z nią ryzyka. Potrzebne są zintensyfikowane badania i poszukiwania optymalnych rozwiązań stosowanych w integrowaniu zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji [21, 176, 196]. Zaprezentowane podejście stanowi rozszerzenie (o zagadnienia ochrony) metodyki zawartej w normach PN-EN 61508 oraz PN-EN 61511 i zostało zaimplementowane w prototypowym oprogramowaniu wspomagającym zarządzanie bezpieczeństwem funkcjonalnym w cyklu życia ProSIL-EAL.

Rozdział 8

KOMPUTEROWE WSPOMAGANIE PROCESU ANALIZY BEZPIECZEŃSTWA FUNKCJONALNEGO Z UWZGLĘDNIENIEM ASPEKTÓW OCHRONY INFORMACJI

8.1. Wprowadzenie

W niniejszym rozdziale omówiono oprogramowanie ProSIL (oraz jego rozbudowaną o aspekty ochrony informacji wersję ProSIL-EAL), wspomagające zarządzanie bezpieczeństwem funkcjonalnym. Program ProSIL składa się trzech modułów wspomagających określanie wymaganego poziomu SIL (moduł ProSILen) oraz weryfikację SIL (moduł ProSILer). W aplikacji ProSIL zaimplementowano opracowaną w trakcie badań metodykę analizy bezpieczeństwa funkcjonalnego w projektowaniu i użytkowaniu systemów SIS zgodnie wymaganiami z PN-EN 61508 i PN-EN 61511. Do określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla zdefiniowanych funkcji bezpieczeństwa w module ProSILen wykorzystuje się metody matrycy oraz grafów ryzyka. Do weryfikacji SIL systemów SIS i BPCS zastosowano metody ilościowe wykorzystujące schematy blokowe niezawodności, grafy Markowa, drzewa niezdatności i technikę cięć minimalnych oraz gotowe modele probabilistyczne systemów E/E/PE zawarte w normach.

Aplikacja ProSIL została zaprojektowana do wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym w cyklu życia systemów technicznych związanych z bezpieczeństwem. Ogólne założenia projektowe tej aplikacji obejmują wspomaganie procesu projektowania systemów E/E/PE, BPCS i SIS zgodnie wymaganiami i kryteriami norm PN-EN 61508 i PN-EN 61511 [161, 162]. Program ProSIL umożliwia wyznaczanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL na podstawie wymagań instytucji nadzorującej dla wyróżnionych funkcji bezpieczeństwa. ProSIL wyposażony jest także w moduł wspomagający komputerową weryfikację poziomu nienaruszalności bezpieczeństwa SIL dla rozważanych architektur sprzętu poszczególnych funkcji bezpieczeństwa. Zapewnia również wspomaganie w ocenie rozwiązań technicznych i organizacyjnych (poprzez uwzględnienie różnych czynników) sprzyjających redukcji wpływu błędów systematycznych oprogramowania i błędów człowieka-operatora podczas eksploatacji systemów E/E/PE, BPCS i SIS [13, 15, 25, 121]. W aplikacji ProSIL dokumentowane są na bieżąco projekty analizy bezpieczeństwa funkcjonalnego; możliwe jest drukowanie części zgromadzonych danych w ramach projektu i finalnego raportu.

8.2. Założenia funkcjonalne aplikacji ProSIL

Wychodząc naprzeciw oczekiwaniom przyszłych analityków bezpieczeństwa funkcjonalnego i użytkowników systemów E/E/PE w krajowym przemyśle, zaproponowano wymienione poniżej założenia dotyczące aplikacji komputerowej ProSIL do wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym w cyklu życia. W budowie aplikacji wykorzystano bazy danych oraz bazę wiedzy, która może być systematycznie aktualizowana o nowe wytyczne i metodyki dotyczące zagadnień bezpieczeństwa funkcjonalnego.

Główne założenia aplikacji ProSIL to:

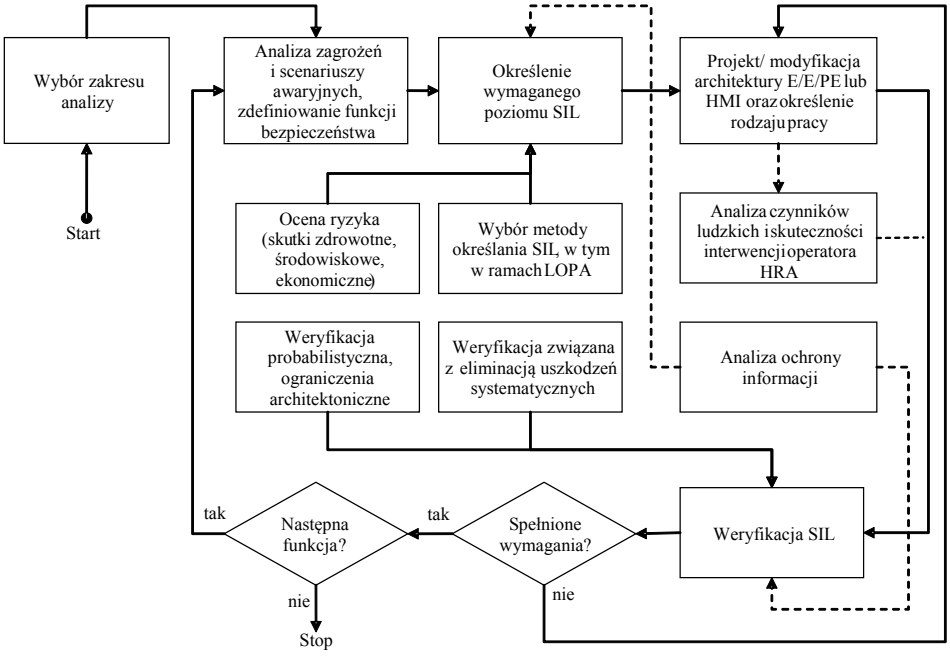
— wspomaganie procesu projektowania systemów E/E/PE, BPCS i SIS zgodnie wymaganiami i kryteriami norm IEC 61508 i IEC 61511;
— możliwość wyznaczania wymaganego poziomu nienaruszalności bezpieczeństwa SIL metodą matrycy ryzyka lub grafu ryzyka bądź wprowadzanie SIL na podstawie wymagań instytucji nadzorującej dla wyróżnionych funkcji bezpieczeństwa;
— wspomagana komputerowo weryfikacja poziomu nienaruszalności bezpieczeństwa SIL dla rozważanych architektur sprzętu poszczególnych funkcji bezpieczeństwa;
— wspomaganie w ocenie rozwiązań technicznych i organizacyjnych sprzyjających redukcji wpływu błędów systematycznych oprogramowania i błędów człowieka podczas eksploatacji systemów E/E/PE, BPCS i SIS;
— wyposażenie aplikacji w pomoc kontekstową;
— możliwość elektronicznego dokumentowania projektów analizy bezpieczeństwa funkcjonalnego; możliwe jest drukowanie fragmentów lub całości raportów.

Dodatkowo założono, że aplikacja ProSIL będzie udostępniać użytkownikom następujące możliwości:

— dostęp do odpowiednich modułów i baz danych do prowadzenia projektów analizy bezpieczeństwa funkcjonalnego dla danego obiektu złożonego lub instalacji procesowej;
— możliwość definiowania scenariuszy awaryjnych bazujących na wynikach metody HAZOP lub metody ET (*event trees*) z uwzględnieniem występujących zagrożeń i zdarzeń inicjujących;
— możliwość definiowania matrycy ryzyka do przedstawienia poziomów ryzyka związanego z wyróżnionymi scenariuszami;
— dostęp do biblioteki grafów ryzyka z możliwością definiowania i modyfikowania parametrów związanych z ryzykiem;
— definiowanie zbioru funkcji bezpieczeństwa w ramach danego projektu (konkretny obiekt złożony lub instalacja w projektowaniu lub eksploatacji);
— przedstawianie architektury sprzętu realizującego funkcję bezpieczeństwa za pomocą schematów blokowych RBD (*reliability block diagram*) z wyróżnieniem podsystemów i elementów;
— możliwość potwierdzenia przeprowadzonej wcześniej analizy błędów systematycznych w systemie E/E/PE przed przystąpieniem do modelowania probabilistycznego tego systemu;
— wspomaganie w określaniu rodzaju pracy podsystemów i systemu E/E/PE: rzadkiego przywołania do działania lub częstego przywołania do działania i pracy ciągłej;
— przeprowadzanie modelowania probabilistycznego systemów na podstawie modeli probabilistycznych podsystemów; podsystemy mogą być traktowane ogólnie jako systemy „*k* z *n*”;
— dostęp do biblioteki modeli probabilistycznych podsystemów zgodnie z PN-EN 61508 oraz modeli w wersji rozszerzonej, wyznaczonych metodami cięć minimalnych (uzyskanych np. na podstawie metody schematów blokowych RBD lub drzew niezdatności FT) i grafów Markowa; baza modeli probabilistycznych będzie uaktualniana w kolejnych wersjach aplikacji;
— dostęp do ogólnej bazy danych niezawodnościowych i innych parametrów modeli probabilistycznych wyróżnionych kategorii elementów (lub podsystemów) z możliwością jej aktualizacji; aplikacja pozwala użytkownikowi na wprowadzenie własnych danych

niezawodnościowych, w tym również danych z istniejących baz danych niezawodnościowych z podaniem źródła informacji;
— możliwość określenia współczynnika pokrycia diagnostycznego elementu lub podsystemu wspomagana przez system z bazą wiedzy;
— optymalizowanie czasów testowania nieautomatycznego elementów (lub podsystemów) w systemie E/E/PE lub SIS;
— możliwość wyznaczania i graficznej reprezentacji przebiegu w czasie prawdopodobieństwa niezadziałania na przywołanie $PFD(t)$ oraz obliczanie przeciętnego prawdopodobieństwa PFD_{avg} podsystemów i systemów E/E/PE i SIS dla rodzaju pracy rzadkiego przywołania do działania oraz częstości występowania niebezpiecznego uszkodzenia na godzinę PFH w przypadku rodzaju pracy częstego przywoływania tych systemów do działania lub ich pracy ciągłej w nawiązaniu do zakresu i wymagań normy PN-EN 61508;
— koncepcja aplikacji umożliwia realizację części rozszerzonej analizy bezpieczeństwa funkcjonalnego, która pozwala m.in. na dołączenie do niej dodatkowych narzędzi do oceny wrażliwości i niepewności w modelowaniu ryzyka i modelowaniu probabilistycznym, a także wybranych aspektów analizy ochrony informacji w sieciach rozproszonych [17, 18, 155].

Strukturę aplikacji komputerowej ProSIL, uwzględniającą jej ogólne oraz szczegółowe założenia, przedstawiono na rys. 8.1. W obecnej wersji opisywanego oprogramowania zostały zaimplementowane założenia ogólne oraz znaczna większość założeń szczegółowych.



Rys. 8.1. Ogólny schemat funkcjonalny aplikacji komputerowej ProSIL

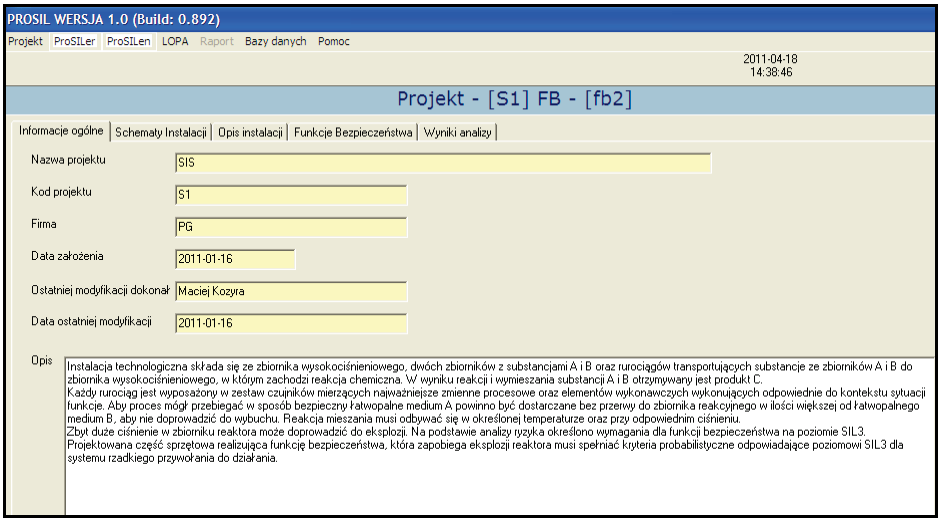
W aplikacji ProSIL przewidziano dodatkowo możliwość uwzględnienia zagadnień związanych z ochroną informacji w przemysłowych skomputeryzowanych rozproszonych systemach sterowania i zabezpieczeń w zarządzaniu bezpieczeństwem funkcjonalnym. Wpływ zagadnień związanych z ochroną informacji na określanie wymaganego poziomu nienaruszalności SIL oraz jego weryfikację zostanie zaimplementowany w najnowszej wersji aplikacji w sposób niezależny dla modułów ProSILen oraz ProSILer.

Program komputerowy ProSIL (ProSIL-EAL) jest przeznaczony do pracy jako indywidualne stanowisko robocze. Program ProSIL powstał w środowisku programowania RAD (*Rapid Application Development*) Delphi®.

8.3. Okna i moduły w aplikacji ProSIL

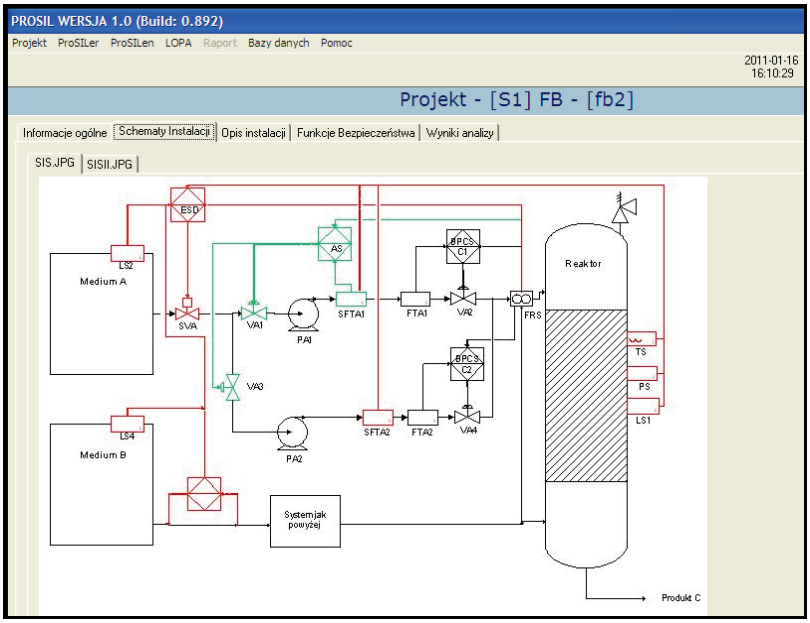
8.3.1. Okno główne

Głównym elementem aplikacji ProSIL jest okno umożliwiające zdefiniowanie nowych lub edytowanie istniejących projektów, w których zawarte są poszczególne funkcje bezpieczeństwa. Każdy nowo wprowadzony projekt ma szczegółowy opis, który jest przechowywany w bazie danych aplikacji ProSIL. Po wyborze funkcji bezpieczeństwa można przejść bezpośrednio do modułów określania i weryfikacji. Na rys. 8.2 przedstawiono główne okno projektu w oprogramowaniu ProSIL.

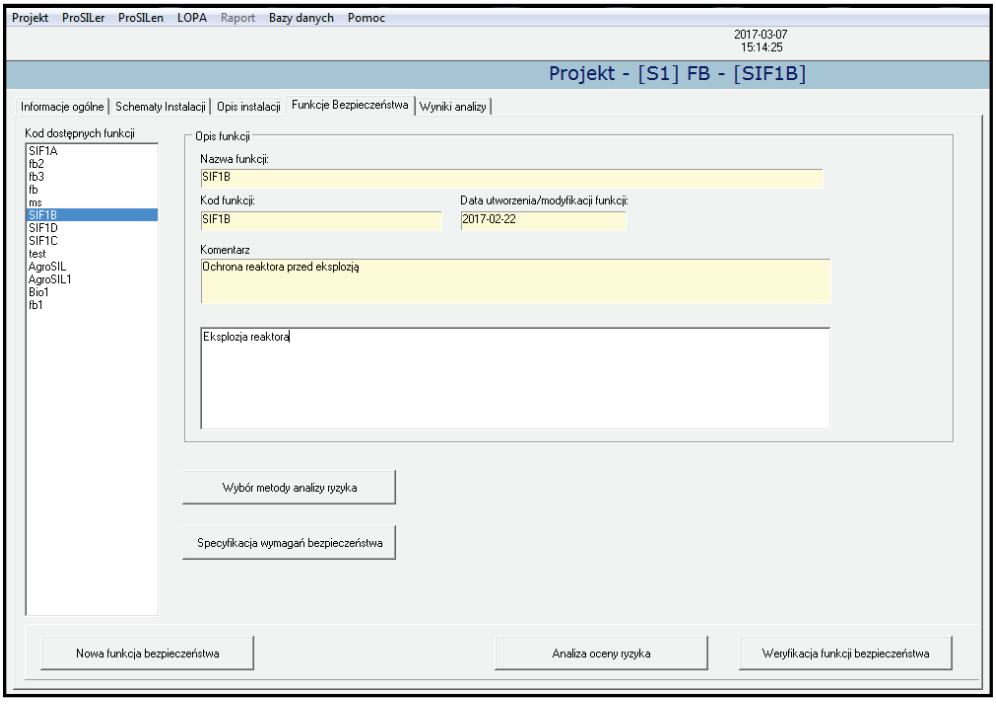


Rys. 8.2. Okno główne aplikacji ProSIL

Z okna głównego projektu użytkownik ma wgląd do informacji ogólnych dotyczących projektu oraz opisu instalacji, dla której projektowane są funkcje bezpieczeństwa, jak również schematów aktualnie opracowywanych instalacji (rys. 8.3).



Rys. 8.3. Schemat przykładowej instalacji



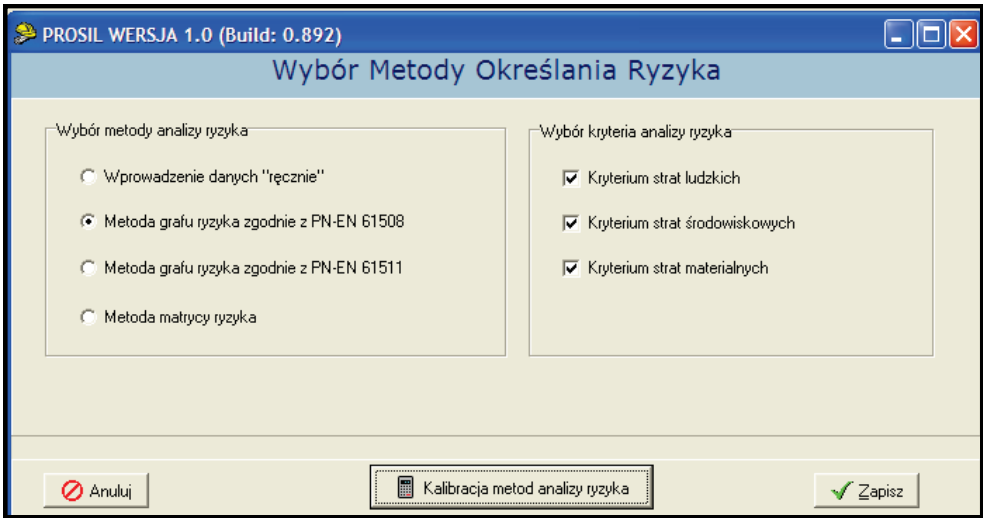
Rys. 8.4. Definiowanie funkcji bezpieczeństwa w aplikacji ProSIL (ProSIL-EAL)

Oprogramowanie ProSIL umożliwia wprowadzenie zbioru funkcji bezpieczeństwa zidentyfikowanych wcześniej, na etapie analizy zagrożeń (rys. 8.4). Każda analiza bezpieczeństwa funkcjonalnego dostępna w aplikacji ProSIL jest przeprowadzana dla odrębnych, zdefiniowanych w projekcie funkcji bezpieczeństwa z osobna. Dotyczy to zarówno procesu określania wymagań SIL, jak i weryfikacji ich poziomu.

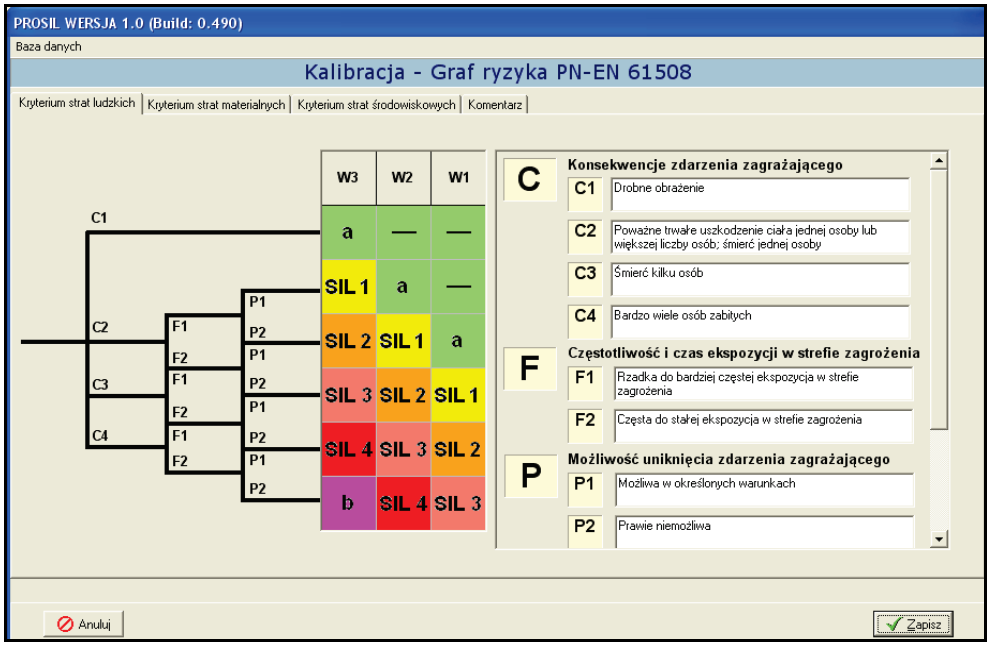
Ponieważ oprogramowanie ProSIL nie ma modułu wspomagającego analizę zagrożeń HAZOP, umożliwiono załączenie do programu wyników takiej analizy w postaci dokumentów tekstowych (będących jednocześnie załącznikami do dokumentacji określania wymaganego poziomu SIL).

8.3.2. Moduł określania wymaganego poziomu SIL

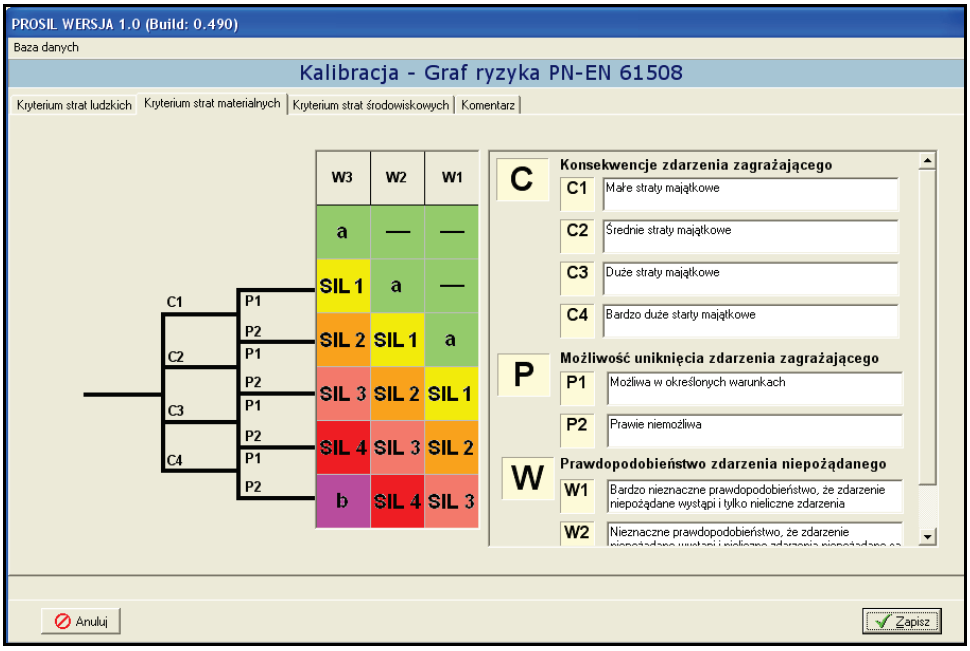
Moduł określania wymaganego poziomu SIL składa się z dwóch powiązanych ze sobą części funkcjonalnych. Pierwszą z nich jest moduł kalibracji wybranej metody oceny ryzyka. Zgodnie z założeniami funkcjonalnymi aplikacji kalibracja taka dokonywana jest jednokrotnie dla projektu zapisanego w ProSIL. Polega ona na wyborze jednej spośród kilku dostępnych w aplikacji metod, a następnie zdefiniowaniu części tabelarycznej metody i określeniu parametrów ryzyka oraz ich przedziałów kryterialnych. W przypadku metody grafu ryzyka jest to część tabelaryczna grafu oraz cztery parametry ryzyka: C, P, F oraz W. Definicja części tabelarycznej polega na wyborze jednego z siedmiu dostępnych poziomów redukcji ryzyka, powiązanych z czterema poziomami SIL, przy braku wymagań lub wymagań szczegółowych. Okno wyboru metody przedstawiono na rys. 8.5, natomiast okna zasadnicze kalibracji wybranej metody – na rys. 8.6, 8.7 oraz 8.8.



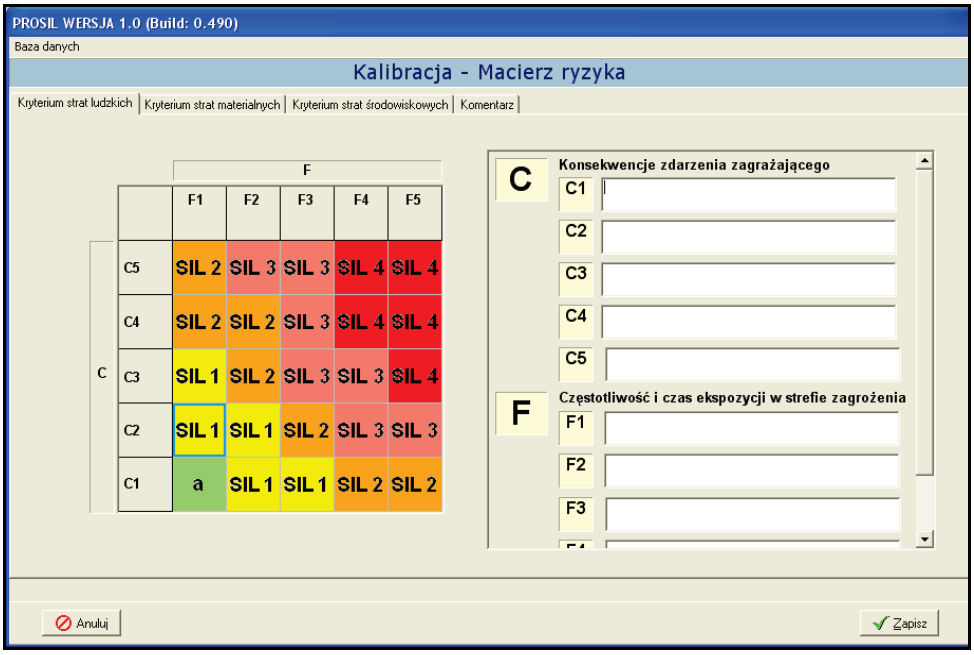
Rys. 8.5. Wybór metody określania wymaganego poziomu SIL



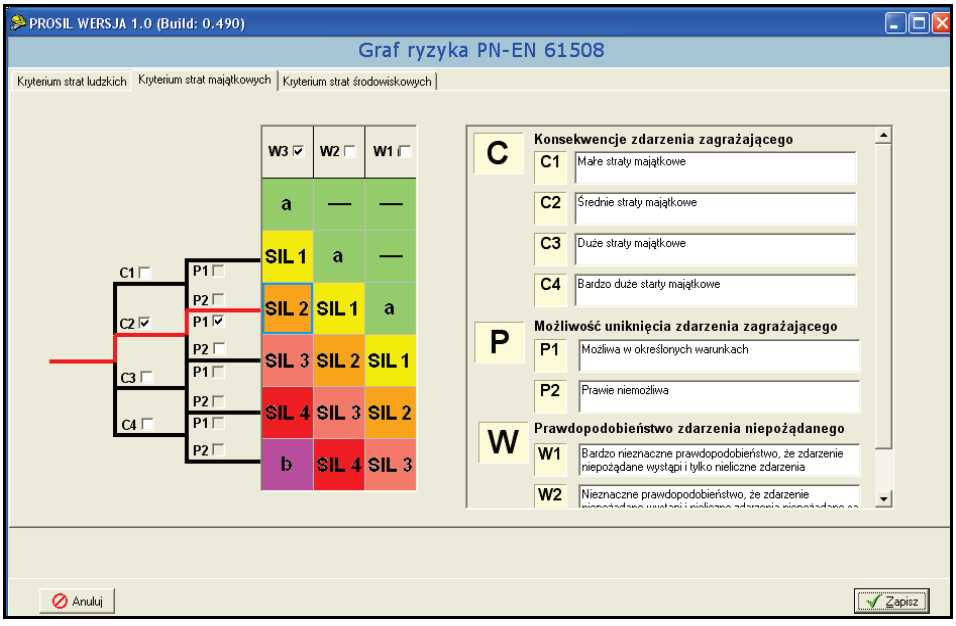
Rys. 8.6. Kalibracja metody grafu ryzyka PN-EN 61508 według kryterium strat ludzkich



Rys. 8.7. Kalibracja metody grafu ryzyka PN-EN 61508 według kryterium strat materialnych



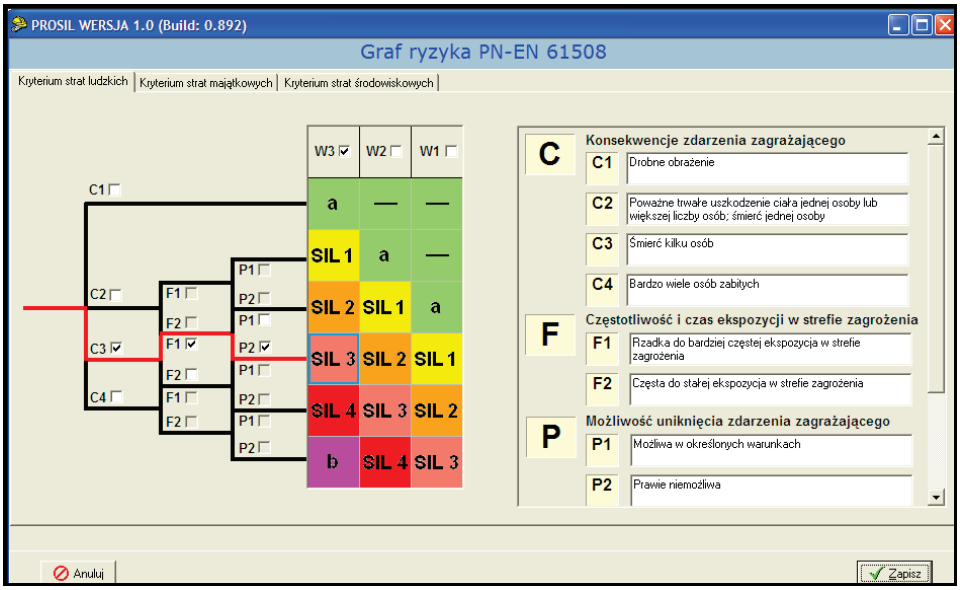
Rys. 8.8. Kalibracja metody macierzy ryzyka PN-EN 61511 według kryterium strat ludzkich



Rys. 8.9. Określanie wymaganego poziomu SIL na podstawie grafu ryzyka wg PN-EN 61508 dla kryterium strat majątkowych

Druga część modułu określania wymaganego poziomu SIL wiąże się z wykorzystaniem wybranej i skalibrowanej metody. Przy kalibracji określa się, względem których kry-

teriów strat zostanie wykonana analiza (patrz rys. 8.5). Determinuje to możliwości wykorzystania tych kryteriów w procesie oceny ryzyka. Z oceny tej dla każdego kryterium otrzymuje się wymagany poziom nienaruszalności bezpieczeństwa SIL. Jeżeli wybrano więcej niż jedno kryterium analizy, program wybiera najbardziej restrykcyjną (maksymalną) wartość SIL jako tę, która ma obowiązywać dla analizowanej funkcji bezpieczeństwa. Na rys. 8.9 i 8.10 przedstawiono przykładowe okna modułu oceny ryzyka – określania wymaganego poziomu SIL.

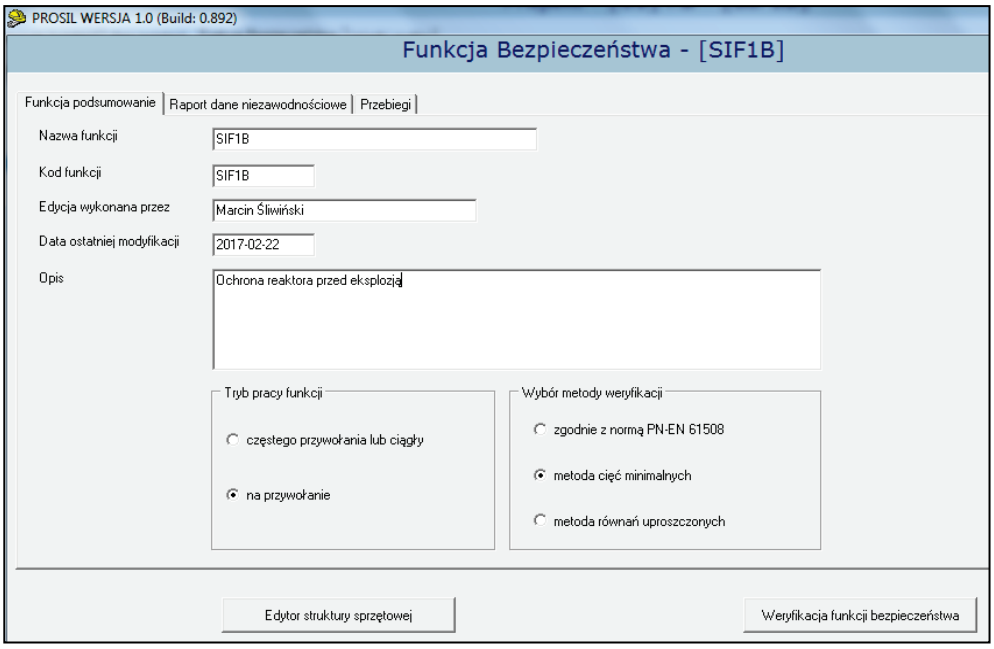


Rys. 8.10. Określanie wymaganego poziomu SIL na podstawie grafu ryzyka wg PN-EN 61508 dla kryterium strat ludzkich

Zakładając, że procesy oceny ryzyka i określenia wymagań SIL dla wybranej, przykładowej funkcji bezpieczeństwa, oznaczonej jako „Ochrona reaktora przed eksplozją", zostały przeprowadzone z wykorzystaniem skalibrowanego grafu ryzyka dla dwóch wybranych kryteriów strat: majątkowych oraz ludzkich, otrzymano dwie wynikowe wartości wymaganego poziomu nienaruszalności bezpieczeństwa: SIL2 i SIL3. W takiej sytuacji, zgodnie z zasadą opisaną niniejszej monografii, należy wybrać wartość SIL3 jako wymaganą dla systemu E/E/PE, który będzie realizował rozpatrywaną funkcję bezpieczeństwa.

8.3.3. Moduł weryfikacji wymaganego poziomu SIL

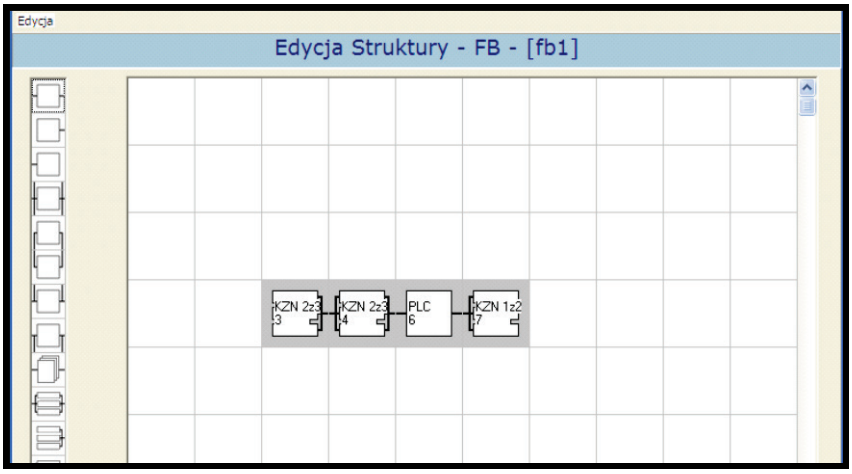
Oprogramowanie ProSIL pozwala na zamodelowanie systemu E/E/PE, realizującego wybrane funkcje bezpieczeństwa, o dowolnej konfiguracji sprzętowej. Podsystemy mogą mieć strukturę „*k* z *n*" i mogą się składać z różnych elementów. Na rys. 8.11 przedstawiono okno główne modułu weryfikacji SIL (ProSILer).



Rys. 8.11. Okno główne modułu wspomagającego weryfikację SIL

W oknie głównym modułu weryfikacji SIL aplikacji ProSIL należy wprowadzić nazwę funkcji bezpieczeństwa realizowanej przez warstwę SIS, kod funkcji, dane osoby odpowiedzialnej za wprowadzenie modelu struktury sprzętowej funkcji bezpieczeństwa oraz datę ostatniej modyfikacji. Dodatkowo można wprowadzić szerszy opis projektowanej funkcji bezpieczeństwa. Następnie należy wybrać tryb pracy systemu realizującego funkcję bezpieczeństwa, tj. „częstego przywołania lub ciągły" albo „na przywołanie". Projektant ma do wyboru trzy metody weryfikacji SIL [196, 197, 198]:
— zgodnie z normą PN-EN 61508;
— metoda cięć minimalnych;
— metoda równań uproszczonych.

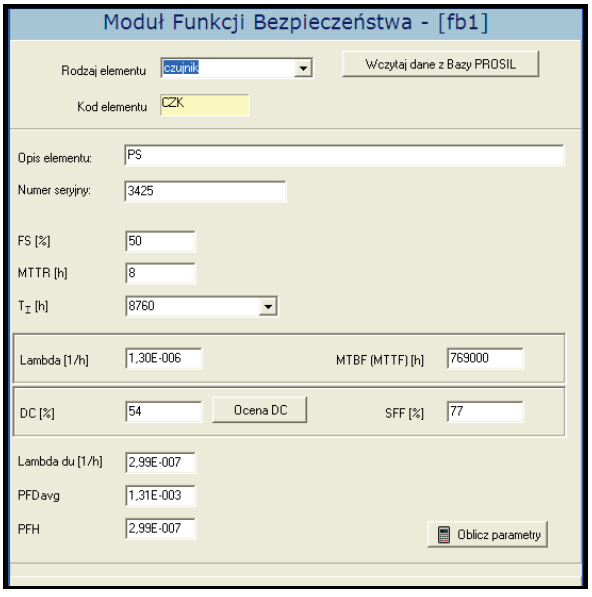
Po odznaczeniu w odpowiednim polu okna głównego wybiera się rodzaj metody, według której będzie pracował algorytm obliczeniowy. W następnym kroku należy przejść do okna projektowego struktury sprzętowej funkcji bezpieczeństwa, wybierając przycisk „Edytor struktury sprzętowej" (rys. 8.12). Projektowana funkcja bezpieczeństwa jest przedstawiona w postaci schematów blokowych dla struktury sprzętowej z wyraźnym podziałem na części podsystemów: pomiarowych (czujniki, detektory), przetwarzania danych (sterowniki PLC lub ESD wraz z modułami wejść/ wyjść, CPU, separatorami i modułami komunikacyjnymi) oraz wykonawczych.



Rys. 8.12. Edytor graficzny struktury warstwy sprzętowej funkcji bezpieczeństwa

Projektant ma do dyspozycji szereg modułów i elementów, które musi wprowadzić do okna projektowego. Po wprowadzeniu należy dokonać testu połączeń bloków, wybierając przycisk „Test struktury".

Na rys. 8.13 przedstawiono edytor graficzny pojedynczego elementu struktury sprzętowej funkcji bezpieczeństwa.

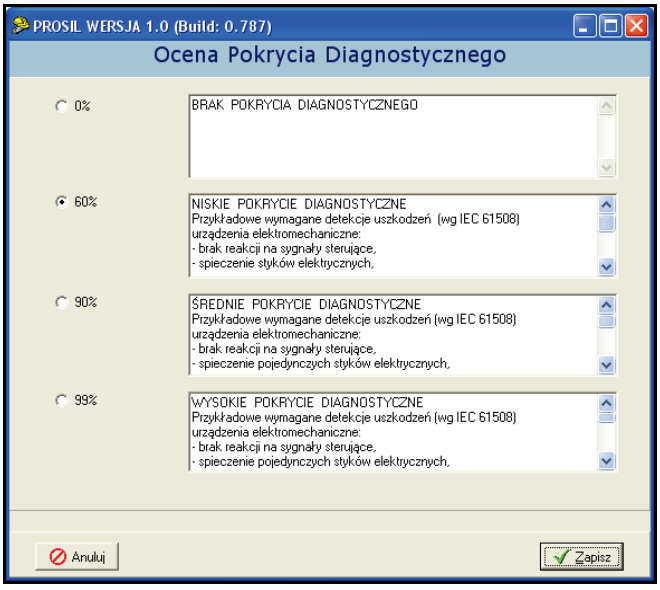


Rys. 8.13. Dane niezawodnościowe pojedynczego elementu systemu SIS

Dane niezawodnościowe dla pojedynczego elementu funkcji bezpieczeństwa, np. czujnika temperatury, mogą być wprowadzane do systemu ręcznie przez projektanta lub poprzez automatycznie bazy danych ProSILcdb [65, 67, 69, 70]. Użytkownik posiadający dokładne dane odnośnie do wartości pokrycia diagnostycznego ma możliwość jej bezpo-

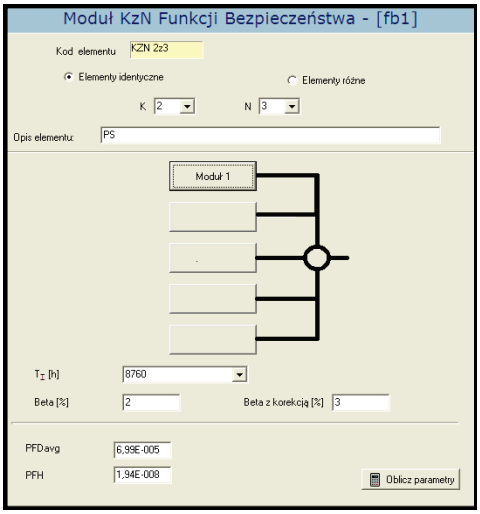
średniego wpisania w odpowiednie pole oznaczone symbolem „*DC* [%]”. W przypadku, gdy użytkownik nie ma takich danych i potrzebuje dodatkowych informacji, program ProSIL umożliwia otwarcie następnego okna dialogowego poprzez kliknięcie w przycisk „Ocena *DC*” (rys. 8.14).

Okno „Ocena pokrycia diagnostycznego” pozwala na przedziałowe określenie pokrycia diagnostycznego na podstawie znajomości właściwości analizowanego podsystemu realizującego daną funkcję bezpieczeństwa. Ocena *DC* polega na wyborze odpowiedniego przedziału zakresu: 0% – brak pokrycia diagnostycznego, 60% – niskie pokrycie diagnostyczne, 90% – średnie pokrycie diagnostyczne oraz 99% – wysokie pokrycie diagnostyczne. Użytkownik wybiera jeden z czterech przedziałów na podstawie przeanalizowania możliwości przeprowadzenia testów diagnostycznych, które przykładowo są podane przy każdej wybranej procentowej wartości *DC*. Zaznaczenie odpowiedniego przedziału wartości *DC* oraz zatwierdzenie przyciskiem „Zapisz” wprowadza wybrane oszacowanie *DC* w kontekście analizowanej funkcji bezpieczeństwa. Przy *DC* = 0% program nie podaje przykładowych testów. Przy niskim pokryciu diagnostycznym użytkownik ma dostępną pomoc w postaci listy przykładowych uszkodzeń, które mogą być wystarczające do uzyskania *DC* = 60%, 90% lub 99%. W oknie dialogowym zastosowano podział całego podsystemu realizującego funkcje bezpieczeństwa na elementy pomiarowe, wykonawcze oraz na sprzęt cyfrowy.



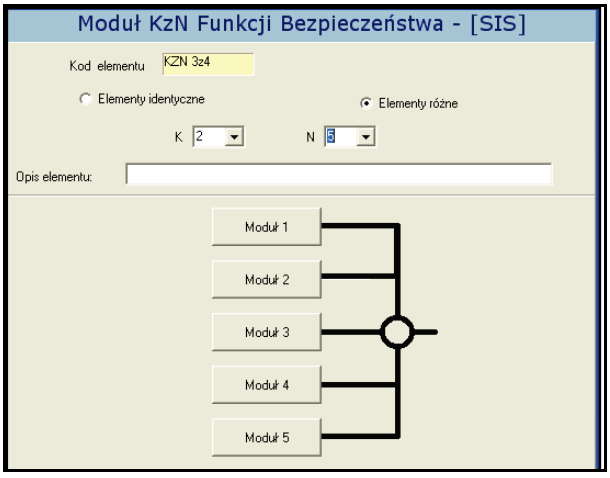
Rys. 8.14. Okno dialogowe modułu oszacowania pokrycia diagnostycznego DC

Przy edycji struktury sprzętowej w oknie RBD (rys. 8.12) istnieje możliwość kliknięcia prawym klawiszem myszy na symbol graficzny wprowadzonych struktur. W przypadku struktury „*k* z *n*” pojawia się okno przedstawione na rys. 8.15.



Rys. 8.15. Moduł weryfikacji SIL – struktura „*k* z *n*”, identyczne elementy

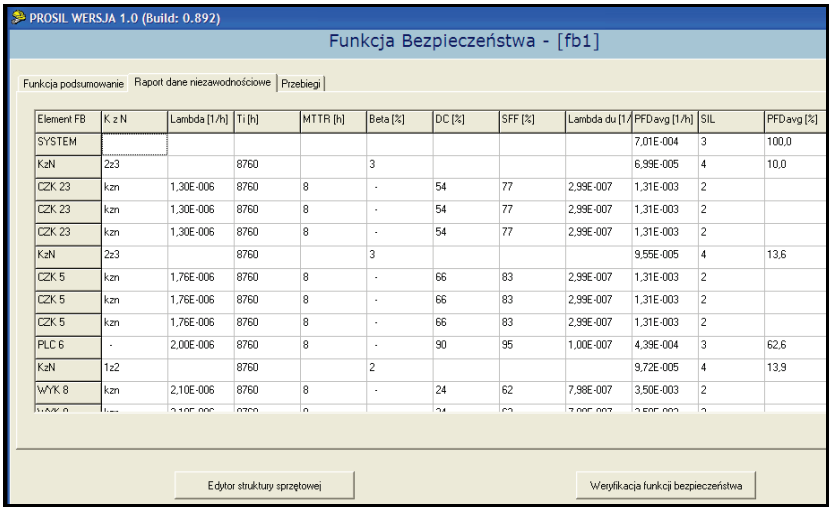
W modelowanym systemie struktura „*k* z *n*” ma wyższy poziom w hierarchii od pojedynczego elementu. Może ona zawierać jednakowe elementy o określonym modelu probabilistycznym. Może się ona składać także z różnych elementów, choć sytuacja ta nie jest możliwa w przypadku wyboru metody opartej na normie PN-EN 61508. Na rys. 8.16 pokazano okno edycji modułu „*k* z *n*” dla różnych elementów (2 z 5).



Rys. 8.16. Moduł weryfikacji SIL – struktura *k* z *n*, różne elementy

Poszczególne elementy (zawory, pompy, czujniki, siłowniki, moduły wejść/ wyjść, procesory), z których składają się podsystemy (część pomiarowa, układ przetwarzania danych, część wykonawcza) stanowiące cały system (układ zabezpieczeniowy układ sterowania), są ze sobą połączone za pomocą punktów węzłowych. Przebieg sygnału następuje od wejścia do wyjścia. Po wprowadzeniu danych niezawodnościowych i przetestowaniu poprawności połączeń struktury sprzętowej należy uruchomić algorytm obliczeniowy,

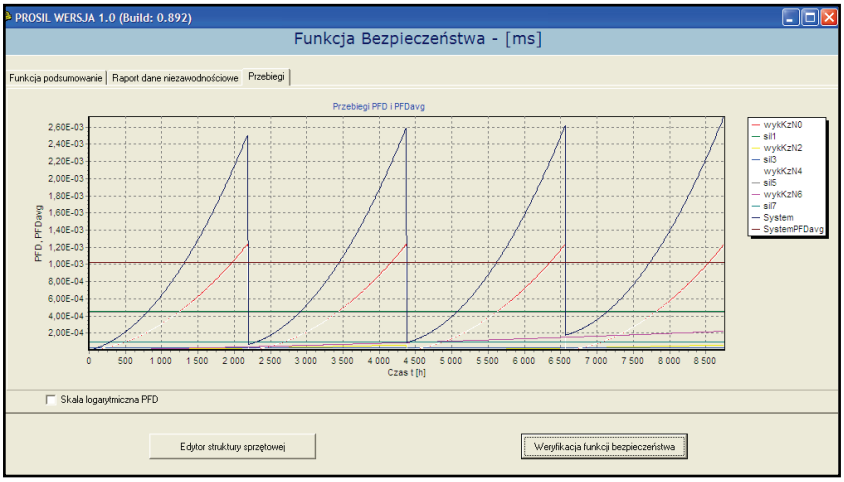
naciskając w oknie głównym modułu weryfikacji SIL przycisk „Weryfikacja funkcji bezpieczeństwa”. Po uruchomieniu weryfikacji pojawia się tablica raportu z weryfikacji SIL w aplikacji ProSIL (osobno dla trybu pracy „częstego przywołania lub ciągłej” i dla trybu „na przywołanie”) (rys. 8.17).



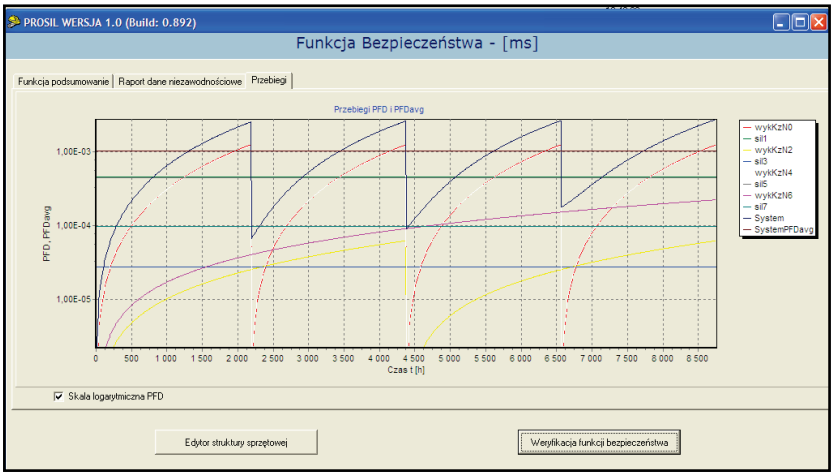
Element FB	K z N	Lambda [1/h]	Ti [h]	MTTR [h]	Beta [%]	DC [%]	SFF [%]	Lambda du [1/	PFDavg [1/h]	SIL	PFDavg [%]
SYSTEM									7,01E-004	3	100,0
KzN	2z3		8760		3				6,99E-005	4	10,0
CZK 23	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
CZK 23	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
CZK 23	kzn	1,30E-006	8760	8	-	54	77	2,99E-007	1,31E-003	2	
KzN	2z3		8760		3				9,55E-005	4	13,6
CZK 5	kzn	1,76E-006	8760	8	-	66	83	2,99E-007	1,31E-003	2	
CZK 5	kzn	1,76E-006	8760	8	-	66	83	2,99E-007	1,31E-003	2	
CZK 5	kzn	1,76E-006	8760	8	-	66	83	2,99E-007	1,31E-003	2	
PLC 6	-	2,00E-006	8760	8	-	90	95	1,00E-007	4,39E-004	3	62,6
KzN	1z2		8760		2				9,72E-005	4	13,9
WYK 8	kzn	2,10E-006	8760	8	-	24	62	7,98E-007	3,50E-003	2	

Rys. 8.17. Okno raportu weryfikacji SIL

Po dokonaniu weryfikacji zostają wyznaczone wartości $PFD(t)$, PFD_{avg}, PFH dla wszystkich elementów systemu (czujniki, zawory, moduły wejść/ wyjść, układy CPU), podsystemów i systemu. Wartości te są przedstawione w postaci raportu – w pliku tekstowym (zawierającym wynikowe dane oraz schemat analizowanej struktury). Na rys. 8.18 przedstawiono okno do wyznaczania i graficznej reprezentacji przebiegu prawdopodobieństwa niewypełnienia funkcji bezpieczeństwa na przywołanie $PFD(t)$, PFD_{avg} natomiast rys. 8.19 pokazuje te same przebiegi w skali logarytmicznej.

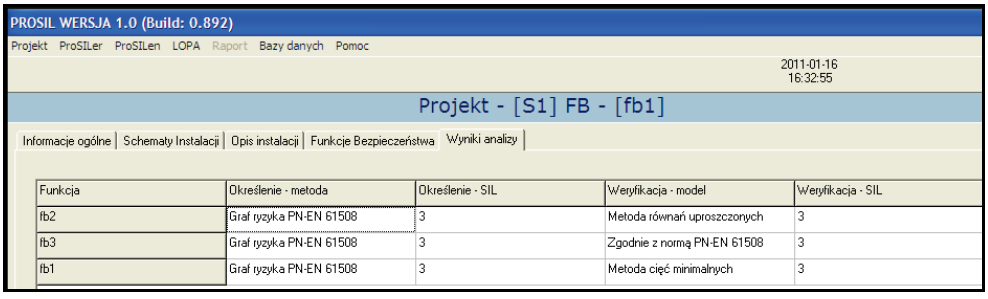


Rys. 8.18. Reprezentacja graficzna przebiegów $PFD(t)$, PFD_{avg}



Rys. 8.19. Reprezentacja graficzna przebiegów $PFD(t)$, PFD_{avg} w skali logarytmicznej

Na rys. 8.20 przedstawiono zbiorcze wyniki dla wszystkich funkcji bezpieczeństwa uwzględnionych w projekcie.



Funkcja	Określenie - metoda	Określenie - SIL	Weryfikacja - model	Weryfikacja - SIL
fb2	Graf ryzyka PN-EN 61508	3	Metoda równań uproszczonych	3
fb3	Graf ryzyka PN-EN 61508	3	Zgodnie z normą PN-EN 61508	3
fb1	Graf ryzyka PN-EN 61508	3	Metoda cięć minimalnych	3

Rys. 8.20. Zbiorcze wyniki analiz bezpieczeństwa funkcjonalnego dla funkcji bezpieczeństwa uwzględnionych w projekcie (z wykorzystaniem różnych metod)

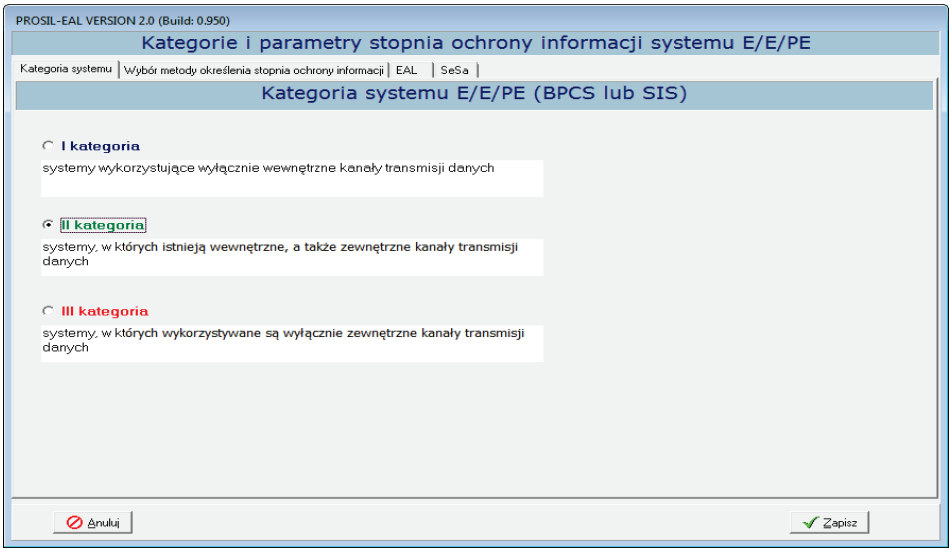
8.4. Aplikacja ProSIL-EAL

Aplikacja ProSIL-EAL została zaprojektowana w celu umożliwienia komputerowego wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym w cyklu życia systemów technicznych. Ogólne założenia projektowe tej aplikacji obejmują wspomaganie procesu projektowania systemów E/E/PE, BPCS i SIS zgodnie wymaganiami i kryteriami norm PN-EN 61508 i PN-EN 61511. Program ProSIL-EAL umożliwia wyznaczanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL na podstawie wymagań instytucji nadzorującej dla wyróżnionych funkcji bezpieczeństwa. ProSIL-EAL wyposażony jest także w moduł wspomagający komputerową weryfikację poziomu nienaruszalności bezpieczeństwa SIL dla rozważanych architektur sprzętu poszczególnych funkcji bezpieczeństwa. Zapewnia również wspomaganie w ocenie rozwiązań technicznych i organizacyjnych oraz wpływu błędów systematycznych oprogramowania i błędów człowieka podczas eksploatacji systemów E/E/PE, BPCS i SIS.

W aplikacji ProSIL-EAL (która stanowi rozbudowaną wersję programu ProSIL) uwzględniono możliwość rozpatrzenia zagadnień związanych z ochroną informacji w przemysłowych skomputeryzowanych rozproszonych systemach sterowania i zabezpieczeń w zarządzaniu bezpieczeństwem funkcjonalnym, na bazie metodyki zaproponowanej w niniejszej monografii.

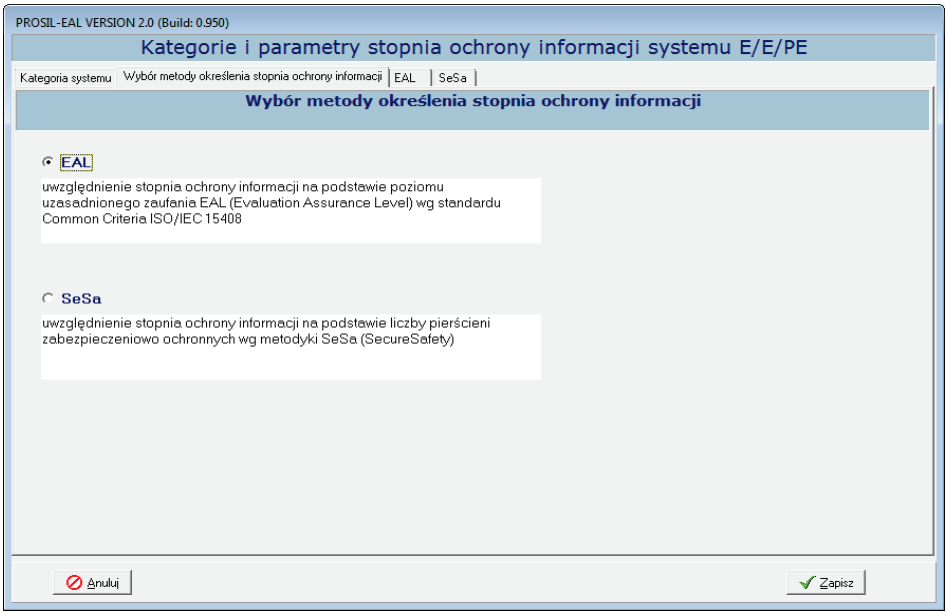
Każda analiza bezpieczeństwa funkcjonalnego dostępna w aplikacji ProSIL-EAL jest przeprowadzana odrębnie dla każdej ze zdefiniowanych w projekcie funkcji bezpieczeństwa. Dotyczy to zarówno procesu określania wymagań SIL, jak i weryfikacji ich poziomu.

Analizując wybrany system techniczny, określa się wymagane funkcje bezpieczeństwa, niezbędne do zapewnienia należytego poziomu ryzyka związanego z pracą takiego systemu. W aplikacji ProSIL-EAL przy wyborze opcji dotyczącej uwzględnienia czynników ochrony informacji należy określić, jaki typ systemu jest analizowany. Zgodnie z opisem kategorii systemów należy podjąć decyzję o stopniu rozproszenia takiego systemu, co będzie wpływać na kolejne etapy przeprowadzanej analizy. Okno wyboru typu systemu przedstawiono na rys. 8.21. Na kolejnych rysunkach pokazano okna związane z określaniem i weryfikacją poziomów SIL w aplikacji ProSIL-EAL, uwzględniające zagadnienia ochrony informacji. W obu przypadkach – według przedstawionej powyżej metodyki – pierwszą czynnością w analizie musi być określenie kategorii systemu (rys. 8.21).

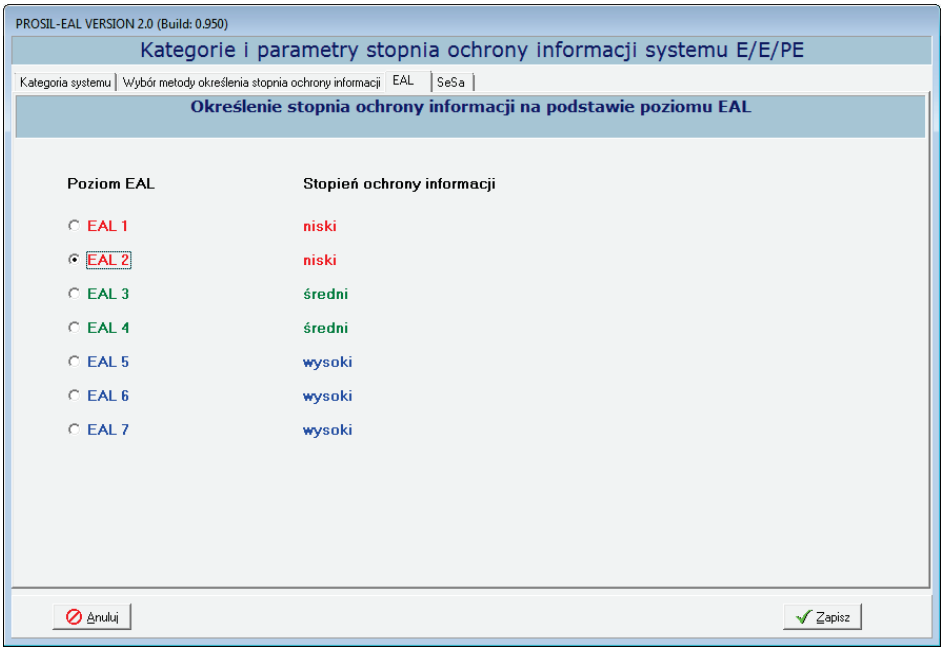


Rys. 8.21. Okno wyboru kategorii systemu E/E/PE (BPCS lub SIS) w aplikacji ProSIL-EAL

Następnym krokiem po wyborze kategorii systemu jest wybór metody określenia stopnia ochrony informacji przypisanej do analizowanego systemu – BPCS w przypadku określania wymagań, SIS w przypadku weryfikacji. Program ProSIL-EAL umożliwia wybór jednej z dwóch metod – na podstawie poziomów uzasadnionego zaufania EAL (rys. 8.22, 8.23).

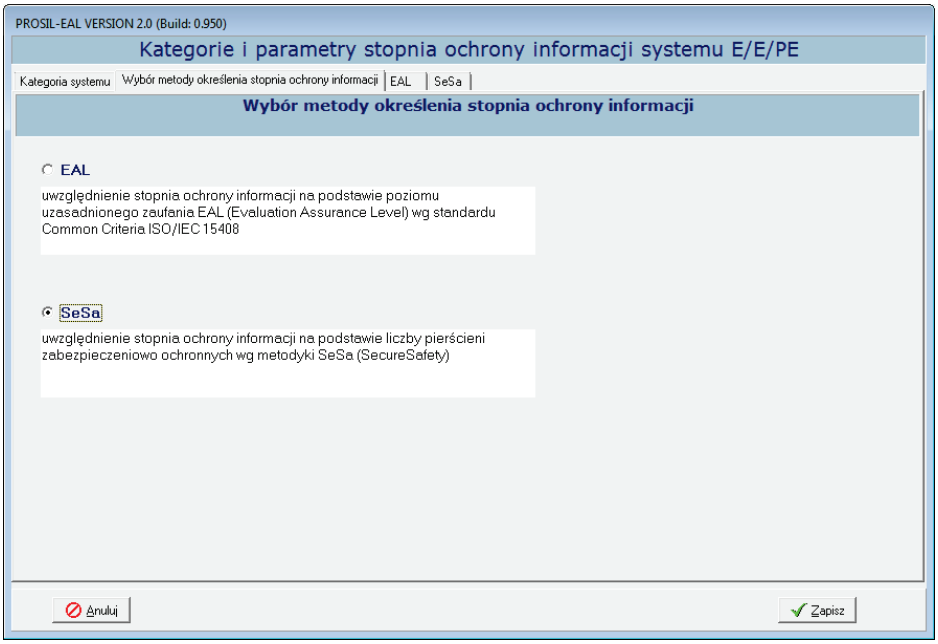


Rys 8.22. Okno wyboru metody określenia stopnia ochrony informacji w aplikacji ProSIL-EAL na potrzeby analiz bezpieczeństwa funkcjonalnego – EAL

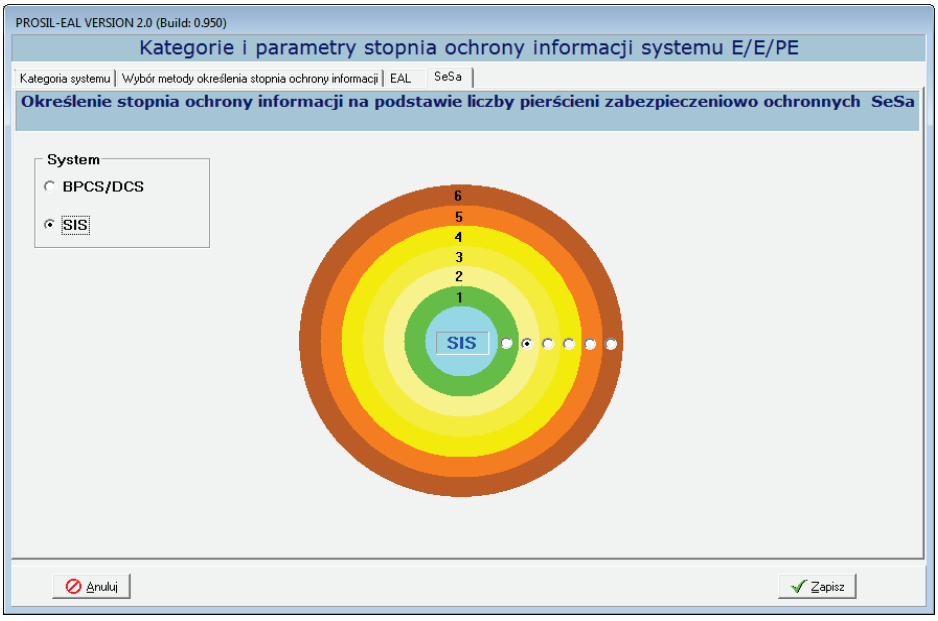


Rys. 8.23. Okno określenia stopnia ochrony informacji w aplikacji ProSIL-EAL wg *Common Criteria* ISO/IEC 15408

Drugą metodę stanowi określenie stopnia ochrony informacji na podstawie liczby pierścieni zabezpieczeniowo-ochronnych, bazujące na metodologii SeSa (rys. 8.24, 8.25).

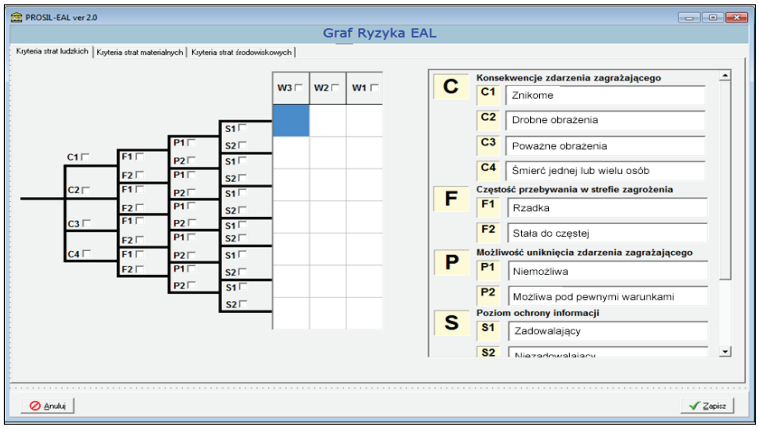


Rys 8.24. Okno wyboru metody określenia stopnia ochrony informacji w aplikacji ProSIL-EAL na potrzeby analiz bezpieczeństwa funkcjonalnego wg metodyki SeSa, SINTEF



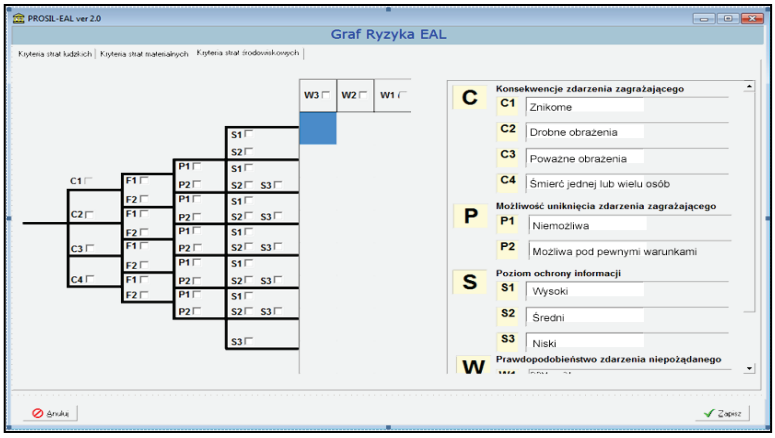
Rys. 8.25. Okno określenia stopnia ochrony informacji w aplikacji ProSIL-EAL wg metodyki SeSa, SINTEF – liczba pierścieni zabezpieczeniowo-ochronnych

Na rys. 8.26 przedstawiono graf ryzyka uwzględniający czynnik ochrony informacji dla systemu I lub II kategorii.

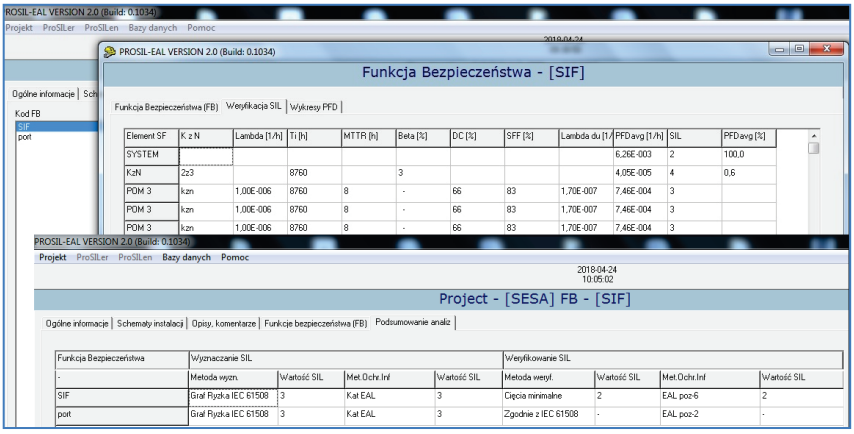


Rys. 8.26. Czynnik ochrony informacji w grafie ryzyka dla systemów I i II kategorii

Z kolei na rys. 8.27 przedstawiono graf ryzyka zbudowany dla systemu III kategorii.



Rys. 8.27. Czynnik ochrony informacji w grafie ryzyka dla systemów III kategorii



Rys. 8.28. Okno raportu weryfikacji SIL w aplikacji ProSIL-EAL

Na rys. 8.28 zaprezentowano raport wynikowy z modułu weryfikacji SIL w aplikacji ProSIL-EAL z uwzględnieniem aspektów ochrony informacji.

8.5. Podsumowanie

W niniejszym rozdziale omówiono komputerowy proces wspomagania zarządzania bezpieczeństwem funkcjonalnym przy wykorzystaniu oprogramowania ProSIL. Narzędzie to zawiera odpowiednie moduły i bazy danych do prowadzenia projektów analizy bezpieczeństwa funkcjonalnego dla danego obiektu złożonego lub instalacji procesowej. Aplikacja ProSIL pozwala na definiowanie zbioru funkcji bezpieczeństwa w ramach danego projektu (konkretny obiekt złożony lub instalacja w projektowaniu lub eksploatacji). Wyznaczanie wymaganego poziomu nienaruszalności bezpieczeństwa SIL dla wybranej funkcji bezpieczeństwa odbywa się za pomocą modułów: grafu ryzyka lub matrycy ryzyka z odpowiednimi interfejsami graficznymi. W aplikacji istnieje biblioteka grafów ryzyka z możliwością definiowania i modyfikowania parametrów związanych z ryzykiem.

Moduł ProSILen, zaproponowany do określania wymaganego poziomu nienaruszalności bezpieczeństwa dla wybranych funkcji bezpieczeństwa, ma za zadanie wspomagać proces przeprowadzania analiz funkcji związanych z bezpieczeństwem oraz jednocześnie umożliwiać szybki i łatwy dostęp do wszystkich informacji na ich temat. Poprzez umożliwienie wyboru jednej z dostępnych metod służących do przeprowadzania oceny ryzyka – między innymi autorskiego rozwiązania modyfikowalnych grafów ryzyka – aplikacja ProSIL-EAL jest uniwersalnym narzędziem wspomagającym osoby odpowiedzialne za kształtowanie poziomu bezpieczeństwa w systemach podwyższonego ryzyka. Jednocześnie moduł został wzbogacony o możliwość integrowania analizy bezpieczeństwa funkcjonalnego z analizą ochrony informacji obiektu technicznego.

W procesie weryfikacji architekturę sprzętu realizującego funkcję bezpieczeństwa przedstawia się za pomocą schematów blokowych z wyróżnieniem podsystemów i elementów. W aplikacji ProSIL dostępna jest baza danych niezawodnościowych i innych parametrów modeli probabilistycznych wyróżnionych kategorii elementów (lub podsystemów) z możliwością jej aktualizacji. Modelowanie probabilistyczne systemów przeprowadza się na podstawie modeli probabilistycznych podsystemów traktowanych ogólnie jako systemy „*k* z *n*" składające się z jednakowych i z różnych elementów. Oprogramowanie ProSIL zawiera bibliotekę modeli probabilistycznych podsystemów zgodnie z PN-EN 61508 oraz modeli w wersji rozszerzonej, wyznaczonych metodami cięć minimalnych (uzyskanych np. na podstawie metody schematów blokowych RBD lub drzew niezdatności FT) i grafów Markowa [6, 76, 126, 196, 197].

Oprogramowanie to umożliwia także optymalizowanie czasów testowania elementów (lub podsystemów) w systemie E/E/PE lub SIS. Moduł weryfikacji SIL pozwala na wyznaczenie i graficzną reprezentację przebiegu w czasie prawdopodobieństwa niezadziałania na przywołanie $PFD(t)$ oraz obliczenie przeciętnego prawdopodobieństwa PFD_{avg} podsystemów i systemów E/E/PE i SIS dla rodzaju pracy. W programie ProSIL warstwy zabezpieczeń są analizowane w nawiązaniu do metodyki LOPA oraz wymagań zawartych w normie PN-EN 61511 [2, 72, 75, 83, 162]. Wybór kategorii systemów oraz poziomu ochrony informacji w systemie SIS umożliwia rozszerzenie procesu weryfikacji SIL o aspekty związane z cyberzagrożeniami.

Rozdział 9

PODSUMOWANIE

W niniejszej monografii przedstawiono metody analizy bezpieczeństwa funkcjonalnego uwzględniające zagadnienia ochrony informacji. Zaproponowana metodyka integracji zagadnień bezpieczeństwa funkcjonalnego i ochrony informacji uwzględnia klasyfikację systemów rozproszonych na kategorie. Należy rozróżnić dwie fazy analiz: związane z określaniem wymaganego poziomu SIL oraz z jego weryfikacją.

W odniesieniu do pierwszej fazy zaproponowano podejście, w którym aspekty ochrony informacji są rozpatrywane jako jeden z czynników mających wpływ na ryzyko związane z funkcjonowaniem obiektu technicznego. Czynnik taki jest następnie wykorzystywany w ocenach ryzyka powiązanych z analizą bezpieczeństwa funkcjonalnego obiektów technicznych, zarówno w metodach półilościowych, jak i w metodzie modyfikowalnego grafu ryzyka, który umożliwia implementację tej metody w praktyce.

Przy weryfikacji SIL zaproponowano trzy podejścia w zakresie uwzględnienia zagadnień ochrony informacji. Pierwsze bazuje na tablicy porównawczej poziomów SIL i EAL. Poziomy EAL dotyczą zdecydowanej większości pojedynczych rozwiązań technicznych (urządzeń, aplikacji komputerowych itp.), nie zaś podsystemów czy też całych systemów. W związku z tym należy poważnie rozważyć stosowność korzystania z miar EAL na rzecz podejść bardziej ogólnych, będących urzeczywistnieniem realnego poziomu bezpieczeństwa związanego z ochroną informacji, a w istocie poziomu związanego z nią ryzyka. Drugie podejście opiera się na uwzględnieni w procesie weryfikacji SIL poziomów uzasadnionej ochrony SAL. Trzecie rozwiązanie uwzględnia liczbę pierścieni zabezpieczeniowo-ochronnych na podstawie metodyki SeSa, którą wskazano jako alternatywne podejście umożliwiające określenie stopnia poziomu ochrony informacji, poprzez zliczanie pierścieni zabezpieczeniowo-ochronnych w proponowanej metodzie weryfikacji SIL.

Zaproponowane metody określania wymagań dotyczących poziomów nienaruszalności bezpieczeństwa SIL oraz ich weryfikacji z uwzględnieniem zagadnień ochrony informacji zostały zaimplementowane w prototypowym oprogramowaniu wspomagającym proces zarządzania bezpieczeństwem funkcjonalnym ProSIL-EAL, odpowiednio w modułach określania wymagań ProSILen, jak również w module weryfikacji ProSILer.

Metodyka zintegrowanego zarządzania bezpieczeństwem funkcjonalnym, uwzględniająca czynniki ochrony informacji, będzie sprzyjać wprowadzaniu nowej jakości w projektowaniu i użytkowaniu rozwiązań do realizacji funkcji związanych z bezpieczeństwem na różnych wymaganych poziomach nienaruszalności bezpieczeństwa SIL, czego nie uwzględniają w wystarczającym stopniu aktualne normy bezpieczeństwa funkcjonalnego.

Kluczowym zagadnieniem do uwzględnienia w zarządzaniu bezpieczeństwem obiektów oraz systemów infrastruktury krytycznej jest uwzględnianie zasad dobrej praktyki, dyrektyw, rozporządzeń, wytycznych, zaleceń, norm i kryteriów związanych z utrzymywaniem marginesów bezpieczeństwa w procesie projektowania i eksploatacji aż do likwidacji. Zaproponowano podejście do zarządzania bezpieczeństwem funkcjonalnym w systemach technicznych, ze szczególnym uwzględnieniem przemysłu procesowego, głównie zakładów dużego ryzyka i zakładów zwiększonego ryzyka. Trzon tej propozycji metodycznej stanowią normy bezpieczeństwa funkcjonalnego z odpowiednimi wymaganiami i kryteriami oraz

propozycjami metodycznymi dotyczącymi wyznaczania poziomów nienaruszalności bezpieczeństwa SIL i ich weryfikacji przy wykorzystaniu metod modelowania probabilistycznego systemów i warstw zabezpieczeniowo-ochronnych.

Metody analizy i oceny ryzyka oraz modelowania probabilistycznego systemów E/E/PE, BPCS i SIS oraz warstw zabezpieczeniowo-ochronnych o rozważanych na etapie projektu architekturach umożliwiają analizowanie tych systemów przy użyciu prototypowej aplikacji komputerowej ProSIL lub jej wersji rozszerzonej ProSIL-EAL.

Norma PN-EN 61508 wprowadza wymagania dotyczące tzw. białych i czarnych kanałów komunikacyjnych w ramach systemów E/E/PE (BPCS lub SIS), realizujących określone funkcje związane z bezpieczeństwem. Zasadne jest więc przeprowadzanie zintegrowanej analizy wiążącej aspekty bezpieczeństwa i ochrony informacji w przemysłowej sieci komputerowej w odniesieniu do norm międzynarodowych PN-ISO/IEC 17779, PN-ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 15408 oraz innych norm dotyczących protokołów komunikacji i niezawodności transmisji danych w przemysłowych sieciach komputerowych. Analiza ta powinna być włączona w proces zarządzania bezpieczeństwem funkcjonalnym w cyklu życia, opisany w części 1 i 2 normy PN-EN 61508.

W niniejszej monografii zaproponowano ogólne podejście do integrowania analizy bezpieczeństwa funkcjonalnego z analizą ochrony informacji w przemysłowych sieciach komputerowych w ramach nadrzędnego systemu zarządzania bezpieczeństwem.

Jedną z tendencji rozwojowych współczesnych układów automatyki przemysłowej, włączając w to również systemy bezpieczeństwa, jest dążenie do decentralizacji systemów sterowania. Wynika to z wielu zalet rozproszenia elementów systemu sterowania, takich jak: zwiększenie przejrzystości struktury systemu, poprawienie niezawodności, skalowalność czy też zmniejszenie liczby przewodów. Dzięki wykorzystaniu sieci przemysłowych możliwa jest wymiana danych pomiędzy: komputerami, sterownikami, stacjami operatorskimi, a także czujnikami i elementami wykonawczymi wyposażonymi w odpowiedni interfejs sieciowy. Działanie przemysłowych sieci komputerowych opiera się na tej samej idei co działanie klasycznych sieci komputerowych. Ponieważ sieci tego typu integrują podsystemy pomiarowe, programowalne systemy elektroniczne (komputery, sterowniki programowalne PLC, specjalistyczne systemy mikroprocesorowe) oraz podsystemy wykonawcze, stanowią newralgiczną część złożonych obiektów i systemów infrastruktury krytycznej.

W związku z tym dokonano identyfikacji rodzajów struktur sieciowych wykorzystywanych w analizowanych obiektach technicznych oraz sklasyfikowano systemy wykorzystujące różne kanały transmisji danych, wraz z określeniem rozwiązań poprawiających stopień bezpieczeństwa informacji w takich systemach. Powyższa identyfikacja i klasyfikacja ułatwia integrację zagadnień analizy bezpieczeństwa funkcjonalnego i ochrony informacji, bazującej na założeniu, że zagadnienia bezpieczeństwa funkcjonalnego są nadrzędne w stosunku do ochrony informacji. Zaproponowano podejście, w którym aspekty ochrony informacji są rozpatrywane jako jeden z czynników mających wpływ na ryzyko związane z funkcjonowaniem obiektu technicznego.

Przy projektowaniu rozproszonych skomputeryzowanych systemów sterowania i zabezpieczeń powinno się uwzględnić wszystkie potencjalne zagrożenia. Należy pamiętać, że duży wpływ na występowanie tych zagrożeń ma fakt, iż we współczesnych systemach technicznych wykorzystywane są zarówno wewnętrzne, jak i zewnętrzne kanały transmisji danych. Kanały zewnętrzne umożliwiają zwiększenie funkcjonalności systemu, lecz mogą być źródłem pogorszenia stanu bezpieczeństwa, jeżeli nie zostaną we właściwy

sposób zaprojektowane i nie będą użytkowane przy wykorzystaniu odpowiednich rozwiązań, np. VPN (*virtual private network*) i/lub DMZ (*demilitarized zone*).

W monografii przedstawiono pewne procedury oraz zalecenia dotyczące metodyki zintegrowanego zarządzania bezpieczeństwem funkcjonalnym, która uwzględnia aspekty związane z ochroną informacji w rozproszonych systemach sterowania i zabezpieczeń. Zastosowanie niniejszych procedur oraz wytycznych będzie sprzyjać wprowadzaniu nowej jakości w projektowaniu i użytkowaniu rozwiązań do realizacji funkcji związanych z bezpieczeństwem na różnych wymaganych poziomach nienaruszalności bezpieczeństwa SIL, określonych na podstawie analizy i oceny ryzyka. Aktualne normy bezpieczeństwa funkcjonalnego nie uwzględniają w wystarczającym stopniu wpływu zagadnień związanych z ochroną informacji na wyniki analiz, przez co zaprezentowane podejście rozszerza aspekty metodyczne możliwe do zastosowania przy tego typu ocenach.

Należy podkreślić, że zagadnienia dotyczące cyberbezpieczeństwa w komputerowych i programowalnych systemach sterowania i zabezpieczeń (rozwiązania bazujące na rozmaitych strukturach PLC, w szczególności strukturach nadmiarowych) są aktualnymi zadaniami badawczymi w licznych zagranicznych ośrodkach naukowo-badawczych oraz innowacyjno-wdrożeniowych. Stanowią one również przedmiot wzrastającego zainteresowania organizacji krajowych i międzynarodowych.

W monografii przedstawiono metody klasyfikacji zagrożeń i czynników ryzyka w przemysłowych sieciach komputerowych. Przy realizacji tego zadania wykorzystano obserwację podatności rozproszonych systemów sterowania i zabezpieczeń na przykładzie systemu SIS współpracującego z systemem DCS. Wzięto pod uwagę zaproponowaną klasyfikację systemów oraz podatności na zagrożenia, które mogą w nich występować. Opracowane metody określenia wymaganego poziomu SIL i jego weryfikacji dla funkcji bezpieczeństwa w kontekście wymagań dotyczących poziomów EAL oraz innych czynników związanych z określonym stopniem ochrony informacji, np. na podstawie poziomów uzasadnionej ochrony SAL, metodyki SeSa oraz wykorzystania wyników analiz FMEA/FMECA (załącznik Z.2), zostały zaimplementowane w prototypowym oprogramowaniu ProSIL-EAL.

Załącznik 1

DEFINICJE [114, 159, 161, 162, 166]

Architektura (*architecture*) – konkretna konfiguracja elementów sprzętu i oprogramowania w systemie. Uporządkowanie elementów sprzętu i/lub oprogramowania w systemie. Uporządkowanie podsystemów przyrządowego systemu bezpieczeństwa SIS. Struktura wewnętrzna podsystemu SIS. Uporządkowanie programów w oprogramowaniu. Według PN-EN 61511 architektura to uporządkowanie elementów sprzętu i/lub oprogramowania w systemie, np.: uporządkowanie podsystemów przyrządowego systemu bezpieczeństwa SIS; struktura wewnętrzna podsystemu SIS; uporządkowanie programów w oprogramowaniu.

Audyt bezpieczeństwa funkcjonalnego (*functional safety audit*) – systematyczne i niezależne badanie w celu stwierdzenia, czy konkretne procedury bezpieczeństwa funkcjonalnego są zgodne z procedurami przewidzianymi, czy są skutecznie wprowadzone do stosowania i czy są odpowiednie do osiągnięcia konkretnych celów. Audyt bezpieczeństwa funkcjonalnego może być częścią oceny bezpieczeństwa funkcjonalnego.

Bezpieczeństwo (*safety*) – niewystępowanie ryzyka nieakceptowalnego.

Bezpieczeństwo funkcjonalne (*functional safety*) – część bezpieczeństwa całkowitego odnosząca się do EUC, która zależy od prawidłowego działania systemów E/E/PE związanych z bezpieczeństwem, systemów związanych z bezpieczeństwem opracowanych w innych technikach i zewnętrznych środków zmniejszania ryzyka. Według PN-EN 61511 jest to część bezpieczeństwa całkowitego odnosząca się do procesu i BPCS, która zależy od prawidłowego działania SIS i innych warstw zabezpieczeń.

Cykl życia bezpieczeństwa (*safety lifecycle*) – czynności konieczne do zaimplementowania systemów związanych z bezpieczeństwem, podejmowane w okresie, który rozpoczyna się w fazie koncepcji projektu i kończy się, gdy wszystkie systemy E/E/PE związane z bezpieczeństwem oraz te opracowane w innych technologiach i zewnętrzne urządzenia do zmniejszenia ryzyka nie nadają się dłużej do użycia.

Cykl życia oprogramowania (*software lifecycle*) – czynności podejmowane w okresie, który rozpoczyna się w fazie opracowania koncepcji oprogramowania i kończy się, gdy oprogramowanie nie jest używane.

Docelowa miara uszkodzeń (*target failure measure*) – zamierzone do osiągnięcia prawdopodobieństwo wystąpienia uszkodzeń niebezpiecznych, wynikające z wymagań nienaruszalności bezpieczeństwa, wyszczególnione jako: przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa realizowanej na rzadkie przywołanie do działania lub prawdopodobieństwo występowania uszkodzenia niebezpiecznego na godzinę w przypadku rodzaju pracy ciągłej lub na częste przywołanie.

Funkcja bezpieczeństwa (*safety function*) – funkcja zaimplementowana przez system E/E/PE związany z bezpieczeństwem, system wiążący się z bezpieczeństwem opracowany

w innej technice lub zewnętrzne urządzenie do zmniejszenia ryzyka, którego przeznaczeniem jest osiągnięcie lub utrzymanie stanu bezpiecznego EUC w odniesieniu do konkretnego zdarzenia zagrażającego. Według PN-EN 61511 jest to funkcja do zaimplementowania przez SIS, system związany z bezpieczeństwem opracowany w innej technice lub zewnętrzne urządzenie do zmniejszenia ryzyka, której przeznaczeniem jest osiągnięcie lub utrzymanie stanu bezpiecznego procesu w odniesieniu do konkretnego zdarzenia zagrażającego.

Interfejs operatora (*operator interface*) – środki, za pomocą których następuje wymiana informacji między operatorem a BPCS lub SIS.

Interwał testu diagnostycznego (*diagnostic test interval*) – odstęp czasowy między testami *on-line* wykonywanymi w celu wykrycia defektów w systemie wiążącym się z bezpieczeństwem, który występuje w konkretnym pokryciu diagnostycznym.

Język o ograniczonej zmienności (*limited variability language*) – język programowania, tekstowy albo graficzny, do komercyjnych i przemysłowych elektronicznych sterowników programowalnych, o zakresie stosowalności ograniczonym tylko do tych sterowników. Wymienione języki programowania, zaczerpnięte z PN-EN 61131 i z innych źródeł, są językami o ograniczonej zmienności, stosowanymi do przedstawiania programów aplikacyjnych systemów PLC: język drabinkowy, algebra boolowska, schematy bloków funkcyjnych, matryce bezpieczeństwa i karty funkcyjne.

Kanał (*channel*) – element lub grupa elementów realizujący/ realizujących funkcję niezależnie.

Konieczna redukcja ryzyka (*necessary risk reduction*) – zmniejszenie ryzyka osiągnięte przez systemy E/E/PE związane z bezpieczeństwem oraz systemy wykonane w innych technikach i zewnętrzne urządzenia do zmniejszania ryzyka w celu zapewnienia, że nie zostanie przekroczone ryzyko tolerowane.

Nienaruszalność bezpieczeństwa (*safety integrity*) – prawdopodobieństwo, że system wiążący się z bezpieczeństwem zrealizuje wymagane funkcje bezpieczeństwa w sposób satysfakcjonujący, w określonych warunkach i określonym czasie.

Nienaruszalność bezpieczeństwa oprogramowania (*software safety integrity*) – część nienaruszalności bezpieczeństwa systemu związanego z bezpieczeństwem, która odnosi się do niebezpiecznych uszkodzeń systematycznych przypisywanych oprogramowaniu.

Nienaruszalność bezpieczeństwa sprzętu (*hardware safety integrity*) – część nienaruszalności bezpieczeństwa systemów wiążących się z bezpieczeństwem, która odnosi się do niebezpiecznych uszkodzeń przypadkowych sprzętu. Termin ten odnosi się do uszkodzeń niebezpiecznych, to znaczy takich, które mogą osłabić nienaruszalność działania systemu wiążącego się z bezpieczeństwem. W tym znaczeniu ocenia się dwa parametry: całkowitą intensywność uszkodzeń niebezpiecznych lub prawdopodobieństwo uszkodzenia przy pracy na przywołanie. Pierwszy z tych wskaźników jest stosowany w przypadku, gdy konieczne jest utrzymanie sterowania ciągłego w celu zapewnienia bezpieczeństwa, natomiast drugi parametr jest stosowany w przypadku typowych systemów zabezpieczeniowych. Według PN-EN 61511 jest to część nienaruszalności bezpieczeństwa przyrządowej funkcji bezpieczeństwa, odnosząca się do niebezpiecznych przypadkowych uszkodzeń sprzętu. Niniejszy termin odnosi się do uszkodzeń niebezpiecznych, czyli takich uszkodzeń przyrządowych funkcji bezpieczeństwa, które mogłyby pogorszyć ich nienaruszalność bezpie-

czeństwa. Dwa istotne w tym kontekście parametry to całkowita intensywność uszkodzeń niebezpiecznych i prawdopodobieństwo uszkodzenia przy pracy na przywołanie.

Nienaruszalność bezpieczeństwa systematyczna (*systematic safety integrity*) – część nienaruszalności bezpieczeństwa systemów wiążących się z bezpieczeństwem, która odnosi się do niebezpiecznych uszkodzeń systematycznych. Nienaruszalność bezpieczeństwa systematyczna nie może być zwykle określona liczbowo, w odróżnieniu od nienaruszalności bezpieczeństwa sprzętu, która normalnie może być określona w ten sposób.

Ocena bezpieczeństwa funkcjonalnego (*functional safety assessment*) – badanie oparte na dowodach, podjęte w celu oceny bezpieczeństwa funkcjonalnego osiągniętego przez jeden lub kilka systemów E/E/PE związanych z bezpieczeństwem, jeden lub kilka systemów związanych z bezpieczeństwem opracowanych w innych technikach i przez zewnętrzne urządzenia do zmniejszenia ryzyka. Według PN-EN 61511 jest to badanie oparte na dowodach, podjęte w celu oceny bezpieczeństwa funkcjonalnego osiągniętego za pomocą co najmniej jednej warstwy zabezpieczeń.

Oprogramowanie (*software*) – wytwór intelektualny zawierający programy, procedury, dane, reguły i wszelką dokumentację z nimi związaną, odnoszącą się do działania systemu przetwarzania danych.

Oprogramowanie wiążące się z bezpieczeństwem (*safety related software*) – oprogramowanie stosowane do zaimplementowania funkcji bezpieczeństwa w systemie związanym z bezpieczeństwem.

Podstawowy system sterowania procesem (BPCS) – system, który odpowiada na sygnały wejściowe z procesu, łącznie ze związanym z nim wyposażeniem, innymi systemami programowalnymi i/lub operatorem, który generuje sygnały wyjściowe powodujące, że proces i związane z nim wyposażenie pracują w zadany sposób, ale który nie realizuje żadnej przyrządowej funkcji bezpieczeństwa, od której wymaga się poziomu SIL większego niż 1.

Pokrycie diagnostyczne (*diagnostics coverage*) – względne zmniejszenie prawdopodobieństwa niebezpiecznych uszkodzeń sprzętu, wynikające z działania automatycznych testów diagnostycznych.

Poziom nienaruszalności bezpieczeństwa (*safety integrity level*, SIL) – poziom dyskretny, jeden z możliwych czterech, do wyszczególnienia wymagań nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które mają być alokowane w systemach E/E/PE związanych z bezpieczeństwem. Przy tym poziom nienaruszalności bezpieczeństwa 4 jest poziomem najwyższym, a poziom nienaruszalności bezpieczeństwa 1 – najniższym. Docelowe miary uszkodzeń wszystkich czterech poziomów nienaruszalności bezpieczeństwa są wyszczególnione w tablicach 2 i 3 w normie IEC 61508-1, odpowiednio dla dwóch rodzajów pracy: rzadkiego przywołania do działania i częstego przywołania do działania lub ciągłego.

Poziom nienaruszalności bezpieczeństwa oprogramowania (*software safety integrity level*) – poziom dyskretny, jeden z możliwych czterech, do wyszczególnienia wymagań nienaruszalności bezpieczeństwa oprogramowania w systemie związanym z bezpieczeństwem.

Przyrządowa funkcja bezpieczeństwa (*safety instrumented function*, SIF) – funkcja bezpieczeństwa o określonym poziomie nienaruszalności bezpieczeństwa, konieczna do osiągnięcia bezpieczeństwa funkcjonalnego, która może być albo przyrządową funkcją bezpieczeństwa zabezpieczającą, albo przyrządową funkcją bezpieczeństwa sterowania.

Przyrządowa funkcja bezpieczeństwa ciągła (*continuous mode safety instrumented function*) – sytuacja, gdy podczas niebezpiecznego uszkodzenia przyrządowej funkcji bezpieczeństwa potencjalne zagrożenie pojawia się bez kolejnego uszkodzenia, jeśli przedtem nie zostanie podjęte działanie zabezpieczające.

Przyrządowa funkcja bezpieczeństwa na przywołanie (*demand mode safety instrumented function*) – sytuacja, gdy określona czynność (np. zamknięcie zaworu) jest wykonywana jako odpowiedź na warunki procesu lub inne przywołanie. W przypadku niebezpiecznego uszkodzenia przyrządowej funkcji bezpieczeństwa potencjalne zagrożenie pojawia się tylko wtedy, gdy nastąpi uszkodzenie w procesie lub w BPCS.

Przyrządowa funkcja bezpieczeństwa sterowania (*safety instrumented control function*) – przyrządowa funkcja bezpieczeństwa o określonym SIL, w ciągłym rodzaju pracy, konieczna do zapobiegania powstawaniu warunków zagrażających i/lub do ograniczenia ich konsekwencji.

Przyrządowy system bezpieczeństwa (*safety instrumented system*, SIS) – system przyrządowy stosowany do zaimplementowania co najmniej jednej przyrządowej funkcji bezpieczeństwa. SIS jest złożony z dowolnej kombinacji czujników, jednostek logicznych i elementów końcowych. Taki system może zawierać albo przyrządowe funkcje bezpieczeństwa sterowania, albo zabezpieczające, albo oba typy funkcji. SIS może zawierać oprogramowanie lub go nie zawierać.

Przyrządowy system bezpieczeństwa sterowania (*safety instrumented control system*) – system przyrządowy stosowany do zaimplementowania co najmniej jednej przyrządowej funkcji bezpieczeństwa sterowania. Przyrządowy system bezpieczeństwa sterowania jest rzadkością w przemysłach procesowych. Kiedy takie systemy zostaną zidentyfikowane, należy je potraktować jako przypadki szczególne i zaprojektowane na odrębnej podstawie. Zaleca się zastosowanie wymagań zawartych w normie PN-EN 61511, lecz może być wymagana dalsza analiza szczegółowa w celu wykazania, że system nadaje się do osiągnięcia wymagań bezpieczeństwa.

Redundancja (*redundancy*) – nadmiarowość, zastosowanie środków dodanych do środków wystarczających w danej jednostce funkcjonalnej do realizacji wymaganej funkcji. Redundancja jest stosowana przede wszystkim w celu poprawienia nieuszkadzalności i dyspozycyjności poprzez zastosowanie wielokrotnych elementów lub systemów do wypełnienia tej samej funkcji. Redundancja może być wprowadzona za pomocą elementów identycznych lub różnych.

Rodzaj pracy (*mode of operation*) – przewidziany sposób pracy systemu związanego z bezpieczeństwem, odniesiony do częstości przywołań. Wyróżnia się dwa rodzaje pracy: rodzaj pracy na rzadkie przywołanie – gdy częstość wezwań zadziałania systemu związanego z bezpieczeństwem nie przekracza jednego na rok i nie jest większa niż dwukrotna częstość testów okresowych; rodzaj pracy na częste przywołanie lub ciągły – gdy częstość wezwań zadziałania systemu wiążącego się z bezpieczeństwem jest większa niż jeden na rok i większa niż dwukrotna częstość testów okresowych. Ten rodzaj pracy obejmuje systemy wiążące się z bezpieczeństwem, które implementują sterowanie ciągłe w celu utrzymania bezpieczeństwa funkcjonalnego. Według PN-EN 61511 jest to sposób, w jaki działa przyrządowa funkcja bezpieczeństwa.

Ryzyko (*risk*) – kombinacja prawdopodobieństwa wystąpienia szkody i ciężkości tej szkody.

Ryzyko procesu (*process risk*) – ryzyko pochodzące od warunków procesu spowodowanych zdarzeniami nienormalnymi, łącznie z usterką BPCS. W tym kontekście ryzyko jest związane z konkretnym zdarzeniem zagrażającym, w którym ma być zastosowany SIS, aby zapewnić konieczne zmniejszenie ryzyka. Analiza ryzyka procesu została opisana w PN-EN 61511. Głównym celem określenia ryzyka procesu jest ustalenie punktu odniesienia ryzyka, gdy nie bierze się pod uwagę warstw zabezpieczeń.

Ryzyko resztkowe (*residual risk*) – ryzyko pozostające po zastosowaniu środków bezpieczeństwa.

Ryzyko tolerowane (*tolerable risk*) – ryzyko, które jest akceptowalne w określonym kontekście opartym na aktualnych wartościach społecznych.

Specyfikacja wymagań bezpieczeństwa (*safety requirements specification*) – specyfikacja zawierająca wszystkie wymagania dotyczące funkcji bezpieczeństwa, które mają być wypełniane przez systemy związane z bezpieczeństwem. Specyfikacja ta obejmuje wymagania odnoszące się do funkcji bezpieczeństwa oraz do nienaruszalności bezpieczeństwa.

Specyfikacja wymagań dotyczących funkcji bezpieczeństwa (*safety functions requirement specification*) – specyfikacja ta precyzuje szczegóły dotyczące funkcji bezpieczeństwa, które mają wypełniać systemy związane z bezpieczeństwem. Specyfikacja powinna być udokumentowana w postaci tekstu, schematów blokowych, macierzy, schematów logicznych itp., przy założeniu, że dokumenty te przekazują jasne informacje o funkcjach bezpieczeństwa.

Specyfikacja wymagań dotyczących nienaruszalności bezpieczeństwa (*safety integrity requirements specification*) – specyfikacja zawierająca wymagania dotyczące nienaruszalności bezpieczeństwa funkcji bezpieczeństwa, które mają być wypełniane przez systemy związane z bezpieczeństwem.

Sprawdzony w użyciu (*proven in use*) – sprawdzenie oparte na analizie doświadczenia eksploatacyjnego konkretnej konfiguracji elementu. Wykazanie, że prawdopodobieństwo niebezpiecznych uszkodzeń systematycznych jest wystarczająco niskie, tak że każda funkcja bezpieczeństwa, która stosuje ten element, osiąga wymagany poziom nienaruszalności bezpieczeństwa.

System sterowania (*control system*) – system, który odpowiada na sygnały wejściowe z procesu i/lub od operatora i generuje sygnały wyjściowe, powodując, że proces działa w pożądany sposób. System sterowania obejmuje urządzenia wejściowe i elementy końcowe i może być albo BPCS, albo SIS lub stanowić kombinację obydwu.

System związany z bezpieczeństwem (*safety-related system*) – system, który jednocześnie implementuje wymagane funkcje bezpieczeństwa konieczne do osiągnięcia lub utrzymania stanu bezpiecznego EUC oraz jest przeznaczony do osiągnięcia koniecznej nienaruszalności bezpieczeństwa wymaganych funkcji bezpieczeństwa.

System związany z bezpieczeństwem opracowany w innej technice (*other technology safety-related system*) – system związany z bezpieczeństwem oparty na innej technice niż elektryczna/ elektroniczna/ programowalna elektroniczna (np. ciśnieniowy zawór bezpieczeństwa PSV).

Szkoda (*harm*) – fizyczny uraz lub pogorszenie stanu zdrowia, zarówno bezpośrednie, jak i pośrednie, albo uszczerbek w majątku lub środowisku.

Sytuacja zagrożenia (*hazardous situation*) – sytuacja, w której osoba jest narażona na zagrożenie.

Test sprawdzający (*proof test*) – test okresowy wykonywany w celu wykrycia uszkodzeń w systemie związanym z bezpieczeństwem, po to by, jeśli to konieczne, system mógł zostać naprawiony do stanu jak nowy lub stanu praktycznie mu bliskiego. Skuteczność testu okresowego będzie zależeć od tego, w jakim stopniu naprawa doprowadziła system do stanu jak nowy. Aby test okresowy był w pełni skuteczny, konieczne jest wykrycie 100% uszkodzeń niebezpiecznych. Chociaż w praktyce w przypadkach innych niż systemy związane z bezpieczeństwem o niskim stopniu złożoności osiągnięcie tych 100% nie jest łatwe, to zaleca się dążenie do tego celu. Jako minimum wszystkie realizowane funkcje bezpieczeństwa są sprawdzane wg specyfikacji wymagań bezpieczeństwa E/E/PES. Jeśli są używane odrębne kanały, test przeprowadza się w każdym kanale oddzielnie.

Urządzenie zewnętrzne do zmniejszenia ryzyka (*external risk reduction facility*) – środek do zmniejszenia lub złagodzenia ryzyka, oddzielony i odrębny od systemów E/E/PE związanych z bezpieczeństwem lub systemów związanych z bezpieczeństwem opracowanych w innych technikach.

Uszkodzenie (*failure*) – zakończenie zdolności jednostki funkcjonalnej do wypełniania wymaganej funkcji. Uszkodzenia są albo przypadkowe, co dotyczy sprzętu, albo systematyczne, co dotyczy oprogramowania.

Uszkodzenie bezpieczne (*safe failure*) – uszkodzenie, które nie ma możliwości wprowadzenia systemu związanego z bezpieczeństwem w stan zagrażający lub w stan niemożliwości wypełniania funkcji.

Uszkodzenie niebezpieczne (*dangerous failure*) – uszkodzenie, które ma możliwość wprowadzenia systemu związanego z bezpieczeństwem w stan zagrażający lub w stan niemożliwości wypełniania funkcji.

Uszkodzenie systematyczne (*systematic failure*) – uszkodzenie wiążące się w sposób deterministyczny z pewnymi przyczynami, które mogą zostać usunięte tylko przez modyfikację projektu lub procesu produkcyjnego, procedur eksploatacyjnych, dokumentacji lub innych odpowiednich czynników.

Uszkodzenie spowodowane wspólną przyczyną (*common cause failure*, CCF) – uszkodzenie, które jest wynikiem jednego lub kilku zdarzeń, powodujące jednoczesne uszkodzenie dwóch lub kilku oddzielnych kanałów w urządzeniu wielokanałowym, prowadzące do uszkodzenia systemu.

Uszkodzenie zależne (*dependent failure*) – uszkodzenie, którego prawdopodobieństwo nie może być wyrażone jako prosty iloczyn prawdopodobieństw bezwarunkowych poszczególnych zdarzeń, które je wywołują.

Walidacja (*validation*) – potwierdzenie przez badanie i przedstawienie obiektywnego dowodu, że zostały spełnione wymagania dotyczące konkretnego użycia. Według PN-EN 61511 jest to wykazanie, że rozpatrywana przyrządowa funkcja bezpieczeństwa i przyrządowy system bezpieczeństwa po zainstalowaniu spełniają pod wszystkimi względami specyfikację wymagań bezpieczeństwa.

Warstwa ochrony (*protection layer*) – niezależny mechanizm zmniejszający ryzyko przez sterowanie, zapobieganie lub ograniczanie.

Weryfikacja (*verification*) – wykazanie poprzez analizę i/lub badania w odniesieniu do każdej fazy odpowiedniego cyklu życia bezpieczeństwa, że określonym danym wejściowym odpowiadają dane wyjściowe zgodne pod wszystkimi względami z celami i wymaganiami ustalonymi dla określonej fazy.

Weryfikacja SIL (*SIL verification*) – formalny dowód, jakościowy lub ilościowy probabilistyczny, wykazujący, że proponowana architektura sprzętu realizującego funkcję lub funkcje bezpieczeństwa spełnia przypisane im wymagania SIL. Weryfikację ilościową SIL przeprowadza się metodami modelowania probabilistycznego systemów E/E/PE (BPCS, ESD, SRS lub SIS) obliczając (przy wykorzystaniu technik: grafów Markowa, schematów blokowych niezawodności, drzew niezdatności lub równań uproszczonych), w zależności od rodzaju pracy funkcji bezpieczeństwa, przeciętne prawdopodobieństwo niewypełnienia funkcji bezpieczeństwa na żądanie PFD_{avg} lub średnią częstość występowania uszkodzenia niebezpiecznego na godzinę PFH. Otrzymane wyniki są następnie porównywane z kryteriami przedziałowymi odpowiadającymi poszczególnym poziomom nienaruszalności bezpieczeństwa SIL dla danego rodzaju pracy funkcji bezpieczeństwa.

Wyposażenie sterowane (*equipment under control*, EUC) – wyposażenie, maszyny, aparaty lub instalacje stosowane do wytwarzania, przetwarzania w przemyśle procesowym, transporcie, medycynie i w innych dziedzinach działalności.

Zagrożenie (*hazard*) – potencjalne źródło szkody. Niebezpieczeństwo dla osób powstające w krótkim czasie, np. pożar lub eksplozja, a także skutki długotrwałego oddziaływania na zdrowie osób.

Zewnętrzne środki zmniejszenia ryzyka (*external risk reduction facilities*) – środki do zmniejszenia lub złagodzenia ryzyka, które są oddzielone i odrębne od SIS.

Zdarzenie zagrażające (*hazardous event*) – sytuacja zagrażająca, której wynikiem jest szkoda.

Zróżnicowanie (*diversity*) – różne środki do wypełnienia wymaganej funkcji bezpieczeństwa.

Załącznik 2

ANALIZA RODZAJÓW, SKUTKÓW I KRYTYCZNOŚCI USZKODZEŃ FMECA WEDŁUG MIL-STD-1629A

W niniejszej monografii zaproponowano metody określania wymaganego poziomu nienaruszalności bezpieczeństwa SIL i jego weryfikacji dla funkcji bezpieczeństwa w kontekście wymagań dotyczących poziomu EAL, poziomu SAL oraz innych czynników związanych z określonym stopniem ochrony informacji na podstawie metodyki SeSa oraz wyników uzyskanych z analiz FMEA i FMECA.

Metoda analizy rodzajów, skutków i krytyczności uszkodzeń FMECA (*failure mode, effect and criticality analysis*) jest metodą indukcyjną analizy nieuszkadzalności i bezpieczeństwa systemu o stosunkowo małej złożoności, która pozwala na określenie kolejności zdarzeń spowodowanych przez możliwe – w tym wcześniej zidentyfikowane w podobnych systemach – rodzaje uszkodzeń i ich skutki. Niektóre narzędzia komputerowe wspomagające analizę pozwalają na klasyfikację i grupowanie uszkodzeń według możliwości ich wykrycia, przeprowadzenia testów funkcjonalnych czy też naprawy lub wymiany elementów. Metoda FMECA umożliwia określanie poziomów krytyczności dla poszczególnych rodzajów uszkodzeń elementów lub całych wyróżnionych zespołów oraz pozwala oszacować prawdopodobieństwo wystąpienia zidentyfikowanych uszkodzeń.

Celem analizy krytyczności jest szeregowanie potencjalnych rodzajów uszkodzeń, zidentyfikowanych zgodnie z zasadami jakościowej analizy rodzajów i skutków uszkodzeń FMEA (*failure mode, effect analysis*) na podstawie przyjętych poziomów krytyczności i prawdopodobieństwa ich wystąpienia. Jeżeli nie ma dostępnych danych szczególnych, dotyczących prawdopodobieństwa wyróżnionych zdarzeń, dozwolone jest stosowanie tzw. podejścia jakościowego. Oszacowane w taki sposób wartości prawdopodobieństw odpowiadające poziomom krytyczności dla konkretnych elementów powinny być jednak w następnej analizie odpowiednio skorygowane, jeżeli pozyskano aktualne dane dotyczące uszkadzalności elementów danej kategorii w danych warunkach ich użytkowania, co jest zgodne z tzw. podejściem ilościowym.

Prawdopodobieństwa możliwych rodzajów uszkodzeń zostały zgrupowane w kilku zakresach. Dla rozważanego zdarzenia z określonym rodzajem uszkodzenia elementu uwzględnia się w odpowiedniej kolumnie formularza FMECA wybrany zakres prawdopodobieństwa. Wyróżniono następujące zakresy (poziomy) prawdopodobieństwa [79, 113]:

A. Zdarzenie częste – duże prawdopodobieństwo wystąpienia danego rodzaju uszkodzenia elementu (większe niż 0,2 łącznego prawdopodobieństwa uszkodzenia elementu w rozważanym przedziale czasu).
B. Zdarzenie umiarkowanie prawdopodobne – średnie prawdopodobieństwo wystąpienia danego rodzaju uszkodzenia elementu (większe niż 0,1, ale równe lub mniejsze niż 0,2 łącznego prawdopodobieństwa uszkodzenia elementu w rozważanym przedziale czasu).

C. Zdarzenie sporadyczne – małe prawdopodobieństwo wystąpienia danego rodzaju uszkodzenia elementu (większe niż 0,01, ale równe lub mniejsze niż 0,1 łącznego prawdopodobieństwa uszkodzenia elementu w rozważanym przedziale czasu).
D. Zdarzenie rzadkie – bardzo małe prawdopodobieństwo wystąpienia danego rodzaju uszkodzenia elementu (większe niż 0,001, ale równe lub mniejsze niż 0,01 łącznego prawdopodobieństwa uszkodzenia elementu w rozważanym przedziale czasu).
E. Zdarzenie bardzo rzadkie – wyjątkowo małe prawdopodobieństwo wystąpienia danego rodzaju uszkodzenia elementu (równe lub mniejsze niż 0,001 łącznego prawdopodobieństwa uszkodzenia elementu w rozważanym przedziale czasu).

Przedstawione powyżej zakresy prawdopodobieństw skupionych w pięciu przedziałach stanowią tzw. podejście jakościowe.

Źródło danych niezawodnościowych dotyczących intensywności uszkodzeń powinno być takie same jak stosowane w innych analizach niezawodnościowych (np. RBD, ET, FTA). Źródłem takim dla elementów elektronicznych może być biblioteka danych niezawodnościowych MIL-HDBK-217 z uwzględnieniem wymaganych współczynników korekcyjnych, odpowiednich dla danych warunków środowiskowych [79, 113].

Wyniki analizy rodzajów, skutków i krytyczności uszkodzeń obejmują oszacowania miar probabilistycznych. Jedną z nich jest parametr β_F, oznaczający prawdopodobieństwo warunkowe wystąpienia wyróżnionego skutku końcowego zdarzenia krytycznego, zgodnie z przyjętą klasyfikacją krytyczności, pod warunkiem wystąpienia danego rodzaju uszkodzenia.

Następnym parametrem ocenianym w analizie krytyczności jest współczynnik rodzaju uszkodzenia α, definiowany jako stosunek intensywności uszkodzeń danego (szczególnego) rodzaju λ_k do całkowitej intensywności uszkodzeń elementu (podsystemu) λ_p:

$$\alpha = \frac{\lambda_k}{\lambda_p} \tag{Z2.1}$$

gdzie: λ_k – intensywność uszkodzeń danego rodzaju, λ_p – całkowita intensywność uszkodzeń badanego podsystemu.

Gdy rozpatrywane są wszystkie potencjalne rodzaje uszkodzeń danego podsystemu, wówczas suma wartości α będzie równa 1. Intensywność uszkodzeń podsystemu λ_p szacuje się, jeśli to tylko możliwe, na podstawie danych statystycznych dotyczących uszkadzalności podsystemów (urządzeń) danej kategorii lub na podstawie odpowiedniego przewodnika (np. MIL-HDBK-217). W przypadku skorzystania z MIL-HDBK-217 uwzględnia się odpowiednie w rozważanej sytuacji współczynniki korekcyjne π_i dla bazowej intensywności uszkodzeń λ_b; wówczas intensywność uszkodzeń w danych warunkach środowiskowych ma postać [79, 115]:

$$\lambda_p = \lambda_b(\pi_Q \cdot \pi_E \cdot \pi_A \ldots) \tag{Z2.2}$$

gdzie: λ_b [h^{-1}] – bazowa intensywność uszkodzeń, oszacowana na podstawie badań niezawodnościowych, przeprowadzonych na obiektach technicznych w normalnych warunkach środowiskowych; $\pi_Q, \pi_E, \pi_A \cdots$ – współczynniki korygujące.

Intensywność uszkodzeń zależy istotnie od warunków środowiskowych, w których pracuje urządzenie, co potwierdziły testy laboratoryjne przeprowadzone na większych próbkach elementów elektronicznych. Współczynniki korekcyjne uwzględniają oddziaływanie ważniejszych czynników wpływu (*influence factors*), związanych z niekorzystnymi

warunkami środowiskowymi (wysoka temperatura, intensywne promieniowanie, duża wilgotność, wibracje, udary itd.), które powinno być uwzględnione w modelowaniu nieuszkadzalności obiektów danej kategorii.

Istotnym parametrem w analizie FMECA jest tzw. liczba krytyczności C_m dla danego rodzaju uszkodzenia urządzenia (dla szczególnego poziomu krytyczności i rozważanej fazy misji systemu), którą wyznacza się ze wzoru [113]:

$$C_m = \beta_F \cdot \alpha \cdot \lambda_p \cdot t \tag{Z2.3}$$

gdzie: β_F – prawdopodobieństwo warunkowe wystąpienia wyróżnionego skutku końcowego zdarzenia krytycznego, zgodnie z przyjętą klasyfikacją krytyczności, pod warunkiem wystąpienia danego rodzaju uszkodzenia; t – rozważany czas pracy urządzenia wyrażony w [h] lub poprzez liczbę cykli działania.

Liczbę krytyczności C_r dla danego urządzenia (podsystemu) oraz dla szczególnego poziomu krytyczności i rozważanej fazy misji systemu definiuje się jako sumę C_m:

$$C_r = \sum_i (C_m)_i = \sum_{i=1}^{n} (\beta_F \cdot \alpha \cdot \lambda_p \cdot t)_i = \sum_{i=1}^{n} (\beta_F \cdot \frac{\lambda}{\lambda_p} \cdot \lambda_p \cdot t)_i = \sum_{i=1}^{n} (\beta_F \cdot \lambda \cdot t)_i \tag{Z2.4}$$

gdzie: i – kolejny rodzaj uszkodzenia urządzenia powodujący szczególny poziom krytyczności; n – liczba uwzględnionych w analizie rodzajów uszkodzeń.

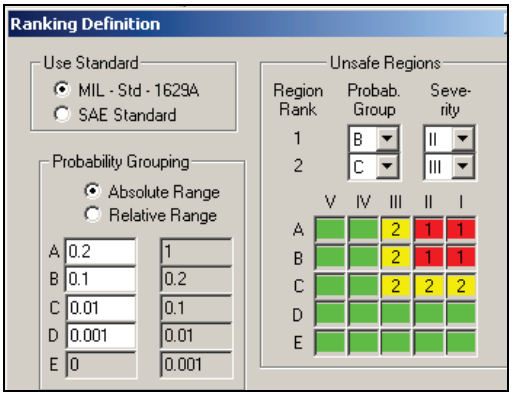
W przypadku podsystemów o wysokim poziomie nieuszkadzalności C_r ma znaczenie prawdopodobieństwa wystąpienia stanu nienormalnego podsystemu, a C_r/t jest częstością jego występowania (prawdopodobieństwem na jednostkę czasu).

Macierz krytyczności wg MIL-STD-1629A (rys Z2.1) umożliwia identyfikowanie i porównywanie poziomów krytyczności dla kolejnego rodzaju uszkodzenia i pozostałych rodzajów uszkodzeń. Macierz taka jest konstruowana przez wprowadzenie numerów identyfikacyjnych elementów (podsystemów) lub rodzajów uszkodzeń w odpowiednie pozycje macierzy, reprezentujące kategorie poziomu krytyczności oraz zakres (przedział) prawdopodobieństwa wystąpienia (lub liczbę krytyczności C_r dla rodzajów uszkodzenia elementu (podsystemu)). Uzyskana w ten sposób macierz przedstawia rozkład krytyczności dla wymienionych rodzajów uszkodzeń jednostki. Jest ona przydatna w określeniu priorytetów dla działań korekcyjnych. Im bardziej wysunięty wzdłuż poprzecznej linii jest numer (reprezentujący dany rodzaj uszkodzenia), tym większa jest potrzeba wprowadzenia odpowiednich działań korekcyjnych redukujących prawdopodobieństwo wystąpienia danego rodzaju uszkodzenia.

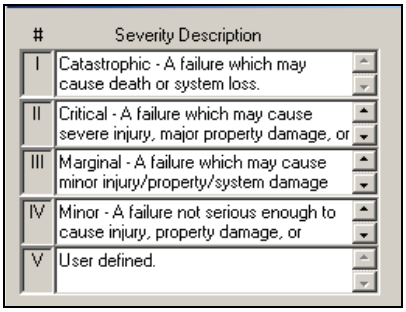
Na osi odciętych macierzy znajdują się kategorie krytyczności (rys. Z2.2).

Kategorie krytyczności wg MIL-STD-1629A:

I. Katastroficzna – uszkodzenie, które może spowodować śmierć lub całkowitą utratę obiektu.
II. Krytyczna – uszkodzenie, które może spowodować ciężkie obrażenia lub znaczną utratę obiektu, co doprowadzi do niepowodzenia misji.
III. Marginalna – uszkodzenie, które może spowodować mniejsze zranienia, mniejszą szkodę materialną lub mniejsze zniszczenie wyposażenia systemu, co doprowadzi do utraty gotowości lub niepowodzenia misji.
IV. Mało znacząca – uszkodzenie niepowodujące obrażeń, utraty własności lub zniszczenia, ale mogące spowodować nieplanowaną obsługę lub remont.

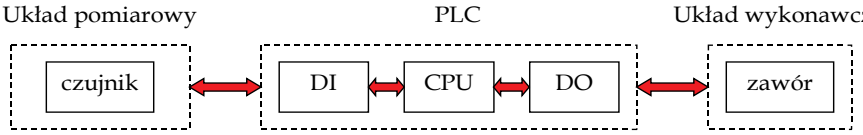


Rys. Z2.1. Macierz krytyczności stosowana w analizie FMECA według standardu 1629A



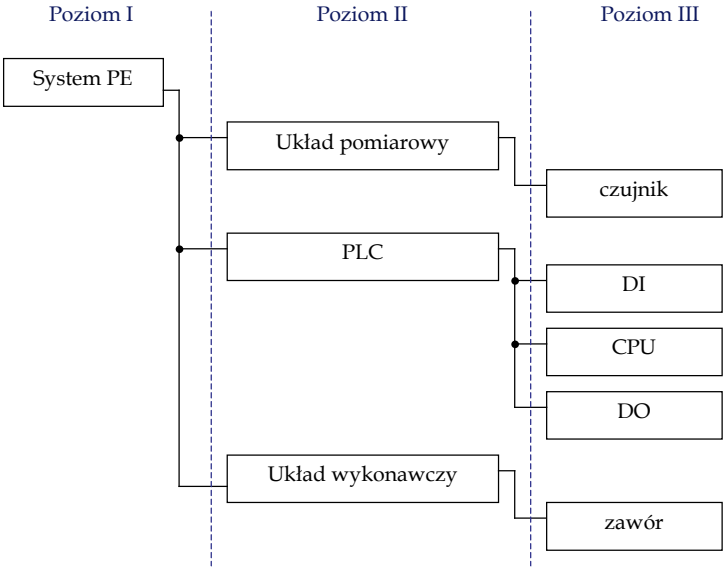
Rys. Z2.2. Ranking krytyczności wg MIL-STD-1629A (BQR moduł FMECA)

Przed rozpoczęciem analizy FMEA/FMECA należy przeprowadzić dekompozycję systemu na podsystemy i elementy. W efekcie dekompozycji uzyskuje się kilka poziomów: poziom systemu, poziomy podsystemów oraz poziom elementów. Jako przykład zostanie rozpatrzony prosty system SIS (rys. Z2.3), składający się z trzech podsystemów: układu pomiarowego (czujnik), układu przetwarzania danych (sterownik PLC: moduł wejść dyskretnych DI, procesor CPU, moduł wyjść dyskretnych DO) oraz układu wykonawczego (zawór).



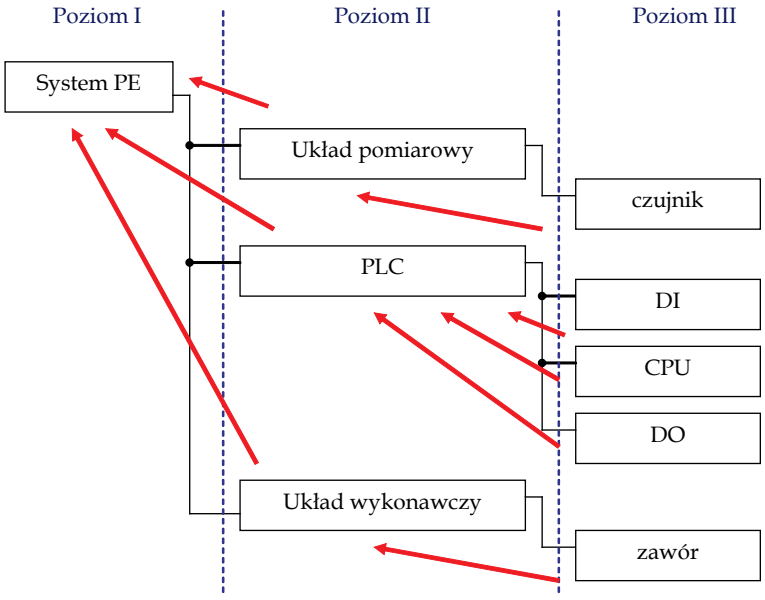
Rys. Z2.3. Schemat rozpatrywanego systemu E/E/PE (SIS)

System PE (SIS) z rys. Z2.3 po dokonaniu dekompozycji można przedstawić w postaci tzw. drzewa hierarchii (rys. Z2.4).



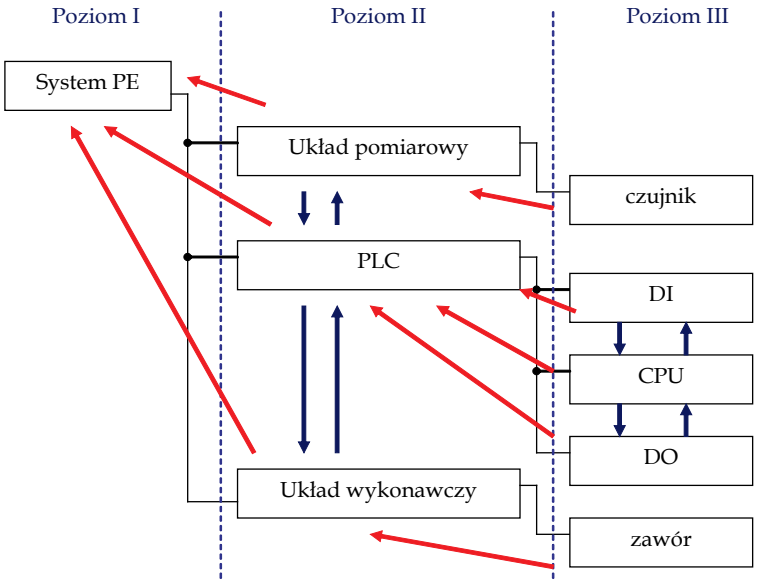
Rys. Z2.4. Drzewo hierarchii systemu PE (trzy poziomy dekompozycji)

Propagacja uszkodzeń przebiega od poziomu najniższego – w danym przypadku jest to poziom III (elementy) – do poziomu najwyższego – I (system) – poprzez poziomy pośrednie (podsystemów), przy czym w danym przypadku występuje tylko jeden poziom pośredni (poziom II) (rys. Z2.5).



Rys. Z2.5. Drzewo hierarchii systemu PE (SIS) (trzy poziomy dekompozycji)

Oprócz prostej propagacji uszkodzeń z dolnego poziomu wyróżnia się również wpływ uszkodzenia elementu bądź podsystemu na inny element bądź podsystem na tym samym poziomie hierarchii. W tym wypadku musi zostać spełniony warunek, aby rozpatrywane elementy bądź podsystemy były częścią: w przypadku elementu – tego samego podsystemu, w przypadku podsystemu – tego samego systemu (rys. Z2.6).



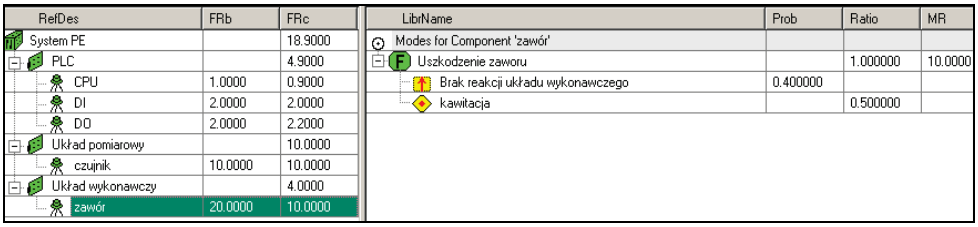
Rys. Z2.6. Wpływ uszkodzeń elementów/ podsystemów znajdujących się na tym samym poziomie na siebie, a następnie na system

Każdemu elementowi można przypisać intensywność uszkodzeń λ. W danym przypadku $\lambda_{\text{czujnik}} = 1 \cdot 10^{-5}$ [h^{-1}], $\lambda_{\text{DI}} = 2 \cdot 10^{-6}$ [h^{-1}], $\lambda_{\text{CPU}} = 1 \cdot 10^{-6}$ [h^{-1}], $\lambda_{\text{DO}} = 2 \cdot 10^{-6}$ [h^{-1}], $\lambda_{\text{zawór}} = 2 \cdot 10^{-5}$ [h^{-1}]. Z każdym elementem znajdującym się na poziomie elementarnym może być związanych kilka rodzajów uszkodzeń. Z każdym rodzajem uszkodzenia może się zaś wiązać kilka skutków lokalnych spowodowanych przez kilka przyczyn elementarnych. Intensywności uszkodzeń podsystemów/ systemów są funkcją:

— intensywności uszkodzeń elementów wchodzących w skład danego podsystemu/ systemu (λ);
— prawdopodobieństw wystąpienia skutków lokalnych (p);
— prawdopodobieństw pojawienia się przyczyn elementarnych (r).

Przykład został sporządzony przy wykorzystaniu modułu FMECA w oprogramowaniu CARE BQR.

Intensywność uszkodzeń zaworu wynosi $\lambda_{\text{zawór}} = 20 \cdot 10^{-6}$ [h^{-1}] ($FR_{\text{bzawór}}$) (co w oprogramowaniu BQR odpowiada wskaźnikowi FR_{b} (*failure rate*)) (rys. Z2.7). Przyczyną elementarną, która może spowodować uszkodzenie tego elementu, może być zjawisko kawitacji, którego prawdopodobieństwo wystąpienia w danym przypadku wynosi $r = 0{,}5$ (wskaźnik *Ratio*). Przyczyna elementarna prowadzi do powstania skutku lokalnego, jakim jest w danym przypadku brak reakcji układu wykonawczego o prawdopodobieństwie wystąpienia $p = 0{,}4$ (*Prob*).



Rys. Z2.7. Poziom elementarny III (zawór)

Każdy rodzaj uszkodzenia charakteryzuje tzw. wskaźnik rodzaju uszkodzenia MR (*mode rate*), który jest równy iloczynowi intensywności uszkodzeń danego elementu i sumy prawdopodobieństw pojawienia się przyczyny elementarnej. W ogólnym przypadku dla *N*-tego poziomu hierarchii można to zapisać w postaci:

$$MR_{Ni} = \lambda_i \cdot \sum_{i=1}^{n} r_i \tag{Z2.5}$$

Intensywność uszkodzeń elementu λ_C (FR_C) po uwzględnieniu sumy prawdopodobieństw pojawienia się przyczyn elementarnych dla każdego rodzaju uszkodzenia tego elementu określa zależność:

$$\lambda_{iC} = \sum_{i=1}^{n} MR_{Ni} = \sum_{i=1}^{n} (\lambda_i \cdot \sum_{i=1}^{n} r_i)_i \tag{Z2.6}$$

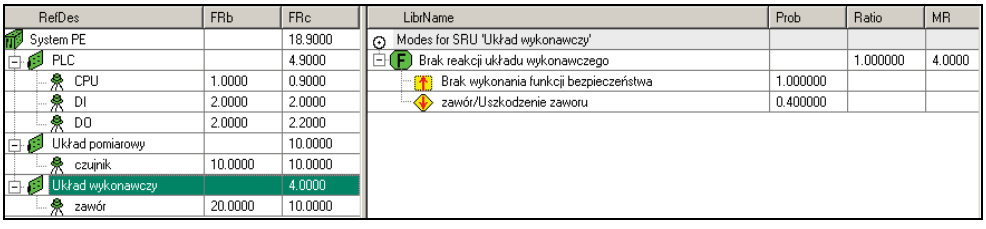
W danym przypadku, przy uwzględnieniu zależności (Z2.5) i (Z2.6), intensywność uszkodzeń zaworu $\lambda_{\text{zawórC}}$ ($FR_{\text{Czawór}}$) ma postać:

$$\lambda_{\text{zawórC}} = MR_{\text{IIIuszkodzenie/zaworu}} = \lambda_{\text{zawór}} \cdot r_{\text{kawitacja}} = 20 \cdot 0{,}5 = 10 \cdot 10^{-6}[h^{-1}] \tag{Z2.7}$$

Intensywność uszkodzeń podsystemu (np. układu wykonawczego (rys. Z2.8)) można wyznaczyć na podstawie wzoru:

$$\lambda_{\text{podsystemu}} = (\sum_{i=1}^{n} MR_{Ni} \cdot (\sum_{i=1}^{n} p_{Ni})) = \sum_{i=1}^{n} (\lambda_i \cdot \sum_{i=1}^{n} r_i \cdot (\sum_{i=1}^{n} p_{Ni}))_i \tag{Z2.8}$$

Jak widać na rys. Z2.8, brak reakcji układu wykonawczego, który na niższym poziomie hierarchii był skutkiem lokalnym, teraz funkcjonuje jako rodzaj uszkodzenia podsystemu, natomiast uszkodzenie zaworu w danym przypadku jest przyczyną, która powoduje pojawienie się skutku lokalnego, czyli *braku wykonania funkcji bezpieczeństwa*.



Rys. Z2.8. Poziom podsystemu II (układ wykonawczy)

Korzystając z zależności (Z2.8), można wyznaczyć intensywność uszkodzeń układu wykonawczego:

$$\lambda_{\text{układ/wykonawczy}} = \lambda_{\text{zawór}} \cdot r_{\text{kawitacja}} \cdot p_{\text{brak/reakcji/układu/wykonawczego}} = 20 \cdot 0{,}5 \cdot 0{,}4 = 4 \cdot 10^{-6}[\text{h}^{-1}] \quad \text{(Z2.9)}$$

Analogicznie jak powyżej (dla zaworu i układu wykonawczego), sytuacja prezentuje się w przypadku czujnika (rys. Z2.9) i układu pomiarowego (rys. Z2.10).

RefDes	FRb	FRc
System PE		18.9000
PLC		4.9000
CPU	1.0000	0.9000
DI	2.0000	2.0000
DO	2.0000	2.2000
Układ pomiarowy		10.0000
czujnik	10.0000	10.0000
Układ wykonawczy		4.0000
zawór	20.0000	10.0000

LibriName	Prob	Ratio	MR
Modes for Component 'czujnik'			
Uszkodzenie czujnika		1.000000	10.0000
Niepoprawna praca układu pomiarowego	1.000000		
przepięcie		0.400000	
zwarcie		0.600000	

Rys. Z2.9. Poziom elementarny III (czujnik)

Korzystając ze wzorów (Z2.5) i (Z2.6), można wyznaczyć intensywność uszkodzeń czujnika $\lambda_{\text{czujnikC}}$ (FR_{Cczujnik}):

$$\lambda_{\text{czujnikC}} = MR_{\text{IIIuszkodzenie/czujnika}} = \lambda_{\text{czujnik}} \cdot (r_{\text{przepięcie}} + r_{\text{zwarcie}}) = 10 \cdot (0{,}4 + 0{,}6) = 10 \cdot 10^{-6}[h^{-1}] \quad \text{(Z2.10)}$$

RefDes	FRb	FRc
System PE		18.9000
PLC		4.9000
CPU	1.0000	0.9000
DI	2.0000	2.0000
DO	2.0000	2.2000
Układ pomiarowy		10.0000
czujnik	10.0000	10.0000
Układ wykonawczy		4.0000
zawór	20.0000	10.0000

LibriName	Prob	Ratio	MR
Modes for SRU 'Układ pomiarowy'			
Niepoprawna praca układu pomiarowego		1.000000	10.0000
Brak wykonania funkcji bezpieczeństwa	1.000000		
czujnik/Uszkodzenie czujnika	1.000000		

Rys. Z2.10. Poziom podsystemu II (układ pomiarowy)

Na podstawie wzoru (Z.8) można wyznaczyć intensywność uszkodzeń układu pomiarowego:

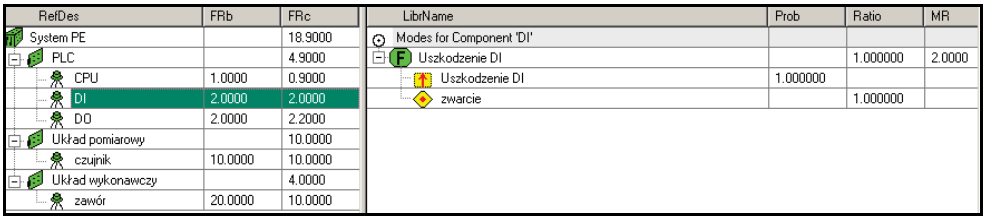
$$\lambda_{\text{układ/pomiarowy}} = \lambda_{\text{czujnik}} \cdot (r_{\text{przepięcie}} + r_{\text{zwarcie}}) \cdot p_{\text{niepoprawna/praca/układu/pomiarowego}} = 10 \cdot 1 = 10 \cdot 10^{-6}[\text{h}^{-1}] \quad \text{(Z2.11)}$$

Następnym krokiem jest przeanalizowanie podsystemu PLC oraz elementów, z których ten podsystem się składa (moduł DI (rys. Z2.11), jednostka centralna CPU (rys. Z212) oraz moduł DO (rys. Z2.13).

Wykorzystując zależności (Z2.5) i (Z2.6), intensywność uszkodzeń modułu wejść dyskretnych (rys. Z2.11) λ_{DIC} (FR_{CDI}) można zapisać w postaci:

$$\lambda_{\text{DIC}} = MR_{\text{IIIuszkodzenie/DI}} = \lambda_{\text{DI}} \cdot r_{\text{zwarcie}} = 2 \cdot 1 = 1 \cdot 10^{-6}[\text{h}^{-1}] \quad \text{(Z2.12)}$$

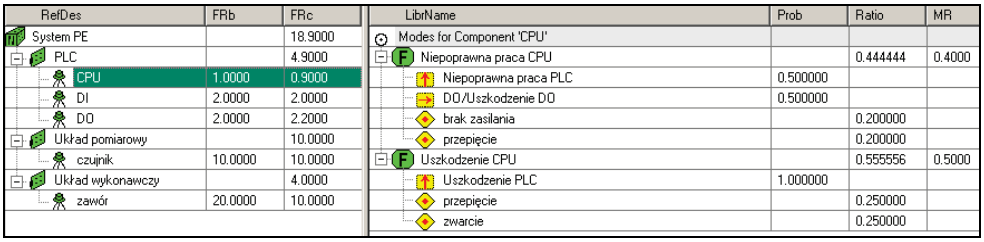
W przypadku jednostki centralnej CPU wyróżniono dwa rodzaje uszkodzeń, tj. *niepoprawną pracę CPU* oraz *uszkodzenie CPU* (rys. Z2.12). Niepoprawna praca CPU może być spowodowana brakiem zasilania lub przepięciem (są to tzw. przyczyny elementarne); w danym przypadku przyczyną elementarną może być *cyberatak* na system PE (SIS), przeprowadzony poprzez przemysłową sieć komputerową.



RefDes	FRb	FRc
System PE		18.9000
PLC		4.9000
CPU	1.0000	0.9000
DI	2.0000	2.0000
DO	2.0000	2.2000
Układ pomiarowy		10.0000
czujnik	10.0000	10.0000
Układ wykonawczy		4.0000
zawór	20.0000	10.0000

LibrName	Prob	Ratio	MR
Modes for Component 'DI'			
Uszkodzenie DI		1.000000	2.0000
Uszkodzenie DI	1.000000		
zwarcie		1.000000	

Rys. Z2.11. Poziom elementarny III (DI)



RefDes	FRb	FRc
System PE		18.9000
PLC		4.9000
CPU	1.0000	0.9000
DI	2.0000	2.0000
DO	2.0000	2.2000
Układ pomiarowy		10.0000
czujnik	10.0000	10.0000
Układ wykonawczy		4.0000
zawór	20.0000	10.0000

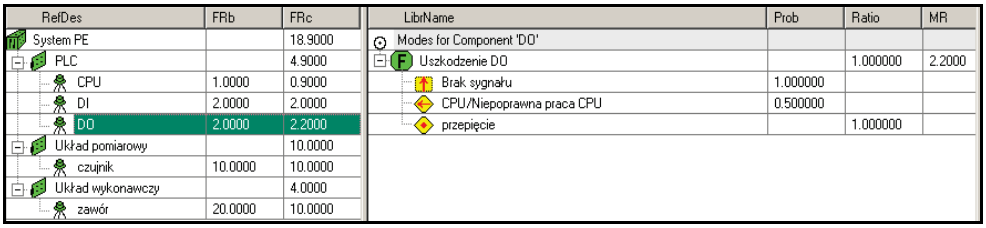
LibrName	Prob	Ratio	MR
Modes for Component 'CPU'			
Niepoprawna praca CPU		0.444444	0.4000
Niepoprawna praca PLC	0.500000		
DO/Uszkodzenie DO	0.500000		
brak zasilania		0.200000	
przepięcie		0.200000	
Uszkodzenie CPU		0.555556	0.5000
Uszkodzenie PLC	1.000000		
przepięcie		0.250000	
zwarcie		0.250000	

Rys. Z2.12. Poziom elementów III (CPU)

Na podstawie równań (Z2.5) i (Z2.6) intensywność uszkodzeń czujnika λ_{CPUC} (FR_{CCPU}) można obliczyć ze wzoru:

$$\lambda_{\text{CPUC}} = MR_{\text{IIIniepoprawna/pracaCPU}} + MR_{\text{IIIuszkodzenieCPU}} = \lambda_{\text{CPU}} \cdot (r_{\text{brak/zasilania}} + r_{\text{przepięcie}}) + \\ + \lambda_{\text{CPU}} \cdot (r_{\text{przepięcie}} + r_{\text{zwarcie}}) = 1 \cdot (0,2 + 0,2) + 1 \cdot (0,25 + 0,25) = 0,4 + 0,5 = 0,9 \cdot 10^{-6}[\text{h}^{-1}] \quad \text{(Z2.13)}$$

Uszkodzenie modułu wyjść dyskretnych może być spowodowane niepoprawną pracą CPU (jest to przyczyna związana z uszkodzeniem sąsiedniego elementu w tym samym podsystemie) bądź przepięciem (rys. Z2.13).



RefDes	FRb	FRc
System PE		18.9000
PLC		4.9000
CPU	1.0000	0.9000
DI	2.0000	2.0000
DO	2.0000	2.2000
Układ pomiarowy		10.0000
czujnik	10.0000	10.0000
Układ wykonawczy		4.0000
zawór	20.0000	10.0000

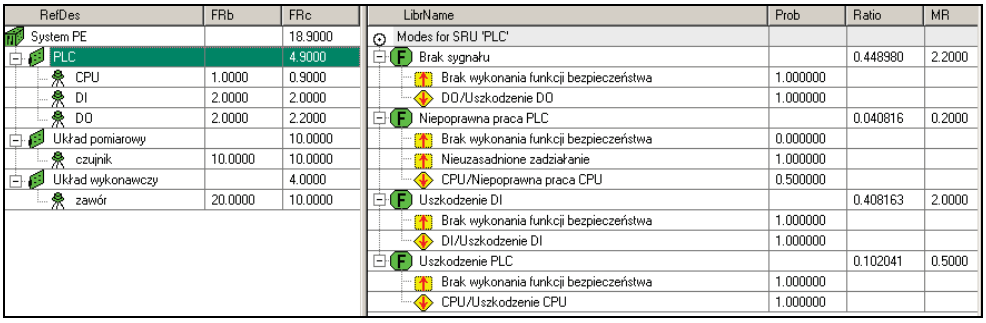
LibrName	Prob	Ratio	MR
Modes for Component 'DO'			
Uszkodzenie DO		1.000000	2.2000
Brak sygnału	1.000000		
CPU/Niepoprawna praca CPU	0.500000		
przepięcie		1.000000	

Rys. Z2.13. Poziom elementów III (DO)

Intensywność uszkodzeń modułu wyjść dyskretnych przedstawia równanie:

$$\lambda_{\text{DOC}} = MR_{\text{IIIUszkodzenieDO}} = \lambda_{DO} \cdot r_{\text{przepięcie}} + MR_{\text{IIIniepoprawna/praca/CPU}} \cdot p_{\text{uszkodzenieDO}} = \\ = 1 \cdot 2 + 0,4 \cdot 0,5 = 2,2 \cdot 10^{-6}[\text{h}^{-1}] \quad \text{(Z2.14)}$$

Poziom podsystemu PLC przedstawiono na rys. Z2.14.

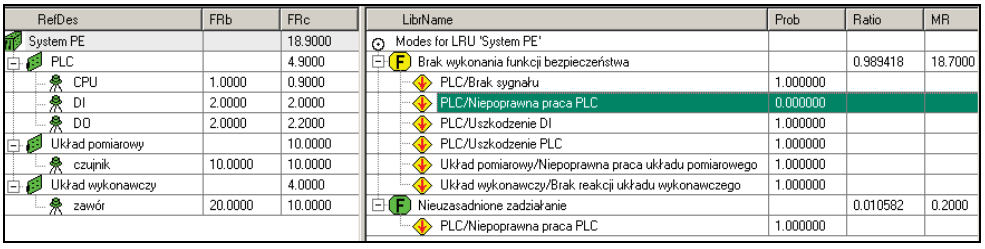


Rys. Z2.14. Poziom podsystemu II (PLC)

Intensywność uszkodzeń podsystemu PLC na podstawie zależności (Z2.8) można obliczyć ze wzoru:

$$\begin{aligned}\lambda_{\text{PLC}} &= \lambda_{\text{CPU}} \cdot (r_{\text{brak/zasilania}} + r_{\text{uszkodzenie/CPU}}) \cdot p_{\text{niepoprawna/praca/PLC}} + \\ &+\lambda_{\text{CPU}} \cdot (r_{\text{przepięcie}} + r_{\text{zwarcie}}) \cdot p_{\text{uszkodzeniePLC}} + \\ &+\lambda_{\text{DI}} \cdot r_{\text{zwarcie}} \cdot p_{\text{uszkodzenieDI}} + \lambda_{\text{DO}} \cdot r_{\text{przepięcie}} \cdot p_{\text{brak/sygnału}} + \\ &+\lambda_{\text{CPU}} \cdot (r_{\text{brak/zasilania}} + r_{\text{przepięcie}}) \cdot p_{\text{uszkodzenieDO}} = 4,9 \cdot 10^{-6}[h^{-1}]\end{aligned} \tag{Z2.15}$$

Na poziomie I *systemu PE* (SIS) wyróżniono z punktu widzenia bezpieczeństwa funkcjonalnego dwa skutki końcowe (będące jednocześnie rodzajami uszkodzeń), tj.: *brak wykonania funkcji bezpieczeństwa* oraz *nieuzasadnione zadziałanie* (rys. Z2.15).



Rys. Z2.15. Poziom systemu I (system PE/SIS)

Intensywność uszkodzeń systemu w danym przypadku jest równa sumie intensywności uszkodzeń uzyskanych dla trzech podsystemów. Jeżeli w analizie uwzględni się *cyberatak* jako jedną z przyczyn elementarnych uszkodzenia, np. jednostki CPU w podsystemie PLC, wówczas wywiera on mierzalny wpływ na intensywność uszkodzeń rozpatrywanego systemu PE:

$$\lambda_{\text{systemuPE}} = \lambda_{\text{układ/pomiarowy}} + \lambda_{PLC} + \lambda_{\text{układ/wykonawczy}} = 18,9 \cdot 10^{-6}[\text{h}^{-1}] \tag{Z2.16}$$

Poradnik MIL-HDBK-217F opisuje uproszczoną metodę analizy nieuszkadzalności systemu złożonego z obiektów prostych. Metoda ta, polegająca na „szacowaniu niezawodności poprzez zliczanie części", zakłada, że system funkcjonuje prawidłowo, kiedy wszystkie jego elementy działają poprawnie, tzn. zakłada się *model probabilistyczny systemu o strukturze szeregowej*. W związku z tym intensywność uszkodzeń systemu λ_S wyznacza się przez sumowanie intensywności uszkodzeń λ_i poszczególnych elementów:

$$\lambda_S = \sum_{i=1}^{n} \lambda_i \tag{Z2.17}$$

Intensywność uszkodzeń systemu w analizowanym przypadku nie jest równa sumie bazowych intensywności uszkodzeń poszczególnych elementów $35 \cdot 10^{-6}$ [h^{-1}]

Ważną kwestią w analizie FMECA jest wyznaczenie częstości występowania skutków końcowych. W przypadku *braku wykonania funkcji bezpieczeństwa* częstość tę określa zależność:

$$\begin{aligned}\lambda_{\text{brak/wykonania/funkcji/bezp}} &= MR_{\textbf{IIukład/wykonawczy}} \cdot p_{\text{brak/wykonania/funkcji/bezp}} + \\ &+ MR_{\text{IIukład/pomiarowy}} \cdot p_{\text{brak/wykonania/funkcji/bezp}} + MR_{\text{IIPLCbrak/sygnału}} \cdot p_{\text{brak/ wykonania/funkcji/bezp}} + \\ &+ MR_{\text{IIPLCuszkodzenieDI}} \cdot p_{\text{brak/wykonania/funkcji/bezp}} + MR_{\text{IIPLCuszkodzeniePLC}} \cdot p_{\text{brak/wykonania/funkcji/bezp}} = \\ &= 4 \cdot 1 + 10 \cdot 1 + 2,2 \cdot 1 + 2 \cdot 1 + 0,5 \cdot 1 = 4 + 10 + 2,2 + 2 + 0,5 = 18,7 \cdot 10^{-6} [\text{h}^{-1}]\end{aligned} \tag{Z2.18}$$

Częstość *nieuzasadnionego zadziałania systemu PE/SIS* w rozpatrywanym przypadku wynosi:

$$\lambda_{\text{nieuzasadnione/zadziałanie}} = MR_{\textbf{IIPLC/niepoprawna/pracaPLC}} \cdot p_{\text{nieuzasadnione/zadziałanie}} = 0,2 \cdot 1 = 0,2 \cdot 10^{-6} [\text{h}^{-1}] \tag{Z2.19}$$

Intensywność uszkodzeń systemu $\lambda_{\text{systemuPE}}$ jest równa sumie częstości pojawiania się skutków końcowych:

$$\lambda_{\text{systemuPE}} = \lambda_{\text{brak/wykonania/funkcji/bezp}} + \lambda_{\text{nieuzasadnione/zadziałanie}} = 18,9 \cdot 10^{-6} [\text{h}^{-1}] \tag{Z2.20}$$

Na (rys. Z2.16 i Z2.17) zestawiono wyniki uzyskane z analizy FMECA przeprowadzonej dla prototypowego systemu SIS.

PFH

PFD_{avg} → SIL1

##	End Effect Name	Severity	System Failure Rate [F/10^6Hrs]	End Effect Ratio (Alpha)	End Effect Rate [F/10^6Hrs]	End Effect Ratio for Severity	End Effect Probability H=exp(-F*t)
a	b	c	d	e	f	g	h
1	Brak wykonania funkcji bezpieczeństwa	I	18.9	0.989418	18.7	1.000000	0.0185262
2	Nieuzasadnione zadziałanie	III	18.9	0.010582	0.2	1.000000	0.00019998
Total				**1.000000**	**18.9**		

Rys. Z2.16. Tablica FMECA (BQR) z zestawieniem skutków końcowych analizowanego systemu PE (SIS)

Dla rozpatrywanego układu istnieją dwa skutki końcowe na poziomie systemu: *brak wykonania funkcji bezpieczeństwa* o poziomie krytyczności I oraz *nieuzasadnione zadziałanie* o poziomie krytyczności III (raport FMECA – rys. Z2.16).

Poziomy krytyczności (*severity*) przypisuje się poszczególnym rodzajom uszkodzeń lub kolejnym analizowanym elementom (podsystemom). Mają one znaczenie miary jakościowej najgorszych potencjalnych skutków (strat) wynikających z błędu projektowego lub uszkodzenia jednostki (związanego np. z błędem systematycznym lub cyberatakiem itd.) (rys. Z2.17).

Severity	Severity Rate [F/10^6Hrs]	Ratio [%]	Severity Description
i	j	k	l
I	18.7	98.94	Catastrophic - A failure which may cause death or system loss.
II	---------	------	Critical - A failure which may cause severe injury, major property damage, or major system damage which will result in mission loss.
III	0.2	1.06	Marginal - A failure which may cause minor injury/property/system damage which will result in delay or lost of availability or mission degradation.
IV	---------	------	Minor - A failure not serious enough to cause injury, property damage, or system damage, but which will result in unscheduled maintenance or repair.
V	---------	------	User defined.
Total	**18.9**	**100.00**	-

Rys. Z2.17. Tablica FMECA (BQR) z procentowym rozkładem krytyczności

Biorąc pod uwagę skutek końcowy o najwyższym poziomie krytyczności I, jakim jest *brak wykonania funkcji bezpieczeństwa*, można stwierdzić, że prototypowy system SIS poddany analizie FMECA w trybie pracy ciągłej lub częstego przywołania do działania nie spełnia wymagań SIL (wartość *PFH* wynosi $18{,}7 \cdot 10^{-6}$ [h^{-1}]) (rys. Z2.16). Natomiast w trybie pracy rzadkiego przywołania do działania prawdopodobieństwo wystąpienia skutku końcowego *end effect probability* (kolumna h tablicy z rys. Z2.16 wraz z wynikami analizy FMECA) odpowiada przeciętnemu prawdopodobieństwu niewypełnienia funkcji bezpieczeństwa na żądanie $PFD_{avg} = 0{,}018$, zatem system SIS spełnia wymagania SIL1.

BIBLIOGRAFIA

[1] Abrahamsson M.: Uncertainty in quantitative risk analysis – characterization and methods of treatment. Department of Fire Safety Engineering. Lund University, Report 1024, Lund 2002.

[2] AIChE: Layers of protection analysis – simplified process risk assessment. Center for Chemical Process Safety, American Institute of Chemical Engineers, New York 2001.

[3] Alarm Management: White paper. Siemens AG, Industry Automation, Karlsruhe 2008.

[4] ARC White Paper, Siemens, Process Safety Systems Deliver Modern Features on a Proven Platform 2004.

[5] Barker W.C., Barker E.: Information security. Recommendation for the triple data encryption algorithm (TDEA) block cipher, NIST Special Publication, January 2012.

[6] Barlow R.E., Porschan F.: Statistical theory of reliability and life testing. Probability models. Holt, Rinehart and Winston, Inc. New York 1975.

[7] Barnert T.: Determining required safety integrity level. Journal of Polish Safety and Reliability Association 2011, Vol. 3, s. 35–43.

[8] Barnert T.: Określenie wymaganego poziomu nienaruszalności bezpieczeństwa w przemyśle procesowym. [W:] K. Kosmowski (red.): Podstawy bezpieczeństwa funkcjonalnego. Wydawnictwo Politechniki Gdańskiej. Gdańsk 2015.

[9] 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.

[10] Barnert T., Kacprzak P. Kosmowski K.T., Kozyra M., Porzeziński M., Śliwiński M., Zawalich J.: ProSIL software for computer aided functional safety management, SSARS 2011, Gdańsk 2011.

[11] Barnert T., Kosmowski K.T., Kozyra M., Porzeziński M., Śliwiński M.: Komputerowe wspomaganie procesu zarządzania bezpieczeństwem funkcjonalnym. [W:] K. Kosmowski (red.): Podstawy bezpieczeństwa funkcjonalnego. Wydawnictwo Politechniki Gdańskiej. Gdańsk 2015.

[12] Barnert T., Kosmowski K.T., Kozyra M., Porzeziński M., Śliwiński M. Opracowanie metod i narzędzi do wspomagania procesu projektowania i eksploatacji programowalnych systemów sterowania i zabezpieczeń w instalacjach przemysłowych podwyższonego ryzyka z uwzględnieniem aspektów technicznych i organizacyjnych bezpieczeństwa funkcjonalnego oraz ochrony informacji w rozproszonej sieci komputerowej. Sprawozdanie z II etapu projektu VI.B.10, CIOP-PIB, Gdańsk 2012.

[13] Barnert T., Kosmowski K.T., Śliwiński M.: A knowledge-based approach for functional safety management. Taylor & Francis Group, European Safety & Reliability Conference ESREL, Prague 2009.

[14] Barnert T., Kosmowski K., Śliwiński M., Analiza bezpieczeństwa funkcjonalnego i ochrony informacji w rozproszonych systemach komputerowych pełniących funkcje sterowania i zabezpieczeń. Pomiary, Automatyka, Kontrola 2007, t. 53, s. 130–134.
[15] Barnert T., Kosmowski K.T., Śliwiński M.: Determining and verifying the safety integrity level of the control and protection systems under uncertainty. ESREL 2008 Valencia, Taylor & Francis Group, London 2008.
[16] Barnert T., Kosmowski K.T., Śliwiński M.: Framework for RIDM within functional safety management process. Journal of Polish Safety and Reliability Association 2012, Vol. 3, No. 1–2.
[17] Barnert T., Kosmowski K.T., Śliwiński M.: Incorporating some security-related aspects in the functional safety analyses of distributed control protection systems. Proceedings of European Safety & Reliability Conference. Reliability, Risk & Safety. Taylor & Francis Group, Rhodos, Greece 2010.
[18] Barnert T., Kosmowski K.T., Śliwiński M.: Integrated functional safety and security analysis of process control and protection systems with regard to uncertainty issue. PSAM, Seattle 2010.
[19] Barnert T., Kosmowski K.T., Śliwiński M.: Security aspects in verification of the safety integrity level of distributed control and protection systems. Journal of KONBiN 2008, No. 6(3), s. 25–40.
[20] Barnert T., Kosmowski K.T, Śliwiński M.: The operation mode of a E/E/PE system and its influence on determining and verifying the safety integrity level, Journal of KONBiN 2010, No. 1(13), s. 289–298.
[21] Barnert T., Kosmowski K.T., Śliwiński M.: Uwagi dotyczące nowej roboczej wersji normy międzynarodowej IEC 61511:2014 (IEC 61511 Ed. 2: Functional safety – safety instrumented systems for the process industry sector). Gdańsk, wrzesień 2013.
[22] Barnert T., Kosmowski K.T., Śliwiński M., Porzeziński M.: Computer aided functional safety management using ProSIL system, PSAM-ESREL, Helsinki 2012.
[23] Barnert T., Piesik E., Śliwiński M.: Real-time simulator of agricultural biogas plant. Computers and Electronics in Agriculture 2014, Vol. 108, s. 1–11.
[24] Barnert T., Śliwiński M.: Bezpieczeństwo funkcjonalne i ochrona informacji w obiektach i systemach infrastruktury krytycznej – analiza i ocena. Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa. Szanse i zagrożenia, Wolters Kluwer, Warszawa 2013, s. 476–507.
[25] Barnert T., Śliwiński M.: Methods for verification safety integrity level in control and protection systems. [In:] K. Kosmowski (ed.): Functional safety management in critical systems. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk 2007, s. 171–185.
[26] Baybutt P.: An improved risk graph approach for determination of safety integrity level (SILs). Process Safety Progress 2007, Vol. 26.
[27] Bell J., Holroyd J.: Review of human reliability assessment methods, Health and Safety Laboratory for the Health and Safety Executive (HSE), Buxton, Derbyshire 2009.
[28] Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie. Wydawnictwo Naukowo Techniczne, Warszawa 2007.
[29] Białas A. (red.): Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria. Instytut Technik Innowacyjnych EMAG, Katowice 2011.

[30] Blackmore L.: IEC 61508 – Practical experience in increasing the effectiveness of SIL assessments. ISA – The Instrumentation, Systems and Automation Society 2000.
[31] Borysiewicz M., Markowski A.: Kryteria akceptowalności ryzyka poważnych awarii przemysłowych. Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, Warszawa 2002.
[32] Byczkowski M., Blim M., Zawiła-Niedźwiecki J.: TSM: Total Security Management – Zalecenia do tworzenia polityki bezpieczeństwa operacyjnego w nawiązaniu do zaleceń Komitetu Bazylejskiego. Podstawowe praktyki zarządzania i nadzoru nad ryzykiem operacyjnym. European Network Security Institute, Warszawa 2003.
[33] 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.
[34] Carlin A.S., Schurr N., Marecki J.: ALARMS: Alerting and Reasoning Management System for Next Generation Aircraft Hazards, NASA No. NNL08AA20B.
[35] CCPS: Guidelines for Chemical Process Quantitative Risk Analysis. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York 2000.
[36] CCPS: Guidelines for Consequence Analysis of Chemical Releases. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York 1999.
[37] COMAH Safety Report Assessment Manual, Part 2, Chapter 4: Major Accident Prevention Policy and Safety Management System. Poradnik oceny raportu bezpieczeństwa COMAH, część 2, rozdział 4: Polityka zapobiegania awariom i system zarządzania bezpieczeństwem, Health and Safety Executive – HSE, Issue 2.2, 2002.
[38] Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances. OJ L 10, 14 01 1997, p. 13. Tekst polski: Dyrektywa Rady 96/82/WE dotycząca zarządzania zagrożeniami poważnymi awariami z udziałem substancji niebezpiecznych. Wydawnictwo CIOP, Warszawa 1998.
[39] Cruz-Campa H.J., Cruz-Gomes M.J.: Determine SIS and SIL using HAZOPs. Wiley Interscience Publication, AIChE, 2009.
[40] CSS PNCSD Control Systems Security Program National Cyber Security Division. Common Cybersecurity Vulnerabilities in Industrial Control Systems, Centre for the Protection of National Infrastructure CPNI, US Homeland Security 2011.
[41] CSS PNCSD Control Systems Security Program National Cyber Security Division. Configuring Managing Remote Access for Industrial Control Systems. Centre for the Protection of National Infrastructure CPNI, US Homeland Security 2010.
[42] CSS PNCSD Control Systems Security Program National Cyber Security Division. Cyber Security Assessments of Industrial Control Systems. Centre for the Protection of National Infrastructure CPNI, US Homeland Security 2010.
[43] CSS PNCSD Control Systems Security Program National Cyber Security Division. Recommended Practice: Improving Industrial Control Systems Cyber security with Defense-In-Depth Strategies. Centre for the Protection of National Infrastructure CPNI, US Homeland Security, 2009.
[44] Directive 1999/92/EC of the European Parliament and of the Council of 16 December 1999 on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres (15th individual Directive within the meaning of Article 16 (1) of Directive 89/391/EEC). Official Journal of the European Communities No L 023, 28.01.2000, Brussels 2000.

[45] Directive 2003/105/EC of the European Parliament and of the Council of 16 December 2003 amending Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances [Dyrektywa Parlamentu Europejskiego i Rady 2003/105/WE z dnia 16 grudnia 2003 r. zmieniająca Dyrektywę Rady 96/82/WE dotyczącą zarządzania zagrożeniami poważnymi awariami z udziałem substancji niebezpiecznych]. OJ L 345, 31. 12. 2003, p. 97.
[46] Directive 94/9/EC of the European Parliament and of the Council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres (ATEX). Official Journal of the European Communities No L 100 of 19/04/94, Brussels 1994 (Corrigendum to Directive 94/9/EC, Official Journal of the European Communities No L 21/42, 26.01.2000).
[47] EEMUA Publication 191: Alarm Systems; A Guide to Design, Management and Procurement (Edition 2). The Engineering Equipment and Materials Users' Association, London 2007.
[48] EEMUA Publication 201: Process Plant Control Desks Utilising Human-Computer Interfaces. The Engineering Equipment and Materials Users' Association, London 2002.
[49] EMERSON Process Management: Alarm Management. DeltaV Whitepaper, Emerson 2010.
[50] EMERSON Process Management: Safety Lifecycle Workbook, For The Process Industry Sector, Emerson 2010.
[51] Ericson C.A.: Hazard analysis techniques for system safety, John Wiley & Sons, Inc. New Jersey 2005.
[52] Evans R., Tsohou A., Tryfonas T., Morgan T.: Engineering secure systems with ISO 26702 and 27001, System of Systems Engineering, 22–24 June 2010, pp. 1–6.
[53] Gertman I.D., Blackman H.S.: Human reliability and safety analysis. Data Handbook, Wiley Interscience Publication. New York 1994.
[54] Goble W.M., Cheddie H.: Safety instrumented systems verification. ISA – the Instrumentation. Research Triangle Park, Systems and Automation Society 2005.
[55] Goslin Ch.: Maritime and port security. Duos Technologies, Inc., Jacksonville 2008.
[56] Grøtan T.O.: Secure safety in remote operations. ESREL Conference, Estoril 2006.
[57] Grøtan T.O., Jaatun M.G., Line M.B. Secure safety: secure remote access to critical safety systems in offshore installations, SINTEF Technology and Society, Trondheim 2008.
[58] Grøtan T.O., Jaatun M.G., Øien K., Onhus T.: The SeSa method for assessing secure remote access to safety instrumented systems. Report No A1626, Trondheim: SINTEF Technology and Society, Safety and Reliability 2007.
[59] Gruhn P., Cheddie H.L.: Safety instrumented systems: design, analysis and justification. Research Triangle Park: ISA – The Instrumentation, Systems and Automation Society 2006.
[60] Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision making. Main Report, Office of Nuclear Regulatory Research, NUREG-1855, Vol. 1, US NRC 2009.
[61] Guidelines for safe automation of chemical processes. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York 1993.
[62] Guidelines on major accident prevention policy and safety management system, as required by Council Directive 96/82/ EC (Seveso II) – Wytyczne dotyczące polityki

zapobiegania awariom i systemu zarządzania bezpieczeństwem, zgodnie z wymaganiami Dyrektywy Rady 96/82/WE (Seveso II). Ed.: Mitchison N., Porter S., Major-Accident Hazards Bureau (MAHB), Instytut Systemów Informatycznych i Bezpieczeństwa (ISIS) Zjednoczonego Centrum Badawczego UE (JRC), EUR 18123 EN.

[63] Gulland W.G.: Methods of determining safety integrity level (SIL). Requirements – pros and cons. Springer-Verlag, Proceedings of the Safety-Critical Systems Symposium 2004.

[64] Gunn A.M.: Encyclopedia of disasters. Environmental catastrophes and human tragedies. Greenwood Press, Westport 2008.

[65] Hauge S., Håbrekke S., Lundteigen M.A.: Reliability prediction method for safety instrumented systems – PDS example collection. SINTEF A17956, SINTEF 2010.

[66] Hauge S., Hoem Å.S., Hokstad P., Håbrekke S., Lundteigen M.A.: Common cause failures in safety instrumented systems. Beta-factors and equipment specific checklist based on operational experience. SINTEF A26922, SINTEF 2015.

[67] Hauge S., Kråknes T., Håbrekke S., Jin H.: Reliability prediction method for safety instrumented systems – PDS method handbook. Edition 2013.

[68] Hauge S., Lundteigen M.A.: Guidelines for follow-up of safety instrumented systems (SIS) in the operating phase. SINTEF 2008.

[69] Hauge S., Lundteigen M.A., Hokstad P., Håbrekke S.: Reliability prediction method for safety instrumented systems – PDS method handbook, Edition 2010. SINTEF A13503, SINTEF 2010.

[70] Hauge S., Onshus T.: Reliability Data for Safety Instrumented Systems - PDS Data Handbook Edition 2010. SINTEF A13502, SINTEF 2010.

[71] Hauge S., Onshus T., Håbrekke S., Hokstad P., Lundteigen M.A.: Reliability of computer based safety systems (PDS). SINTEF 2013.

[72] Hauge S., Øien K.: Guidance for barrier management in the petroleum industry. SINTEF A27623, SINTEF 2016.

[73] Hazard analysis methodologies. A selection guide. Risk Topics, Vol. 10. Risk Engineering, Zurich 1998.

[74] Herard J., Hedberg J., Kivipuro M., Malm T., Edler H., Sjostrom H., Strawinski T.: Validation of communication in safety-critical controls system. Nordtest Tekniikantie 2003.

[75] Hildebrandt P.: Critical aspects of safety, availability and communication in the control of a subsea gas pipeline. Requirements and Solutions, HIMA 2000.

[76] Hokstad P.: A generalisation of the beta factor model. European Safety & Reliability Conference, Berlin 2004.

[77] Hokstad P.: Probability of failure on demand (PFD) – the formulas of IEC 61508 with focus on the 1oo2D voting. European Safety & Reliability Conference, ESREL 2005, Taylor & Francis Group, London 2005.

[78] Holmberg D.G.: Secure messaging in BACnet. A supplement to ASHRAE Journal. BACnet® Today 2005.

[79] Høyland A., Rausand M.: System reliability theory. Models and statistical methods. John Wiley & Sons, Inc., New York 2004.

[80] HSE, IEE & BCS: Managing competence for safety-related systems. A guidance issued by the health and safety executive, the Institution of Electrical Engineers and the British Computer Society 2006.

[81] HSE-HRA: Review of human reliability assessment methods. Research Report RR679 prepared for Health and Safety Executive 2009.
[82] HSE-R2P2: HSE's decision making process reducing risk, protecting people. Norwich: Health and Safety Executive 2001.
[83] Human reliability analysis method. U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research, Washington 2004.
[84] IAEA INSAG-15: Key practical issues in strengthening safety culture. A report by the International Nuclear Safety Group. International Atomic Energy Agency, Vienna 2002.
[85] IAEA INSAG-25: A framework for an Integrated risk informed decision making process. A report by the International Nuclear Safety Group. International Atomic Energy Agency, Vienna 2011.
[86] IAEA NSS 2011: Computer security at nuclear facilities. Reference manual. IAEA Nuclear Security Series No. 17, Technical Guidance. International Atomic Energy Agency, Vienna 2011.
[87] IEC 61882: Hazard and operability studies (HAZOP studies) – application guide. International Electrotechnical Commission, Geneva 2001.
[88] IEC 62280: Railway applications – communication, signalling and processing systems. Part 2: Safety-related communication in closed transmission systems. International Electrotechnical Commission, Geneva 2002.
[89] IEC 62443: Industrial communication networks – network and system security for industrial-process measurement and control. Parts 1–5. International Electrotechnical Commission, Geneva 2008.
[90] ISA 18.02: Management of alarm systems for the process industries. The ISA 18 Committee, CDR 11, 2009.
[91] ISA 99.00.01: Security for industrial automation and control systems. Part 1: Terminology, concepts, and models. International Society of Automation 2007.
[92] ISA/IEC 62443-3-3: Security for industrial automation and control systems, system security requirements and security levels. International Society of Automation/ International Electrotechnical Commission 2013.
[93] ISO/IEC 15408: Information technology. Security techniques — evaluation criteria for IT security. Parts 1–3. International Organization for Standardization/ International Electrotechnical Commission 2005.
[94] ISO/IEC 26702, IEEE Std. 1220-2005: Systems engineering — application and management of the systems engineering process. International Organization for Standardization/ International Electrotechnical Commission 2007.
[95] ISO/IEC 27001: Information technology. Security techniques. Information security management systems engineering process. International Organization for Standardization/ International Electrotechnical Commission 2005.
[96] ISO 31000: Risk management – principles and guidelines. International Organization for Standardization, Geneva 2009.
[97] Jaatun M.G., Grøtan T.O., Line M.B.: Secure safety: secure remote access to critical safety systems in offshore installations Autonomic and trusted computing. Springer, Berlin-Heidelberg 2008, s. 121–133.
[98] Jaatun M.G., Line M.B., Grøtan T.O.: Secure remote access to autonomous safety systems; A good practice approach. International Journal of Autonomous and Adaptive Communications System 2009, Vol. 2, s. 297–312.

[99] Johnsen S.O., Bjørkli C., Steiro T., Fartum H., Haukenes H., Ramberg J., Skriver J.: A scenario method for crisis intervention and operability analysis. SINTEF Report A4312, 2008.
[100] Karpiński M.: Bezpieczeństwo informacji, Wydawnictwo PAK, Warszawa 2012.
[101] Kirkwood D.: Developments in SIL determination. IEE Computing & Control Engineering 2005, Vol. 16, No. 3, s. 21–27.
[102] Kirwan B.: A guide to practical human reliability assessment. CRC Press LLC, London 1994.
[103] Kirwan B., Ainsworth L.K. (eds.): A guide to task analysis. CRC Press, Taylor & Francis Group, London 1992.
[104] Kletz T.: What went wrong? Case histories of process plant disasters. Gulf Professional Publishing, Huston 1999.
[105] Kosmowski K.T.: Functional safety analysis including human factors. International Journal of Performability Engineering 2011, Vol. 7, No. 1, s. 61–76.
[106] Kosmowski K.T.: Functional safety analysis including human factors. Proceedings of the Third Summer Safety & Reliability Seminars 2009. ESRA-PSRA, Gdańsk–Sopot, July 19–25 2009, Vol. 2, s. 251–263.
[107] Kosmowski K.T.: Functional safety and reliability analysis methodology for hazardous industrial plants. Gdańsk University of Technology Publishers, Gdańsk 2013.
[108] Kosmowski K.T.: Functional safety and security management in critical systems. TEHOSS, Gdańsk 2005, s. 323–332.
[109] Kosmowski K.T.: Functional safety concept for hazardous system and new challenges. Journal of Loss Prevention in the Process Industries 2006, Vol. 19, s. 298–305.
[110] Kosmowski K.T.: Functional safety in the context of risk appraisal criteria and cost-benefit analysis., Functional Safety Management in Critical Systems, Gdańsk 2006.
[111] Kosmowski K.T.: Metodyka analizy ryzyka w zarządzaniu niezawodnością i bezpieczeństwem elektrowni jądrowych. Seria: Monografie 33. Wydawnictwo Politechniki Gdańskiej, Gdańsk 2003.
[112] Kosmowski K.T.: Rozwój techniki i problemy zarządzania bezpieczeństwem. Politechnika Gdańska, Gdańsk 2004.
[113] Kosmowski K.T. (ed.): Functional safety management in critical systems. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk 2007.
[114] Kosmowski K.T. (ed.). Podstawy bezpieczeństwa funkcjonalnego. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk 2013.
[115] Kosmowski K.T., Barnert T., Śliwiński M., Porzeziński M.: Functional safety assessment within the risk informed decision making process. Proceedings of Joint American and European Conference PSAM 11/ ESREL 2012, Helsinki 2012.
[116] Kosmowski K.T., Porzeziński M.: Bezpieczeństwo funkcjonalne i ochrona informacji w obiektach i systemach infrastruktury krytycznej – wymagania i kryteria. [W:] A.R. Pach, Z. Rau, M. Wągrowski (red. nauk.): Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa – szanse i zagrożenia. LEX a Wolters Kluwer business, Warszawa 2013.
[117] Kosmowski K.T., Śliwiński M.: Analiza integralności obiektów i instalacji rozproszonych w strefie nadmorskiej zorientowana na zarządzanie ryzykiem. VII Międzynarodowa Konferencja Zarządzanie Kryzysowe 2009 – bezpieczeństwo i ochrona portów morskich oraz miast portowych. Akademia Marynarki Wojennej, Gdynia 2009.

[118] Kosmowski K., Śliwiński M.: Knowledge-based functional safety and security management in hazardous industrial plants with emphasis on human factors. Advanced Systems for Automation and Diagnostics. Pomeranian Science and Technology Publishers, Gdańsk 2015, s. 81–96.
[119] Kosmowski K., Śliwiński M.: Organizational culture as prerequisite of proactive safety and security management in critical infrastructure systems including hazardous plants and ports. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars 2016, Vol. 7, No. 1.
[120] Kosmowski K.T., Śliwiński M., Barnert T.: Functional safety and security assessment of the control and protection systems. Proceedings of European Safety & Reliability Conference – ESREL. Taylor & Francis Group, London 2006.
[121] Kosmowski K.T., Śliwiński M., Barnert T.: Methodological aspects of functional safety assessment. Journal of Machines Operation and Maintenance 2006, Vol. 41, Z4 (148), s. 159–176.
[122] Kosmowski K.T., Śliwiński M., Gołębiewski D., Piesik E.: Procedure based proactive functional safety management for the risk mitigation of hazardous events in the oil port installations including insurance aspects. Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars 2016, Vol. 7, No. 1.
[123] Kosmowski K.T., Śliwiński M., Piesik J.: Czynniki ludzkie w analizie bezpieczeństwa funkcjonalnego. Materiały konferencji naukowo-technicznej Zarządzanie Bezpieczeństwem Funkcjonalnym. Gdańsk–Jurata, 16–18 września 2004.
[124] Kosmowski K.T., Śliwiński M., Zabielski A.: Obliczanie wartości PFD dla funkcji bezpieczeństwa obwodu SIS o różnych konfiguracjach. Materiały konferencji naukowo-technicznej Zarządzanie Bezpieczeństwem Funkcjonalnym. Gdańsk–Jurata 16–18 września 2004.
[125] Krawczyk P.: Struktura i historia protokołu IPSec. Bezpieczeństwo IT. Marzec 2001.
[126] Kumamoto H.: Satisfying safety goals by probabilistic risk assessment. Springer Series in Reliability Engineering, Springer, London 2007.
[127] Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. PWN, Warszawa 2008.
[128] Liderman K.: Bezpieczeństwo informacyjne. PWN, Warszawa 2012.
[129] Lumbe Aas A., Skramstad T.: A case study of ISO 11064 in control centre design in the Norwegian petroleum industry. Applied Ergonomics 2010, 42, s. 62–70.
[130] Malm T., Kivipuro M., Hérard J., Bøegh J.: Validation of safety-related wireless machine control systems. Technical Report, Nordic Innovation Centre 2007.
[131] Marszal E.M., Weil Ch.P.: Implementing protective functions in BPCS and combined systems. Kenexis Consult. Corporation, Columbus, USA 2011.
[132] McLeod R.: Human factors assessment model validation study. Prepared by Nickleby HFE Ltd for the Health and Safety Executive. HSE, Reseach Raport 194, 2004.
[133] Michalik J.S.: Legislation and research questions concerning the safety management in the context of major accident control. [In:] K.T. Kosmowski (ed.): Functional safety management in critical systems. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk 2007.
[134] Michalik J.S.: Zapobieganie poważnym awariom przemysłowym. Zalecenia i wytyczne dla zakładów dużego ryzyka. Główny Inspektorat Pracy, Warszawa 2005.
[135] Milstein R.I.: Integrated safety analysis guidance document. U.S. Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards, Washington 2001.

[136] Missala T.: Analiza wymagań i metod postępowania przy ocenie ryzyka i określaniu wymaganego poziomu nienaruszalności bezpieczeństwa. Seria wydawnicza Monografie – Studia – Rozprawy. Wydawnictwo Oficyna Wydawnicza PIAP, Warszawa 2009.
[137] Missala T.: Księga procedur do oceny zgodności bezpieczeństwa funkcjonalnego w przemyśle procesowym. Seria wydawnicza Monografie – Studia – Rozprawy. Wydawnictwo Oficyna Wydawnicza PIAP. Warszawa 2010.
[138] Moskowitz R.: Weakness in passphrase choice in WPA interface, WNN Wi-FI Net News, November 2003.
[139] Musgrave G., Larsen A., Sgobba T.: Safety design for space systems, Elsevier 2009.
[140] Nait-Said R., Zidani F., Ouzraoui N.: Fuzzy risk graph model for determining safety integrity level. International Journal of Quality, Statistics, and Reliability 2008, Hindawi Publishing Corporation, Volume 2008, Article ID 263895, s. 1–12.
[141] NASA: NASA risk-informed decision making handbook. Office of Safety and Mission Assurance. NASA Headquarters 2010.
[142] National Institute of Standards and Technology: ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, November 2001.
[143] National Institute of Standards and Technology: DATA ENCRYPTION STANDARD (DES), Federal Information Processing Standards Publication 46-3, October 1999.
[144] National Institute of Standards and Technology: DIGITAL SIGNATURE STANDARD (DSS), Federal Information Processing Standards Publication 186, May 1994.
[145] OECD: Wytyczne OECD w zakresie bezpieczeństwa systemów i sieci informatycznych – w kierunku kultury bezpieczeństwa. OECG 1992/1997.
[146] OECD EHS: Guidance on safety performance indicators. OECD Environment, Health and Safety Publications, Series on Chemical Accidents 2005, No 11.
[147] OECD EHSP: Guiding principles for chemical accidents prevention, preparedness and response. OECD Environment, Health and Safety Publications, Series on Chemical Accidents 2003, No 10.
[148] OECD IFP: Project on future global shocks. Reducing systemic cybersecurity risk. IFP/ WKP/ FGS 2011.
[149] OECD PCI: Protection of „critical infrastructure" and the role of investment policies relating to national security. Organization for Economic Co-operation and Development, Paris 2008.
[150] OREDA: Offshore reliability data handbook (5^{th} ed.). SINTEF Industrial Management. Prepared by SINTEF, Trondheim 2009.
[151] Ormos L., Ajtonyi I.: Soft computing method for determining the safety of technological system by IEC 61508. Proceedings of the 1^{st} Romanian-Hungarian Joint Symposium on Applied Computational Intelligence (SACI '04). Timisoara, Rumunia 2004.
[152] Øien K., Hauge S., Størseth F., Tinmannsvik R.K.: Towards a holistic approach for barrier management in the petroleum industry. SINTEF A26845, SINTEF 2015.
[153] Petersen S., Aakvaag N.: Wireless instrumentation for safety critical systems, technology, standards, solutions and future trends. SINTEF A26762, SINTEF 2015.
[154] Piesik E., Kosmowski K., Śliwiński M.: Analiza niezawodności człowieka ramach funkcji związanych z bezpieczeństwem w przykładowej instalacji. Advanced Sys-

tems for Automation and Diagnostics, Pomeranian Science and Technology Publishers, Gdańsk 2015, s. 167–178.
[155] Piesik E., Śliwiński M., Barnert T.: Determining and verifying the safety integrity level of the safety instrumented systems with the uncertainty and security aspects. Reliability Engineering & System Safety 2016, nr 152, s. 259–272.
[156] Piwowar J., Châtelet E., Laclémence P.: An efficient process to reduce infrastructure vulnerabilities facing malevolence. Reliability Engineering & System Safety 2009, Vol. 94, s. 1869–1877.
[157] PN-EN 15233: Metodyka oceny bezpieczeństwa funkcjonalnego systemów ochronnych do przestrzeni zagrożonych wybuchem. Polski Komitet Normalizacyjny 2009.
[158] PN-EN 50402: Elektryczne przyrządy do wykrywania i pomiaru gazów palnych lub toksycznych oraz par albo tlenu Wymagania dotyczące bezpieczeństwa funkcjonalnego stacjonarnych systemów detekcji gazu. Polski Komitet Normalizacyjny 2007.
[159] PN-EN 61131: Sterowniki programowalne. Część 6. Bezpieczeństwo funkcjonalne. Polski Komitet Normalizacyjny 2013.
[160] PN-EN 61158: Przemysłowe sieci komunikacyjne – specyfikacje magistrali miejscowej. Części 1–6. Polski Komitet Normalizacyjny 2011.
[161] PN-EN 61508: Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem. Części 1–7. Polski Komitet Normalizacyjny 2010.
[162] PN-EN 61511: Bezpieczeństwo funkcjonalne. Przyrządowe systemy bezpieczeństwa do sektora przemysłu procesowego. Części 1–3. Polski Komitet Normalizacyjny, lipiec 2017.
[163] PN-EN 61784-1: Przemysłowe sieci komunikacyjne – profile. Część 1. Profile magistrali miejscowej. Polski Komitet Normalizacyjny 2011.
[164] PN-EN 61784-2: Przemysłowe sieci komunikacyjne – profile. Część 2. Profile dodatkowe magistrali miejscowej do sieci czasu rzeczywistego oparte o ISO/IEC 8802−3. Polski Komitet Normalizacyjny 2011.
[165] PN-EN 61784-3: Przemysłowe sieci komunikacyjne – profile. Część 3. Magistrale miejscowe bezpieczne funkcjonalnie – ogólne zasady i definicje profili. Polski Komitet Normalizacyjny 2011.
[166] PN-EN 62061: Bezpieczeństwo maszyn. Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i elektronicznych programowalnych systemów sterowania związanych z bezpieczeństwem. Polski Komitet Normalizacyjny 2008.
[167] PN-EN ISO 9001: Systemy zarządzania jakością. Wymagania. Polski Komitet Normalizacyjny 2009.
[168] PN-EN ISO 11064-7: Ergonomiczne projektowanie centrów sterowania. Część 7. Zasady oceny centrów sterowania. Polski Komitet Normalizacyjny 2006.
[169] PN-EN ISO 14001: Systemy zarządzania środowiskowego. Wymagania i wytyczne stosowania. Polski Komitet Normalizacyjny 2009.
[170] PN-IEC 60300-3-9: Analiza ryzyka w systemach technicznych. Polski Komitet Normalizacyjny 1999.
[171] PN-ISO/IEC 17779: Technika informatyczna – techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji. Polski Komitet Normalizacyjny 2007.
[172] PN-ISO/IEC 27000: Technika informatyczna – techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia. Polski Komitet Normalizacyjny 2012.

[173] Porzeziński M., Redlarski G., Śliwiński M.: Industrial computer networks functional safety. [In:] Functional safety management in critical systems. Fundacja Rozwoju Uniwersytetu Gdańskiego, Gdańsk 2007, s. 271–288.
[174] Process Safebook 1: Functional safety in the process industry. Principles, standards and implementation. Rockwell Automation 2013.
[175] Projekt 5.R.02: Opracowanie metod analizy i narzędzi do komputerowo wspomaganego zarządzania bezpieczeństwem funkcjonalnym w ramach systemu warstw zabezpieczeniowo-ochronnych obiektów przemysłowych podwyższonego ryzyka, Opracowania końcowe etapów I, II i III/ Gdańsk 2008, 2009, 2010.
[176] Projekt VI.B.10: Opracowanie metod i narzędzi do wspomagania procesu zarządzania bezpieczeństwem funkcjonalnym i ochroną informacji w programowalnych systemach sterowania i zabezpieczeń z uwzględnieniem czynników ryzyka. Opracowania końcowe etapów I, II i III. Gdańsk 2011, 2012, 2013.
[177] Rasmussen J., Svedung I.: Proactive risk management in a dynamic society.Swedish Rescue Services Agency, Karlstad 2000.
[178] Reason J.: Human error. Cambridge University Press 1990.
[179] RFC 1321, The MD5 Message-Digest Algorithm 1992.
[180] RFC 2104, HMAC: Keyed-Hashing for Message Authentication 1997.
[181] RFC 3174, US Secure Hash Algorithm 1 (SHA1) 2001.
[182] RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, 2008.
[183] Rivest R.L., Shamir A., Adleman L.: A method for obtaining digital signatures and public-key cryptosystems, communication. ACM 21, Feb 1978, s. 120–126.
[184] Roos C.J., Myers P.E.: The engineer's guide to overfill prevention. Emerson Process Management. Emerson 2015.
[185] Rothenberg D.H.: Alarm management for process control. Momentum Press, LLC, New York 2009.
[186] Rypkema J.A., Neerincx M.A., Passenier P.O.: PRISM – Best practice guide human factors in high-demand situations for the process industries. TNO Human Factors, Soesterberg, The Netherlands 2004.
[187] SESAMO.: Integrated design and evaluation methodology. Security and safety modelling. Artemis JU Grant Agr. no. 2295354, 2014.
[188] Schneider Electric: Pipeline management solution an integrated solution for pipeline operators, Schneider Electric 2004.
[189] Simon C., Sallak M., Aubry J.: SIL allocation of SIS by aggregation of experts' opinions, Proceedings of the Safety and Reliability Conference (ESREL '07), Stavanger 2007.
[190] Smith D., Simpson K.: Functional safety, 2nd ed. A straightforward guide to applying IEC 61508 and related standards. Elsevier, Oxford 2004.
[191] SPAR-H: Human Reliability Analysis (HRA) Method, NUREG/CR-6883, INL/EXT-05-00509, USNRC 2005.
[192] Stavrianidis P.: Reliability and uncertainty analysis of hardware failures of programmable electronic system. Reliability Engineering and System Safety 1992, 39, s. 309–324.
[193] Summers A.: Techniques for assessing a target safety integrity level. ISA Transactions 37. Elsevier 1998.
[194] Swain A.D., Guttmann H.E.: Handbook of human reliability analysis with emphasis on nuclear power plant application. NUREG/CR-1278, 1983.

[195] Śliwiński M.: Designing control and protection systems with regard to functional safety aspects. IEEE International Conference on Technologies for Homeland Security and Safety, TEHOSS 2005, Gdańsk 2005.
[196] Śliwiński M.: Implementacja metod weryfikacji poziomów nienaruszalności SIL z uwzględnieniem aspektów ochrony informacji w aplikacji ProSIL-EAL. Zadanie B III etapu projektu VI.B.10, CIOP-PIB, Warszawa 2013.
[197] Śliwiński M.: Integrity level verification for safety-related functions. Journal of Polish Safety and Reliability Association 2011, Vol. 3.
[198] Śliwiński M.: Metody analizy systemów sterowania i zabezpieczeń z uwzględnieniem kryteriów bezpieczeństwa funkcjonalnego. Politechnika Gdańska, Gdańsk 2006.
[199] Śliwiński M.: Weryfikacja poziomu nienaruszalności funkcji związanych z bezpieczeństwem. Podstawy bezpieczeństwa funkcjonalnego. Wydawnictwo Politechniki Gdańskiej, Gdańsk 2015.
[200] Śliwiński M., Barnert T., Piesik E.: Weryfikacja poziomów nienaruszalności bezpieczeństwa z uwzględnieniem aspektów ochrony informacji. ZNWEiA PG Nr 40, Gdańsk 2014.
[201] Śliwiński M., Barnert T., Piesik E.: Wspomagana komputerowo weryfikacja poziomu nienaruszalności bezpieczeństwa z wykorzystaniem autorskiej aplikacji ProSIL, ZNWEiA PG nr 36, Gdańsk 2013.
[202] Śliwiński M., Kosmowski K.T., Piesik E.: Verification of the safety integrity levels with regard of information security issues: advanced systems for automation and diagnostics. PWNT, Gdańsk 2015.
[203] Śliwiński M., Piesik E.: Determining and verifying the safety integrity level with security aspects. [In:] W. Mitkowski et al. (ed.): Trends in advanced intelligent control, optimization and automation. Springer 2017.
[204] Śliwiński M., Piesik E.: Procedure based functional safety and information security management of industrial automation and control systems on example of the oil port installations. Journal of Polish Safety and Reliability Association 2017, Vol. 8, No. 1, s. 129–138.
[205] Ten Chee-Wooi T., Chen-Ching L., Govindarasu M.: Vulnerability assessment of cybersecurity for SCADA systems using attack trees. IEEE Power Engineering Society General Meeting 2007.
[206] Timms C.R.: Achieving ALARP with safety instrumented systems. Asset Integrity Management Limited. Riverview Business Centre, Aberdeen 2007.
[207] US-CERT, Control Systems Security Program (CSSP). Overview of cyber vulnerabilities (http://www.us-cert.gov/control_systems/csvuls.html) [dostęp: listopad 2016].
[208] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dz.U. z 2017 r., poz. 209.
[209] White paper, architecture for secure SCADA and distributed control system networks 2010.
[210] Wojas M., Kosmowski K.T., Kościelny J.M.: System certyfikacji osób odpowiedzialnych za bezpieczeństwo funkcjonalne. Journal of Polish Safety and Reliability Association, 2011, Vol. 3, s. 125–133.
[211] Wright M., Turner D., Horbury C.: Competence assessment for the hazardous industries. Prepared by Greenstreet Berman Ltd for the Health and Safety Executive. HSE 2003.

[212] Załącznik do sprawozdania z II etapu realizacji projektu VI.B.10: Wytyczne i zalecenia metodyczne do wspomagania analizy i oceny rozwiązań ochrony informacji w programowalnych systemach sterowania i zabezpieczeń z uwzględnieniem czynników ryzyka. Gdańsk, styczeń 2013.

BEZPIECZEŃSTWO FUNKCJONALNE I OCHRONA INFORMACJI W OBIEKTACH I SYSTEMACH INFRASTRUKTURY KRYTYCZNEJ

W monografii przedstawiono aktualną problematykę związaną z analizą bezpieczeństwa funkcjonalnego rozproszonych systemów sterowania i automatyki zabezpieczeniowej w obiektach i systemach infrastruktury krytycznej, wykorzystujących przemysłową sieć komputerową, z uwzględnieniem zagadnień ochrony informacji. W obiektach tego typu systemy sterowania i automatyki zabezpieczeniowej są projektowane jako systemy rozproszone, których nieprawidłowe działanie może prowadzić do poważnych skutków, np.: skażenia środowiska, pożaru, wybuchu, utraty zdrowia i życia osób, spadku lub załamania produkcji, a w konsekwencji znacznych strat ekonomicznych. Zagadnienia bezpieczeństwa funkcjonalnego i ochrony informacji powinny być zatem rozpatrywane w sposób zintegrowany, w zależności od rodzaju kanałów komunikacji stosowanych w transmisji danych pomiędzy elementami systemu. Zagadnienia związane z zarządzaniem bezpieczeństwem funkcjonalnym systemów sterowania i automatyki zabezpieczeniowej są zawarte w normie PN-EN 61508 o charakterze ogólnym (dotyczącej różnych zastosowań) oraz w normach sektorowych, np. PN-EN 61511, opracowanej dla potrzeb przemysłu procesowego i wydobywczego. Ogólne wymagania dotyczące zagadnień ochrony informacji w opisywanych systemach są zawarte w normach międzynarodowych ISO/IEC 15408, PN-ISO/IEC 17779, PN-ISO/IEC 27001 oraz IEC 62443. Normy te dotyczą różnych aspektów bezpieczeństwa systemów komputerowych i ochrony informacji. W niniejszej monografii omówiono konwencjonalne podejście do oceny bezpieczeństwa funkcjonalnego oraz nowe, integrujące aspekty bezpieczeństwa funkcjonalnego, a także czynniki związane z ochroną informacji w cyklu życia bezpieczeństwa systemów sterowania i automatyki zabezpieczeniowej obiektów i systemów infrastruktury krytycznej. Zaprezentowano całościowe podejście do formułowania wymagań i kryteriów, z uwzględnieniem aspektów *safety* i *security* w analizie zagrożeń i ocenie ryzyka.

W monografii przedstawiono także zagadnienia związane z etapem analizy i oceny ryzyka obiektu technicznego podwyższonego ryzyka. Opisano metody określania wymagań SIL dla zidentyfikowanych funkcji bezpieczeństwa. Funkcje takie są realizowane przez systemy E/E/PE (BPCS i/lub SIS) i stanowią część systemu bezpieczeństwa składającego się z wielu warstw zabezpieczeniowo-ochronnych. Zarówno w metodach jakościowych, jak i półilościowych wyznaczenie wymaganego SIL opiera się na kilku podstawowych parametrach ryzyka. Są one związane z częstością występowania zdarzenia awaryjnego oraz jego potencjalnymi konsekwencjami. W związku z tym, że systemy techniczne są coraz częściej budowane na bazie architektury rozproszonej, pojawiają się nowe zagrożenia, które do tej pory nie były uwzględniane w analizach ryzyka. Mogą one mieć wpływ na zwiększenie częstości występowania zdarzeń i scenariuszy awaryjnych, jak również mogą zwiększać prawdopodobieństwo niewypełnienia funkcji związanej z bezpieczeństwem na przywołanie. Oba te zagadnienia powinny być uwzględniane w procesie przypisania wymaganego poziomu nienaruszalności bezpieczeństwa SIL do funkcji bezpieczeństwa.

W niniejszej monografii zaproponowano rozszerzenie stosowanych obecnie metod o aspekty związane z uwzględnieniem stopnia ochrony informacji systemu technicznego. Przedstawiono także zastosowanie metod weryfikacji SIL z uwzględnieniem zagadnień

ochrony informacji, m.in. przez wykorzystanie w tym procesie poziomów uzasadnionego zaufania EAL, poziomów uzasadnionej ochrony SAL lub przypisanie analizowanemu systemowi stopnia ochrony informacji na podstawie liczby pierścieni zabezpieczeniowo-ochronnych wg metodyki SeSa – SINTEF, wraz z uwzględnieniem klasyfikacji systemów rozproszonych. Metody te zaimplementowano w module weryfikacji SIL autorskiego oprogramowania ProSIL-EAL.

FUNCTIONAL SAFETY AND INFORMATION SECURITY IN THE CRITICAL INFRASTRUCTURE SYSTEMS AND OBJECTS

In this monography the current functional safety analysis issue connected with information security aspects is presented. It relates to the distributed control and protection systems in critical infrastructures which consist of different types industrial computer networks. Incorrect work of such distributed systems may be a cause of critical consequences like environment contamination, fires, explosions, loose of people health or deaths, production breakdowns and serious economical loses. Therefore the aspects of functional safety and security analyses should be treated together, in case of type of communication channel used between system's elements. The functional safety aspects are described in normative documents PN-EN 61508 (in general) and PN-EN 61511 (process industry and mining). The general requirements for security are described in international standards like ISO/IEC 15408, PN-ISO/IEC 17779, PN-ISO/IEC 27001 and IEC 62443. This monography presents both a conventional functional safety assessment approach and a new one taking into account security factors in the whole safety lifecycle of the control, monitoring and protection systems in critical infrastructures. An integrated approach to formulating the requirements and criteria taking into account aspects of safety and security in the hazard analysis and risk assessment is outlined.

This monography presents the issues related to the risk assessment process of a technical object. It describes methods for determining the safety integrity requirements (SIL) for the identified safety functions. Such functions are performed by the E/E/PE (BPCS and/or SIS) system, and are part of the safety-related system included in the layers protection concept. A required SIL determination using the methods based on qualitative and semi-quantitative analysis are related to several basic parameters of risk. They are associated with the frequency of occurrance of a dangerous event and its potential consequences. Due to the fact that more technical systems are build based on distributed architecture, there are some new threats that have not yet been taken into account in the risk analysis. They can affect both the increse in the incidence of events and risk scenarious, and can increse the probability of failure of safety-related functions for reference. Both of these issues should be taken into acount in the assigment of the required safety integrity level for the safety-related functions. The monography proposes extension of the currently used methods of functional safety analyses. It can be done with inclusion of the level of information security assigned to the technical system.

The monography addresses some important issues of the functional safety analysis, namely the safety integrity level (SIL) verification, based on so called evaluation assurance level (EAL), security assurance level (SAL) and Secure Safety (SeSa) methodology, is presented. In this monography is described a prototyle ProSIL and ProSIL-EAL software system for computer aided functional safety management. In ProSIL-EAL the methods (e.g. veryfying the safety integrity level SIL of safety instrumented function SIF) concerning functional safety analysis in the process of the design and operation safety instrumented systems (SIS) with security aspects are implemented according to PN-EN 61508, PN-EN 61511, ISO/IEC 15408 standards and SeSa – SINTEF methodology.

WYDAWNICTWO POLITECHNIKI GDAŃSKIEJ

Wydanie I. Ark. wyd. 14,9, ark. druku 13,75, 171/1010

Druk i oprawa: Volumina.pl Daniel Krzanowski
ul. Księcia Witolda 7-9, 71-063 Szczecin, tel. 91 812 09 08