MARCIN ŚLIWIŃSKI

BEZPIECZEŃSTWO FUNKCJONALNE I OCHRONA INFORMACJI W OBIEKTACH I SYSTEMACH INFRASTRUKTURY KRYTYCZNEJ

GDAŃSK 2018

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.