dr MIECZYSŁAW J. BORYSIEWICZ*
prof. dr hab. inż. JERZY S. MICHALIK
Centralny Instytut Ochrony Pracy
– Państwowy Instytut Badawczy

Cyberbezpieczeństwo przemysłowych systemów sterowania

Jednym z istotnych zagadnień zarządzania bezpieczeństwem instalacji chemicznych w aspekcie ochrony przed działaniami terrorystycznymi i sabotażowymi jest zapewnienie cyberbezpieczeństwa systemów informatycznych wykorzystujących sieci komputerowe. W artykule przedstawiono informacje o opracowaniach zawierających wytyczne i zalecenia dotyczące cyberbezpieczeństwa, omówiono zasady cyberbezpieczeństwa w odniesieniu do przemysłowych systemów sterowania (ICS – Industrial Control Systems), w szczególności zagadnienia stosowania systemowego profilu ochrony (SPP). Ważnym instrumentem oceny i zapewnienia bezpieczeństwa ICS jest metodyka STOE (System Target of Evaluation – systemowy cel oceny). Przedstawiono zakres STOE, rodzaje podatności i zabezpieczeń oraz założenia dotyczące bezpiecznego użytkowania ICS.

Cybersecurity of industrial control systems
Assurance of cybersecurity of informatics systems using computer networks is an important aim of chemical installations safety management in the context of protection against terrorist or sabotage acts. The article presents and discusses information on published documents containing the guidelines and recommendations concerning cybersecurity, and the principles of cybersecurity of the Industrial Control Systems (ICSs), especially application of the System Protection Profile (SPP). Also discussed is the System Target of Evaluation method (STOE), a very important tool for assessing assuring ICS's security, its scope, vulnerabilities, protection measures as well as the assumptions for secure use of ICSs.

Współczesne technologie przemysłu chemicznego, które czynią operacje procesowe i procesy wytwarzania bardziej efektywnymi, mogą być podatne na nowe zagrożenia. Przemysł chemiczny musi być odpowiednio przygotowany w celu przeciwdziałania takim zagrożeniom, w szczególności zagrożeniom związanym z naruszeniem cyberbezpieczeństwa.

Poza bezpieczeństwem procesowym instalacji chemicznych, na które mają wpływ również zagrożenia od niepożądanych działań stron trzecich (terroryzm, sabotaż), istnieją jeszcze dwa obszary zagadnień, które należy rozważyć w przypadku analiz zagrożeń wynikających z takich działań. Są to: bezpieczeństwo transportu materiałów (surowców i produktów) oraz bezpieczeństwo systemów sterowania, zabezpieczeń, przetwarzania i dostępu do ważnych informacji, nazywane cyberbezpieczeństwem.

Redukcja zagrożeń dla cyberbezpieczeństwa wymaga stosowania kombinacji zaawansowanych technologii z uwzględnieniem praktyk akceptowanych przez sektor chemiczny [1-4]. Ważnym zadaniem jest również upowszechnianie informacji dotyczących takich rozwiązań.

* Miejsce stałego zatrudnienia: Instytut Energii Atomowej, Centrum Doskonałości MANHAZ, Otwock-Świerk

Działania w celu zapewnienia cyberbezpieczeństwa

Organizacje w coraz większym stopniu polegają na systemach wykorzystujących sieci komputerowe. W ten sposób mogą utracić kontrolę nad przetwarzaniem informacji, które dawniej było wykonywane w tradycyjnych centrach przetwarzania danych. W tej sytuacji staje się bardzo istotne, aby przedsiębiorstwa rozumiały naturę ryzyka dotyczącego bezpieczeństwa. Należy podkreślić, że w odniesieniu do bezpieczeństwa systemów komputerowych występują pewne unikalne problemy, które należy zrozumieć w celu bardziej efektywnego wdrożenia środków bezpieczeństwa.

W związku ze znaczeniem problemu dla praktyki powstaje coraz więcej opracowań o charakterze wytycznych wspomagających wdrażanie rozwiązań mających na celu zapewnienie odpowiedniego poziomu cyberbezpieczeństwa systemów. Należy odnotować tu intensywne działania prowadzone w tym obszarze przez różne instytucje w USA oraz przez międzynarodowe organizacje, stowarzyszenia i zespoły. Główny wysiłek koncentruje się na ujednoliconych kryteriach ocen i zasadach zapewnienia cyberbezpieczeństwa oraz na problematyce powiązania cyberbezpieczeństwa z ogólnym bezpieczeństwem systemów, w tym systemów technologicznych. W dalszej części tej publikacji zostaną omówione reprezentatywne – zdaniem autorów – problemy i osiągnięcia w tej dziedzinie.

Stowarzyszenie ISA (*Instrumentation, Systems and Automation Society*) w celu analiz problematyki wynikającej z zagrożeń bezpieczeństwa systemów przemysłowych, bezpieczeństwa w rozumieniu nie *safety*, a słowa *security* (ochrona), ustanowiło komitet SP99. W tym artykule słowo „bezpieczeństwo" będzie się odnosiło właśnie do tak rozumianej koncepcji bezpieczeństwa, obejmującej środki ochrony i zapobiegania zagrożeniom związa-

nym z atakami, aktami terroru czy sabotażem. Celem SP99 jest rozpoznanie potrzeb systemów wytwarzania oraz sterowania i zabezpieczeń. Komitet SP99 koncentruje się na opracowaniu materiałów, które wspomagają organizacje w przygotowaniu zaawansowanych rozwiązań w zakresie bezpieczeństwa. Dwa pierwsze raporty, które wydał ten komitet to: *Technologie bezpieczeństwa dla systemów wytwarzania, sterowania i zabezpieczeń* (ISA-TR99.00.01--2004), znane jako TR1, oraz *Zintegrowanie bezpieczeństwa elektronicznego ze środowiskiem systemów wytwarzania, sterowania i zabezpieczeń* (ISA-TR99.00.02-2004), znane jako TR2.

TR1 opisuje elektroniczne technologie bezpieczeństwa dostępne dla systemów wytwarzania oraz sterowania i zabezpieczeń. Zbadano dwadzieścia osiem technologii w kontekście takich kategorii zagadnień, jak: uwierzytelnianie i autoryzacja; filtrowanie, blokowanie, kontrola dostępu; utajnianie/kodowanie i walidacja danych; audyty, pomiary, monitorowanie; narzędzia detekcji oraz kontrola oprogramowania komputerowego i bezpieczeństwa fizycznego.

TR2 zawiera bardziej zaawansowane metodologie i elementy niezbędne do zbudowania pełnego programu w zakresie bezpieczeństwa. W zakresie objętym TR2, SP99 wprowadza pojęcie cyklu życia bezpieczeństwa. TR2 podaje specyficzne wytyczne i referencje dla każdego kroku cyklu bezpieczeństwa.

Na początku lat 80. w USA zostały opracowane kryteria o nazwie: *Trusted Computer System Evaluation Criteria* – TCSEC (*Kryteria ewaluacji wiarygodności systemów komputerowych*). W następnej dekadzie szereg krajów podjęło próby opracowania własnych kryteriów bazujących na TCSEC, które nadążałyby za szybko rozwijającymi się technologiami informatycznymi (IT). W Europie wersja 1.2 dokumentu *Information Technology Security Evaluation Criteria* – ITSEC (*Kryteria ocen cyberbezpieczeństwa*) została opublikowana w roku 1991 jako opracowanie zespołów z Francji, Niemiec, Holandii i Zjednoczonego Królestwa. W Kanadzie w 1993 r. została opublikowana wersja 3.0 dokumentu: *Canadian Trusted Computer Product Evaluation Criteria* – CTCPEC (*Kanadyjskie kryteria ewaluacji wiarygodności systemów komputerowych*). Była to kombinacja podejść zastosowanych w TCSEC i ITSEC.

Organizacje zaangażowane w opracowanie kolejnych wersji dokumentów dotyczących wytycznych znanych pod nazwą *Common Criteria* (CC – *Wspólne kryteria*) współpracowały z Międzynarodową Organizacją Normalizacyjną ISO. W wyniku tych działań wersja 2.1 CC została uznana za normę ISO 15408*.

* http://isotc.iso.org/livelink/livelink/fetch/2000/2489/Ittf_Home/PubliclyAvailableStandards.htm

Ogólne zasady bezpieczeństwa systemów sterowania i bezpieczeństwa procesowego

System sterowania stosowany w przemyśle (*Industrial Control System* – ICS) jest skomputeryzowanym systemem używanym do sterowania procesami przemysłowymi i funkcjami fizycznymi. ICS automatyzuje funkcje sterowania, umożliwiając kontrolę szybszych, większych i bardziej złożonych procesów. ICS i sprzężone z nim systemy zapewniają bezpieczne i akceptowalne dla środowiska działania określonych procesów przemysłowych. Szczególnym przykładem ICS są przyrządowe programowalne systemy bezpieczeństwa SIS (*Safety Instrumented System*). W kontekście bezpieczeństwa procesowego przy wykorzystaniu koncepcji bezpieczeństwa funkcjonalnego są one przedmiotem normy IEC 61511 (w Polsce jest to obecnie norma PN-EN 61511). Kwestie te nie są jednakże rozpatrywane w tej publikacji, która dotyczy problematyki bezpieczeństwa w sensie ochrony (*security*).

Ogólne postrzeganie zagrożeń bezpieczeństwa ICS wiąże się zazwyczaj z próbami niepożądanych działań stron trzecich, mających na celu spowodowanie zakłóceń w określonych operacjach procesu przemysłowego (np. doprowadzenie do przestoju w dostarczaniu mocy) lub wywołanie negatywnego wpływu na środowisko i/lub bezpieczeństwo personelu (na przykład wybuch zbiorników paliwowych lub destabilizacja procesu chemicznego w celu uwolnienia szkodliwych gazów). Istnieje kilka rodzajów ICS, ale wszystkie składają się z tych samych podstawowych elementów. Są to: czujniki, urządzenia sterujące, urządzenia sterowane (w tym elementy wykonawcze) i interfejs człowiek-maszyna (HMI) oraz zdalna diagnostyka i konserwacja.

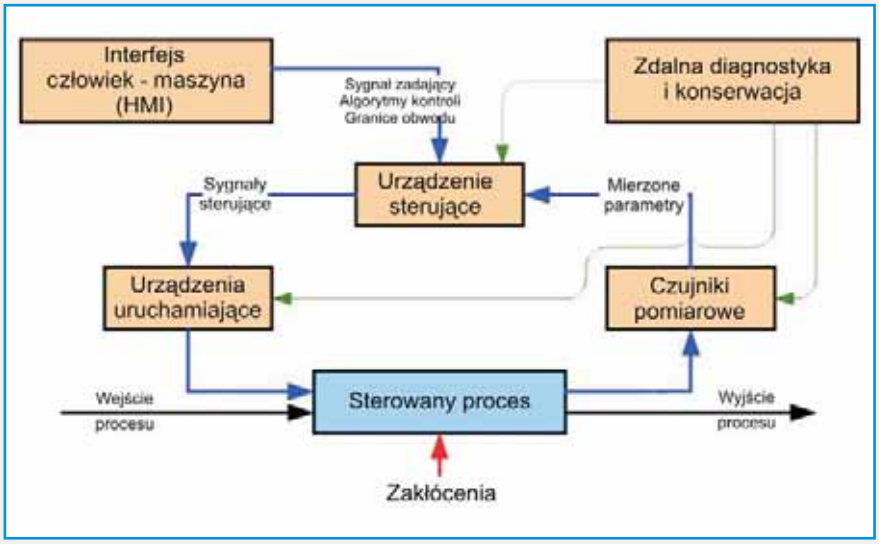
Uproszczony schemat działania ICS (rys. 1.) i funkcje elementów wyglądają następująco.

Algorytmy sterowania urządzenia sterującego oparte są na matematycznym modelu procesu, który ma być sterowany i na celach sterowania. Czujniki umożliwiają analizę stanu procesu przez pomiar takich parametrów procesu, jak temperatura, ciśnienie, napięcie, pH, pozycja, rozmiar itd. Stan procesu może ulegać zmianom w wyniku zewnętrznych „zakłóceń", zmian na wejściu (np. w miejscu podawania materiału) lub zmian w reakcji na działanie zainicjowane przez urządzenie sterujące.

Urządzenie sterujące przetwarza informacje z czujnika i na podstawie algorytmu sterowania i znajomości pożądanego stanu procesu, wysyła polecenia do elementów wykonawczych, które wpływają na sterowany proces, aż do wywołania odpowiednich zmian w jego stanie. Elementy wykonawcze obejmują wiele różnych rodzajów urządzeń, w tym zawory, przełączniki, przekaźniki, silniki itd., w zależności od natury sterowanego procesu. Interfejs człowiek-maszyna umożliwia operatorom obserwację stanu procesu oraz ICS.

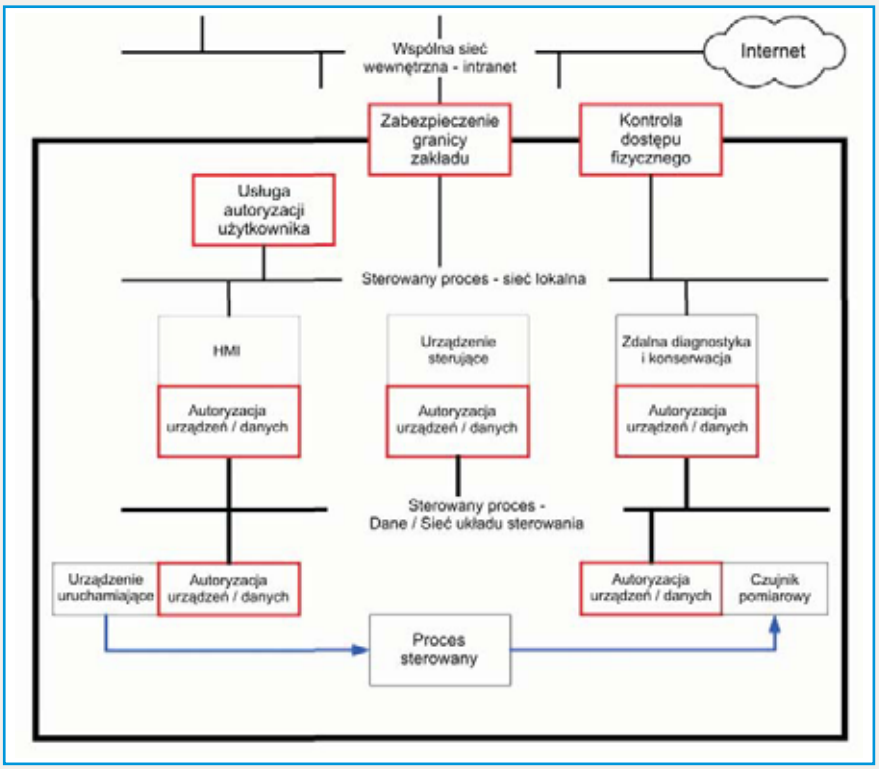
Systemowy profil ochrony (SPP) dla ICS

Kilka czynników spowodowało ostatnio wzrost niepokoju o bezpieczeństwo systemów sterowania stosowanych w przemyśle. Pierwszy czynnik, to ogólny trend, by zastępować specjalistyczne urządzenia sterujące, w szczególności regulatory i elementy komunikacji, specjalizowanymi komputerami z dedykowaną technologią przekazu danych. Drugi czynnik, to sposób, jaki wybrało wiele przedsiębiorstw, a mianowicie wzajemne połączenie pewnych części swoich sieci sterowania procesem w firmowym intranecie po wprowadzeniu



Rys. 1. Ogólny schemat ICS

Fig. 1. General diagram of an Industrial Control System



Rys. 2. Graficzne przedstawienie zakresu tematycznego STOE

Fig. 2. Graphic presentation of the thematic scope of a System Target of Evaluation

specjalizowanego sprzętu do systemu kontroli procesu. Te dwa czynniki wprowadzają potencjalne podatności związane z operacjami sieciowymi, w szczególności jeśli firmowy intranet powiązany jest z siecią zewnętrzną, np. z Internetem.

Trzeci czynnik związany jest z sytuacją, gdy do elementów ICS, które są rozdzielone przestrzennie, stosowane są różne środki komunikacji, włączając publiczny system telefoniczny, sieć bezprzewodową i Internet. Potencjalne podatności na zaburzenie bezpieczeństwa związane są z każdą z tych ścieżek komunikacji.

W celu neutralizacji tych podatności, organizacje przede wszystkim instalują nowe, dodatkowe elementy zabezpieczające ICS. Wprowadzenie koncepcji ***profilu ochrony systemu*** (*System Protection Profile* – SPP) ma na celu ujednolicenie podstaw dla tych działań i opracowania projektów nowych systemów. Przyjmuje się w każdym z tych przypadków, że funkcjonalność bezpieczeństwa powinna być wprowadzona do praktyki z wykorzystaniem analiz ryzyka, które określają wymagania bezpieczeństwa wynikające z oszacowania zagrożeń, podatności i skutków. Wyznaczanie i ocena SPP zostały przedstawione w formie wytycznych w dokumencie „System Protection Profile – Industrial Control Systems", przygotowanym w 2004 r. w ramach prac sponsorowanych przez National Institute of Standards and Technology (NIST) [5]. Dokument jest zgodny z wersją 2.1 CC (*Common Criteria*) [6-8].

SPP dla ICS określa zintegrowany zbiór wymagań w zakresie bezpieczeństwa dla systemów sterowania stosowanych w przemyśle. Zintegrowany zestaw zawiera wymagania dla procedur operacyjnych i polityki bezpieczeństwa, wymagania dla elementów systemu opartych na technologii informacyjnej, wymagania dla interfejsów i współdziałania pomiędzy elementami systemu oraz wymagania dla środowiska fizycznego i ochrony systemu. W realizacji ICS szczególną uwagę przywiązuje się do interakcji i zależności pomiędzy podsystemem bezpieczeństwa a nadrzędnym systemem sterowania.

Systemowy cel oceny

W dokumencie na temat SPP opracowanym dla NIST [5] wprowadzono koncepcję *Systemowego celu oceny* (*System Target of Evaluation* – STOE) w celu ułatwienia i ujednolicenia działań dla zabezpieczenia poufności i spójności danych oraz zapewnienia gotowości operacyjnej systemu bez zakłócania funkcji systemu bezpieczeństwa. Spójność danych skupia się na zabezpieczeniu ich przepływu do i od urządzenia sterującego i innych elementów lub podsystemów systemu sterowania.

Zakres tematyczny STOE przedstawiono na rys. 2. Kolorem czerwonym zaznaczone są elementy przedstawiające podstawowe funkcje zabezpieczeń systemu. Tymi funkcjami są: obsługa autoryzacji użytkownika (włączając kontrolę dostępu użytkownika), fizyczna kontrola dostępu, zabezpieczenia granic zakładu oraz autoryzacja danych/urządzeń. Obsługa autoryzacji użytkownika kontroluje dostęp do komputerowych systemów sterowania procesem, włączając interfejs człowiek-maszyna, zdalną diagnostykę i przeglądy. Ponadto, autoryzacja użytkownika jest wykorzystywana przez fizyczny system kontroli dostępu dla autoryzacji personelu. Autoryzacja danych/urządzeń jest pokazana jako oddzielna funkcja w celu uwydatnienia potrzeby autoryzacji danych i sygnałów sterujących. Należy zauważyć, że intranet jest w zewnętrznym środowisku STOE.

Niebieskie linie poprowadzone od urządzenia uruchamiającego do kontrolowanego procesu i od kontrolowanego procesu do czujnika wskazują, że mają miejsce fizyczne połączenia przedstawiające bezpośrednie interakcje. Pozostała część diagramu przedstawia połączenia logiczne. Elementy kontroli bezpieczeństwa oparte na zarządzaniu i procedurach operacyjnych nie zostały pokazane na tym rysunku.

Cechy bezpieczeństwa STOE przedstawia tabela.

Zagrożenia są określane z uwzględnieniem zidentyfikowanego rodzaju zagrożenia, możliwego ataku, oraz zasobów zakładu, które mogą być celem ataku. Rodzaje zagrożeń określane są na podstawie ekspertyz, w których bierze się pod uwagę dostępne zasoby oraz motywacje atakujących. Ataki charakteryzowane są poprzez połączenie sposobu ataku, możliwość wykorzystania jakichkolwiek podatności zakładu przez strony trzecie oraz występujących okoliczności.

W celu określenia względnej istotności wymagań w zakresie bezpieczeństwa STOE i jego środowiska operacyjnego, w SPP zostały uwzględnione elementy ryzyka. Te elementy ryzyka pozwalają na ukierunkowanie określania celów bezpieczeństwa: zapewniają one, że przez STOE, albo jego środowisko operacyjne, będą uwzględnione tylko te potrzeby w zakresie bezpieczeństwa, które zostaną uznane jako krytyczne dla przedsiębiorstwa.

Podsumowanie

Unormowania w zakresie cyberbezpieczeństwa oraz związane z nimi wytyczne mogą istotnie pomóc w identyfikowaniu problemów i redukcji podatności przemysłowych systemów sterowania (ICS) na ataki. Znajomość tych problemów i podatności systemu umożliwia zastosowanie odpowiednich unormowań w celu zmniejszenia ryzyka nie-

Tabela

CECHY BEZPIECZEŃSTWA STOE
SECURITY CHARACTERISTICS OF STOE

Rodzaj	Opis
Autoryzacja	• informacje istotne z punktu widzenia finansów i prowadzenia interesów przesyłane z ICS do zewnętrznych systemów współpracujących firm • zmiany konfiguracji wywierające wpływ na podstawowe funkcje ICS (np. algorytmy sterowania, nastawy, punkty graniczne itd) • użytkowników mających dostęp do zabezpieczonych zasobów (np. urządzeń uruchamiających, systemów sterowania)
Poufność	zabezpieczenie operacyjnych, finansowych i sterujących danych przed nielegalnym ujawnieniem (dane określone na podstawie oceny ryzyka i zatwierdzone przez właściciela systemu), łącznie z, ale nie ograniczając się do odpowiednich segmentów w zasięgu sieci ICS
Spójność	zabezpieczenie przed nieautoryzowanymi zmianami: • przepływów informacji wrażliwej natury na temat narażonych segmentów sieci • informacji na temat wewnętrznych danych sterujących, używanych przez system ICS • konfiguracji operacyjnego systemu ICS
Gotowość operacyjna	zabezpieczenie przed utratą gotowości operacyjnej wszystkich krytycznych i ważnych systemów operacyjnych ICS, łącznie z, ale nie ograniczonych do: • serwerów sterujących • głównego łącza komunikacyjnego (lub sieci) • operacyjnej możliwości konfiguracji systemu ICS
Zabezpieczenie granicy	zabezpieczenie przeciw próbom naruszenia zarówno fizycznych jak i logicznych granic systemu ICS
Kontrola dostępu	ścisłe przestrzeganie kontroli dostępu: • wewnętrznego i zewnętrznego zdalnego dostępu do sieci ICS • zewnętrznie widocznych interfejsów ICS • zasobów systemowych uznanych za wymagające zabezpieczeń • funkcji systemu zdolnych do modyfikowania konfiguracji ICS • krytycznych procesów ICS bazujących na informacjach o stanie, istotnych dla tych procesów (np. lokalizacja)
Elementy rezerwowe/ odzyskiwanie	istnienie rezerwowych mechanizmów dla krytycznych danych ICS i dla informacji sterujących w celu umożliwienia odzyskania ich w rozsądnym czasie w przypadku awarii systemu
Audyt	zapisy w rejestrze audytu dot. odpowiednich elementów ICS, wyszczególniające udane i zakończone niepowodzeniem działania użytkowników i aplikacji istotne z punktu widzenia bezpieczeństwa
Monitoring	monitoring i wykrywanie nieautoryzowanych działań, działań nadzwyczajnych i prób naruszenia funkcji bezpieczeństwa ICS, łącznie z zastosowaniem systemów wykrywania włamań do krytycznych części infrastruktury ICS
Nieingerowanie w funkcje o decydującym znaczeniu	nieingerowanie w funkcje bezpieczeństwa ICS i funkcje o decydującym znaczeniu dla bezpieczeństwa przy jednoczesnym utrzymaniu pracy ICS
Samo-weryfikacja	auto-testy weryfikujące konfigurację i integralność funkcji bezpieczeństwa ICS
Awaryjne zasilanie energią elektryczną	układ awaryjnego zasilania energią elektryczną umożliwiający łagodne wyłączenie ICS i sterowanego procesu, w przypadku awarii podstawowego i rezerwowego układu zasilania
Plany, polityka i procedury bezpieczeństwa	plany, polityka i procedury bezpieczeństwa obejmujące co najmniej: • całościową politykę bezpieczeństwa zarządzającą dostępem i koniecznymi zabezpieczeniami dla wszystkich elementów ICS • zarządzanie bezpieczeństwem ICS i związanych z nim infrastruktur • przydzielanie ról i odpowiedzialności w systemie zarządzania bezpieczeństwem poprzez infrastrukturę zarządzania ICS • dokumentację organizacyjnego procesu zarządzania ryzykiem i jego powiązań z systemem ICS • plany utrzymania ciągłości działań operacyjnych i naprawy dla ICS, w przypadku szkód wyrządzonych katastrofami • strategię migracji obejmującą identyfikowanie, ocenę i neutralizację nowych lub istniejących podatności (zgodnie z polityką zarządzania ryzykiem) podczas cyklu życia ICS • politykę zarządzającą rolami, zakresami odpowiedzialności i działaniami autoryzowanych stron trzecich, pracujących przy elementach ICS • politykę i procedury konieczne do zapewnienia zgodności z określonymi aktami prawnymi i normami (np. audyty systemu)

pożądanych ingerencji stron trzecich w działanie ICS. Oceny projektowanych i istniejących rozwiązań ICS powinny wykorzystywać ujednolicone i uznane przez międzynarodowe zespoły ekspertów zasady prowadzenia analiz i kryteria, takie jak CC, oraz stowarzyszone z nimi lub opracowane na ich podstawie szczegółowe wytyczne w rodzaju takich, jak przedstawiony w niniejszym artykule profil ochrony systemu (SPP) i systemowy cel oceny (STOE).

PIŚMIENNICTWO

[1] J. S. Michalik, M. Borysiewicz, A. Wasiuk *Metodyka zintegrowanych ocen ryzyka poważnych awarii i zagrożeń terrorystycznych zakładów chemicznych.* Opracowanie zasad prowadzenia ocen rozwiązań inżynieryjnych i organizacyjnych dotyczących niebezpiecznych scenariuszy w stacjonarnych instalacjach chemicznych z uwzględnieniem istniejących interfejsów z instalacjami transportu i przeładunku substancji niebezpiecznych oraz systemów informatycznych w aspekcie ochrony przed działaniami terrorystycznymi i sabotażowymi. (Wykonano w ramach programu wieloletniego pn. *Dostosowywanie warunków pracy w Polsce do standardów Unii Europejskiej*). CIOP-PIB, Warszawa, listopad 2006

[2] American Chemistry Council's – Chemical Information Technology Council (ChemITC)™ - Chemical Sector Cyber Security Program. Guidance Document. Guidance for Addressing Cyber Security in the Chemical Industry - Version 3.0., 2006

[3] Chemical Industry Data Exchange (CIDX). *Cybersecurity Practices, Standards, and Technology.* Cybersecurity Reference Model - Revision 1.0, 2004

[4] *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, Center for Chemical Process Safety (CCPS), August 2002

[5] National Institute of Standards & Technology. *System Protection Profile – Industrial Control Systems* – Version 1.0, www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc, April 2004

[6] *Common Criteria for Information Technology Security Evaluation* Part 1: *Introduction and general model*, September 2006, Version 3.1 Revision 1, CCMB-2006-09-001

[7] *Common Criteria for Information Technology Security Evaluation* Part 2: *Security functional components* September 2006 Version 3.1 Revision 1, CCMB-2006-09-002

[8] *Common Criteria for Information Technology Security Evaluation* Part 3: *Security assurance components*, September 2006 Version 3.1 Revision 1, CCMB-2006-09-003

Publikacja opracowana na podstawie wyników uzyskanych w ramach programu wieloletniego pn. „Dostosowywanie warunków pracy w Polsce do standardów Unii Europejskiej" dofinansowywanego w latach 2005 – 2007 w zakresie zadań służb państwowych przez Ministerstwo Pracy i Polityki Społecznej. Główny koordynator: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy