mgr inż. ADAM BROJA
mgr inż. DAMIAN CAŁA
mgr inż. MARCIN MAŁACHOWSKI
mgr inż. KAROL ŚPIECHOWICZ
mgr ADRIAN SZCZUREK
Instytut Technik Innowacyjnych EMAG

Zastosowanie metodyki Common Criteria podczas procesu projektowania urządzeń na przykładzie czujnika gazometrycznego

Artykuł przedstawia wyniki prac związanych z zastosowaniem metodyki Common Criteria (ISO/IEC15408) w projektowaniu czujników gazometrycznych, które spełniają wymagania stawiane górniczym urządzeniom budowy przeciwwybuchowej. Omówiono kluczowe założenia standardu Common Criteria oraz poszczególne etapy tworzenia dokumentu Security Target opisującego koncepcję bezpieczeństwa dla oceny przykładowego czujnika gazometrycznego. Opisano konstrukcję teoretycznego urządzenia, określono wszystkie zasoby, których scharakteryzowanie niezbędne jest do zdefiniowania problemu bezpieczeństwa. Omówiono podmioty związane z produkcją i użytkowaniem czujnika, zagrożenia, które mogą w negatywny sposób wpłynąć na bezpieczeństwo urządzenia oraz przedstawiono założenia dotyczące jego pracy.

Projekt jest realizowany w ramach dofinansowania Unii Europejskiej, nr umowy UDA POIG 01.03.01.156/08.

1. WSTĘP

Common Criteria (CC) to uznana na świecie norma dostarczająca jasnej i wiarygodnej oceny możliwości produktów IT w kwestii bezpieczeństwa. Dokonując niezależnej, formalnej weryfikacji bezpieczeństwa produktu, Common Criteria daje klientom większe zaufanie do produktów IT w kwestii bezpieczeństwa i prowadzi do podejmowania decyzji w oparciu o dokładniejsze informacje. Klienci świadomi zagrożeń dla bezpieczeństwa informatycznego, wymagają certyfikatów CC, jako decydującego czynnika w podejmowaniu decyzji o zakupie danego produktu. Ze względu na fakt, że wymagania certyfikacyjne są jasno określone, sprzedawcy mogą w swojej ofercie posiadać produkty stanowiące odpowiedź na bardzo specyficzne potrzeby dotyczące zabezpieczeń, jednocześnie oferując szeroką gamę produktów.

Standard Common Criteria (CC, ISO 15408) udostępnia procedury pozwalające na zdefiniowanie zagrożeń oraz zabezpieczeń, które na te zagrożenia odpowiadają, a następnie przeprowadzenie formalnej weryfikacji ich faktycznego działania w produkcie. Certyfikacją według normy CC zajmują się niezależne, akredytowane laboratoria badawcze na całym świecie [1].

Wynikiem procesu certyfikacji produktu lub systemu IT jest raport techniczny z przebiegu niezależnej oceny oraz certyfikat potwierdzający skuteczność zabezpieczeń pod pewnymi warunkami. Proces certyfikacji może być prowadzony według różnych poziomów bezpieczeństwa (EAL – *Evaluation Assurance Level*), począwszy od EAL1 (tylko testy funkcjonalne) aż do EAL7 (formalna weryfikacja projektu oraz testy).

Posiadanie certyfikatu CC nie gwarantuje, że produkt jest bezpieczny pod każdym względem – zapewnia jedynie o działaniu wszystkich zadeklarowanych przez producenta zabezpieczeń.

Międzynarodowy charakter certyfikatów Common Criteria, przyjmowany przez coraz większą liczbę państw, pozwala użytkownikom z innych krajów kupować produkty IT z większym zaufaniem, ponieważ

certyfikaty te są uznawane we wszystkich krajach akceptujących te normy [6]. Tabela 1 przedstawia najważniejsze terminy używane podczas procesu walidacji.

Tabela 1
Terminy używane w Common Criteria [1]

Akronim	Znaczenie
Target of Evaluation (TOE)	Przedmiot oceny, zestaw oprogramowania (software), firmware i/lub sprzętu poddawany ocenie i certyfikacji; np. czujnik gazometryczny MCX 1.0
EAL - Evaluation Assurance Levels	Predefiniowany zestaw wymagań dotyczących bezpieczeństwa – poziomy od EAL1 do EAL7
SAR – Security Assurance Requirement	Wymagania uzasadniające zaufanie do zabezpieczeń
SFR – Security Functional Requirements	Wymagania funkcjonalne bezpieczeństwa
+	Zadanie zabezpieczeń
TSF - TOE Security Functions	Funkcje zabezpieczeń TOE

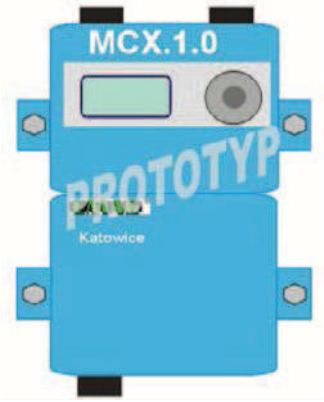
Artykuł przedstawia kolejne kroki tworzenia dokumentu ST przez konstruktora urządzenia. Zaprezentowane zostały najważniejsze etapy przygotowywania dokumentu.

2. CHARAKTERYSTYKA PRZEDMIOTU OCENY (TOE)

Jednym z pierwszych etapów pracy konstruktora nad zadaniem zabezpieczeń jest opis i charakterystyka przedmiotu oceny.

Czujnik gazometryczny MCX 1.0 jest modelem urządzenia pomiarowego, którego konstrukcja i zasada działania została oparta na wielu rozwiązaniach z dziedziny gazometrii oferowanych przez Instytut Technik Innowacyjnych EMAG [4].

Czujnik MCX 1.0 pozwala na ciągły pomiar stężenia metanu w zakresie 0÷100% oraz dodatkowo stężenia gazów mierzonych przez zaimplementowane sensory, w zależności od wersji czujnika. Czujnik charakteryzuje się szybkim czasem odpowiedzi oraz elastycznym sposobem konfigurowania swojej funkcjonalności. Zasadniczym przeznaczeniem czujnika gazometrycznego jest praca w ramach systemu metanometrii automatycznej. Pracując w ramach systemu czujnik MCX realizuje funkcje związane ze sterowaniem wyjść dwustanowych. Sterując wyjściami czujnik MCX dokonuje automatycznych wyłączeń energii elektrycznej w przypadku przekroczenia stężeń dopuszczalnych metanu. Wygląd opisywanego urządzenia przedstawia rysunek 1.



Rys. 1. Czujnik gazometryczny MCX 1.0

Czujnik MCX może również pracować lokalnie, poza systemem metanometrii automatycznej. W przypadku pracy lokalnej w czujniku nie są dostępne funkcje związane ze sterowaniem wyjść dwustanowych. Czujnik składa się z dwóch połączonych obudów, z których jedna zawiera układ elektroniczny metanomierza, a druga stanowi komorę przyłączową umożliwiającą dołączenie obwodów zewnętrznych. Komora przyłączowa wyposażona jest w trzy wpusty do wprowadzania kabli oraz w złącze do przyłączania klawiatury kalibracyjnej. Głowica pomiarowa wyposażona jest w wymienny filtr składający się z siatki stalowej, folii hydrofobowej oraz warstwy węgla aktywnego. Obudowy czujnika MCX i głowicy pomiarowej wyposażone są w specjalne zawiesia umożliwiające ich zawieszenie pod stropem w wymaganej pozycji.

Układ elektroniczny czujnika MCX rozmieszczony jest na obwodach drukowanych, połączonych ze sobą przewodami taśmowymi. Podział układu elektronicznego zaprojektowano tak, aby możliwe było tworzenie, na życzenie użytkownika, wersji przyrządu różniącego się możliwościami funkcjonalnymi i ceną. Moduł procesora zawiera kontroler sterujący wszystkimi funkcjami czujnika MCX i odpowiedzialny za komunikację ze sterownikiem centrali telemetrycznej.

Dla mikroprocesorowego czujnika gazometrycznego w wykonaniu iskrobezpiecznym typu MCX zaprojektowano komory pomiarowe wyposażone w jednolity, asynchroniczny interfejs szeregowy umożliwiający podłączenie do podsystemu MCXcore (Rys. 3). Komory pomiarowe zasilane są napięciem z globalnego zasilania czujnika, co pozwala na stabilizację napięcia dopiero w poszczególnych komorach pomiarowych.

Otoczenie TOE (*TOE physical environment*) dostarcza do TOE mierzone sygnały (gaz znajdujący się w otoczeniu czujnika), które są przetwarzane i kondycjonowane przez mikrokontroler komory pomia-

rowej. Przede wszystkim kontroluje skrośne działanie detektora na temperaturę otoczenia (*TOE physical environment*) oraz dryf (niestałość czasową) napięcia na wyjściach sensora podłączonych bezpośrednio do mikrokontrolera w podsystemie MCXdet.

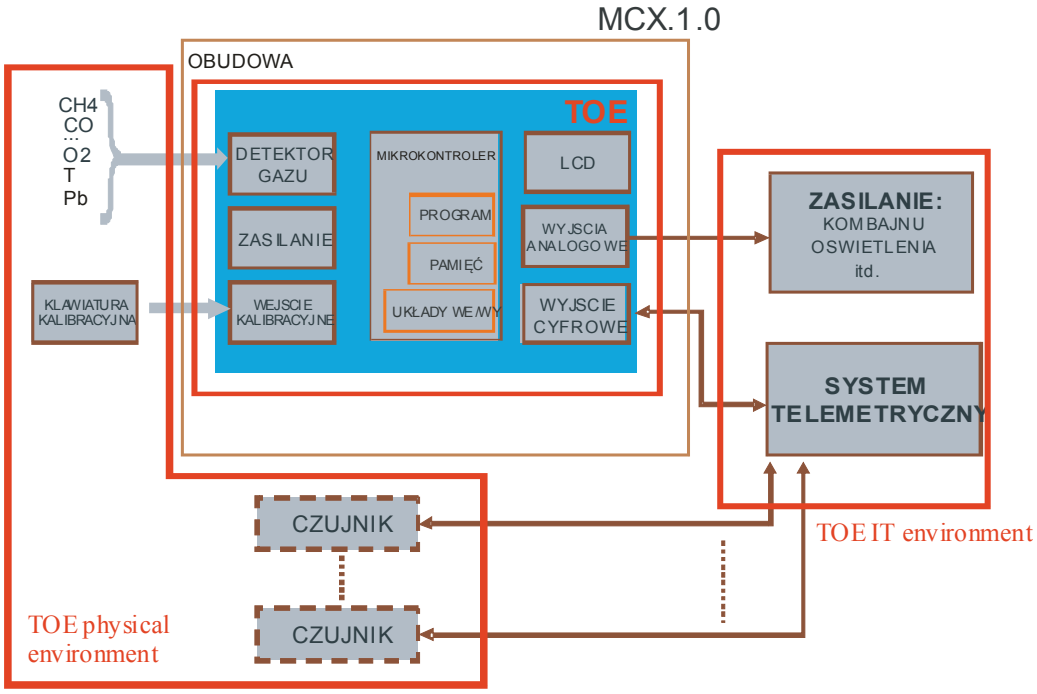
Czujnik może być wyposażony w kilka komór pomiarowych, w których każda niezależnie posiada funkcje zabezpieczające poprawność wprowadzonych danych ze środowiska TOE, weryfikację danych oraz kontrolę poziomu ochrony otoczenia TOE. W zależności od zastosowanej komory pomiarowej wyróżnia się następujące elementy zabezpieczające poprawność zapisu informacji i przekazania do monitora głównego (podsystemu MCXcore):

- sprawdzenie poprawności napięcia zasilania dostarczanego do detektora pomiarowego,
- kontroli i porównania sygnału napięciowego analogowego z detektora do wartości zapisanej w pamięci podczas produkcji i kalibracji komory pomiarowej,
- weryfikacji sygnałów cyfrowych z detektora poprzez porównanie z zakresem pomiarowych zapisanym w pamięci procesora podczas produkcji komory pomiarowej,
- porównania czasu pracy detektorów zapisanych w pamięci procesora podczas produkcji komory pomiarowej i wyłączenia pomiaru przy przekroczeniu „czasu życia" detektora,
- kontroli temperatury pracy czujnika i przekazanie alarmu (awarii) do aplikacji głównej czujnika w momencie przekroczenia dozwolonej temperatury pracy,
- kompensacji termicznej (ciśnieniowej) detektorów, które nie posiadają automatycznej kompensacji.

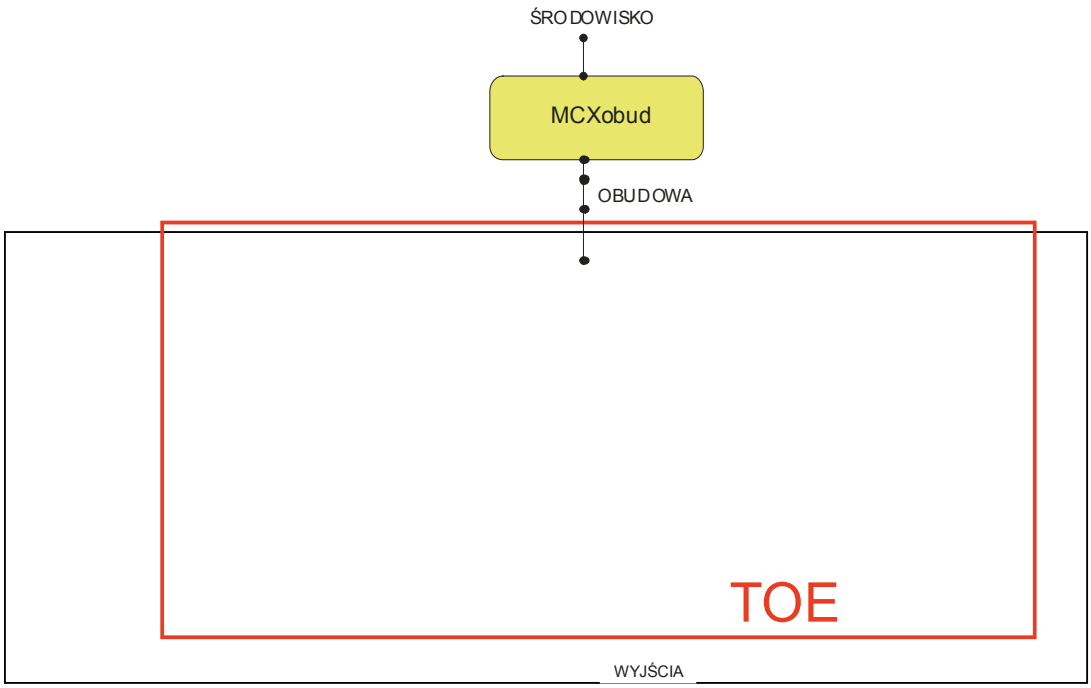
Program zapisany w procesorze jest wprowadzany przez producenta w laboratorium sprzętowo-programowym o podwyższonych wymaganiach bezpieczeństwa, które zostało stworzone i pracuje zgodnie z normą Common Criteria.

Czujnik MCX może zapamiętać niektóre zdarzenia wraz z datą i czasem ich wystąpienia (np. data i czas kalibracji czujnika, narażenia na przeciążenia gazowe podczas kalibracji). Wszystkie nastawy konfiguracyjne czujnika MCX, tzn. wartości progów alarmowych, logiczny adres czujnika w systemie, sposób sterowania wyjściami dwustanowymi itp. ustawiane są tylko i wyłącznie ze stacji powierzchniowej, ze stanowiska dyspozytora systemu w momencie przeprowadzania konfiguracji danego czujnika.

Obiektem weryfikacji (TOE) jest część wewnętrzna czujnika gazometrycznego – obudowa urządzenia traktowana jest jako część otoczenia obiektu (Rys. 2). TOE ma możliwość autonomicznej pracy, jednakże jego podstawowym przeznaczeniem jest praca jako element systemu telemetrycznego. W przypadku takiego trybu pracy potrzebna jest linia transmisyjna (zasilanie, transmisja), która umożliwia połączenie TOE z modułem zasilająco-transmisyjnym. Informacje z modułu przekazywane są do głównego komputera PC, z poziomu którego zarządza się systemem, urządzeniami i interpretuje pomiary uzyskane z urządzeń.



Rys. 2. TOE i jego otoczenie



Rys. 3. Interfejsy TOE [5]

Opis interfejsów

Przedstawiono te interfejsy czujnika MCX (Rys. 3), które odpowiadają funkcjom zabezpieczającym TOE oraz te, które posiadają zabezpieczenie przed ominięciem funkcji zabezpieczających TOE [5]. Przytoczono podstawowy opis interfejsów znajdujący się w materiale dowodowym ADV_ARC.

Interfejsy podsystemu MCXdet:

- MCXdet: GAZ – Interfejs zewnętrzny transportu gazu do komory pomiarowej.
- Interfejsy podsystemu MCXklaw:
- MCXklaw: KLAWIATURA – interfejs odpowiedzialny za przesyłanie danych z klawiatury kalibracyjnej do podsystemu MCXklaw.

Interfejsy podsystemu MCXtranzas:

- MCXtranzas: LINIA – interfejs, którym przesyłane są dane pomiarowe, informacja o zaistniałych przekroczeniach progów alarmowych, dane identyfikacyjne czujnika, stan wejść/wyjść dwustanowych do systemu telemetrycznego oraz zasilanie.

Interfejsy podsystemu MCXwewy:

- MCXwewy: WYJŚCIA – interfejs zawierający wyjścia dwustanowe czujnika MCX,
- MCXwewy: WEJŚCIA – interfejs zawierający wejścia dwustanowe czujnika MCX.

Interfejsy podsystemu MCXcore:

- MCXcore: OBUDOWA – interfejs mechaniczny pośredniczący w zabezpieczeniu przed nieautoryzowanym otwarciem obudowy, plomba zabezpieczająca dane i program w podsystemie MCXcore.

3. DEFINICJA PROBLEMU BEZPIECZEŃSTWA

Zdefiniowanie problemu bezpieczeństwa czujnika gazometrycznego dotyczy urządzenia oraz środowiska, w którym czujnik będzie pracował (*TOE IT environment* i *TOE physical environment*). Poszczególne aspekty problemu bezpieczeństwa wyrażone są poprzez zagrożenia i politykę bezpieczeństwa organizacji, w której jest eksploatowany czujnik. Pierwszym etapem definicji problemu bezpieczeństwa jest określenie chronionych zasobów oraz podmiotów związanych z cyklem życia TOE. Następnie konstruktor identyfikuje zagrożenia, które mogą w negatywny sposób wpłynąć na przedmiot oceny oraz definiuje cele zabezpieczeń zarówno dla TOE jak i jego środowiska operacyjnego, które przeciwstawiają się tym zagrożeniom.

Zasoby

Sekcja przedstawia wszystkie zasoby (*Assets*), których identyfikacja jest niezbędna do zdefiniowania problemu bezpieczeństwa. Zasoby podzielone są według ich logicznego oraz fizycznego przeznaczenia i związku z TOE [1].

Tabela 2

Zasoby [2]

Symbol	Opis
DTO.SensorData	Przetwarzane wielkości fizyczne (ciśnienie, temperatura) lub chemiczne (stężenie gazu) na wielkość elektryczną (informatyczną) oraz protokół transmisji
DTO.SensorID	Dane identyfikacyjne czujnika
DTO.UserData	Dane użytkownika; Ustawienie progów alarmowych (wyłączenie energii)
DIT.TelemSyst	Nadrzędny system telemetryczny
DIT.CalibKeyb	Urządzenie podłączane do czujnika w celu jego kalibracji i zmiany jego ustawień
DIT.Power	Układy zasilane energią wyłączane przez czujnik (matryca wyłączeń)
DAP.DesignData	Informacje dotyczące projektowanych rozwiązań (sprzętowych, informatycznych), dokumentacja projektowa

Kolejnym etapem jest określenie podmiotów związanych z cyklem życia TOE.

Podmioty

Sekcja definiuje podmioty (*Subjects*) związane lub współpracujące z TOE. Podmioty, pod kątem kryterium autoryzacji, podzielone są na dwie grupy – użytkowników autoryzowanych (SAU) oraz użytkowników nieautoryzowanych (SNA) [1].

Tabela 3

Podmioty współpracujące z TOE [2]

Symbol	Opis
SAU.Developer	Osoba zaangażowana w prace rozwojowe dotyczące czujnika
SAU.ManufPers	Osoba zaangażowana w procesy wytwórcze (wytwarzanie komponentów programowych i sprzętowych) ich integrację i testowanie
SAU.ServicePers	Osoba odpowiedzialna za serwis czujnika i ewentualną naprawę
SAU.User	Osoba autoryzowana (dozór kopalni, górnik-metaniarz, górnik-elektryk)
SAU.Dispatch	Osoba zarządzająca z poziomu systemu telemetrycznego konfiguracją czujników oraz interpretująca dane wysłane przez czujniki oraz stan urządzeń
SAU.MiningAuth	Osoba odpowiedzialna za kontrolę poprawności pracy urządzeń (Wyższy Urząd Górniczy)
SAU.MaintPers	Personel obsługujący TOE (maintenance)
SNA.MiningPers	Osoba należąca do personelu kopalni, która w sposób celowy lub niecelowy może uszkodzić czujnik
SNA.HighPotIntrud	Osoba bez uprawnień, próbująca TOE lub zniekształcić dane pomiarowe (rozkalibrować czujnik)
SNA.IndSpy	Osoba próbująca uzyskać nieautoryzowany dostęp do dokumentacji projektowej

Następnym etapem definicji problemu bezpieczeństwa jest zidentyfikowanie zagrożeń, które mogą negatywnie wpłynąć na pracę przedmiotu oceny.

Zagrożenia

W poniższej sekcji przedstawione zostały wszystkie zagrożenia zidentyfikowane przez konstruktora dla czujnika, które mogą w negatywny sposób wpłynąć na bezpieczeństwo TOE lub bezpieczeństwo pracy TOE [1].

Tabela 4

Zagrożenia [2]

Symbol	Opis
TDA.Access	Możliwość dostępu przez użytkowników [SAU.Developer], [SAU.MaintPers], [SAU.ServicePers], [SAU.User], [SNA.HighPotIntrud] do funkcji czujnika i sfałszowania jego danych [DTO.SensorData]
TDA.Faults	Błędy pomiaru i transmisji. Wyjaśnienie: uszkodzenie czujnika, linii transmisyjnej lub detektora
TDA.Calib	Możliwość nieautoryzowanej zmiany parametrów pracy czujnika [DTO.SensorData] przez personel serwisowy [SAU.ServicePers]
TDA.Test	Niewłaściwa procedura testowania [SAU.Developer]
TDA.PowerSupply	Możliwość uszkodzenia czujnika przez użytkowników lub intruzów [SAU.User], [SNA.HighPotIntrud], [SAU.ManufPers] poprzez podłączenie zasilania niezgodnego ze specyfikacją czujnika. Możliwość wyczerpania się baterii
TDA.SensorID	Możliwość fałszowania indywidualnych i unikalnych identyfikatorów przez użytkowników [SNA.MiningPers]
TDA.ForceMajeure	Możliwość uszkodzenia czujnika przez tąpnięcia, czynniki atmosferyczne i środowiskowe takie jak: wybuch, pożar, powódź, itd.
TDA.Software	Możliwość modyfikacji oprogramowania w kontrolerze przez użytkowników lub intruzów [SNA.HighPotIntrud], [SAU.ManufPers], [SAU.ServicePers]
TPH.MechnicalOrgin	Możliwość dostania się do wnętrza obudowy i modyfikacji lub uszkodzenia czujnika przez użytkowników [SAU.User], [SNA.MiningPers]
TPH.IndSpy	Możliwość kradzieży danych projektowych przez nieautoryzowane osoby [SNA.IndSpy]

Kolejną czynnością w pracach konstruktora nad definicją problemu bezpieczeństwa jest określenie celów zabezpieczeń dla TOE oraz dla jego środowiska.

Cele zabezpieczeń

Konstruktor określając cele zabezpieczeń, które stanowią rozwiązanie zidentyfikowanego problemu bezpieczeństwa, musi uwzględnić założenia dotyczące otoczenia oraz przewidywane zagrożenia. Ponadto konstruktor musi uzasadnić, że wobec wszystkich zidentyfikowanych zagrożeń podjęto środki zaradcze [7].

Cele zabezpieczeń przedstawione są w dwóch aspektach: dla TOE i dla środowiska operacyjnego [1].

Tabela 5

Cele zabezpieczeń dla TOE [2]

Symbol	Opis
OINT.DataTransProt	TOE zapewnia kontrolę poprawności protokołu przesyłu informacji z klawiatury kalibracyjnej
OINT.DataWrite	TOE zapewnia prawidłowość zapisu informacji w pamięci danych
OACC.CalibCtrl	TOE zapewnia identyfikację klawiatury kalibracyjnej
ODEX.DataChange	TOE przesyła informacje do systemu telemetrycznego o zmianie parametrów swojej pracy spowodowanej podłączeniem klawiatury kalibracyjnej
OADT.ErrorInfo	TOE zapewnia wyświetlenie oraz przekazanie do systemu telemetrycznego informacji o błędach w działaniu oprogramowania
OINT.ElectProt	TOE zapewnia odporność na wysokie napięcia; w skrajnych przypadkach następuje przepalenie się bezpiecznika
OEIT.TransCheck	Otoczenie TOE wykrywa brak transmisji (bez zasilania czujnik przechodzi w tryb autonomiczny – transmisja jest wyłączona)
OINT.PowInter	Złącze zasilania znajduje się wewnątrz TOE, co uniemożliwia dostęp do obwodu elektrycznego
OEIT.DblCheck	Wykrywanie podwojonych numerów identyfikacyjnych
OEIT.Log	Zapisywanie adresów i identyfikatorów czujników
OINT.TOESecur	TOE zapewnia kontrolę poprawności działania elementów, protokołów transmisyjnych, ochronę części informatycznej i elektronicznej przed niepowołanym dostępem

Cele zabezpieczeń dla środowiska operacyjnego

Cele zabezpieczeń dla środowiska operacyjnego opisują w jaki sposób środowisko przeciwstawia się zidentyfikowanym zagrożeniom. Cele te również wspierają poznane cele zabezpieczeń dla TOE [8].

Tabela 6

Cele zabezpieczeń dla środowiska operacyjnego [2]

Symbol	Opis
OEIT.DataTransmIntegrity	System telemetryczny współpracujący z TOE zapewnia kontrolę integralności przesyłanych danych
OEIT.MeasureData	System telemetryczny zapewnia kontrolę stanu detektora (wykrywanie awarii detektora, awarii zasilania)
OEIT.DataTransProt	Klawiatura kalibracyjna zapewnia kontrolę poprawności protokołu przesyłu informacji
OEIT.DataChange	System telemetryczny zapewnia informację o zmianie parametrów pracy czujnika
OSMN.WorkOrg	Otoczenie zapewnia odpowiednią organizację prac projektowych produkcyjnych
OSMN.WorkSecur	Otoczenie zapewnia odpowiednie zabezpieczenie danych projektowych
OINT.CasePlomb	TOE zapewnia ochronę części elektronicznej i informatycznej przed nieautoryzowanym dostępem
OADT.Audit	Otoczenie zapewnia regularne kontrole i kalibracje urządzenia

4. PODSUMOWANIE

W artykule opisano wyniki prac związanych z zastosowaniem metodyki Common Criteria w procesie projektowania urządzeń. Jako przedmiot oceny wybrano model czujnika gazometrycznego. Przedstawiono opis urządzenia, jego interfejsów i podsystemów, ze zwróceniem uwagi na elementy wymagane do jego oceny wg standardu Common Criteria. Następnie opisano najważniejszy element definicji problemu bezpieczeństwa, na który składają się zasoby, podmioty oraz zagrożenia związane z projektowaniem, produkcją oraz serwisowaniem urządzenia. W wyniku prac prowadzonych w projekcie powstał gotowy dokument Security Target, będący podstawą do stworzenia pełnego materiału dowodowego. Artykuł przedstawia jego wybrane elementy.

Prace prowadzone w projekcie CCMODE, związane z tworzeniem kompletu materiału dowodowego

miały na celu zdobycie fachowej wiedzy o metodyce standardu CC oraz na zweryfikowaniu możliwości zastosowania tego standardu w procesie projektowania czujnika gazometrycznego. Biorąc pod uwagę przeznaczenie opisywanego urządzenia i jego charakter, należy dołożyć wszelkich starań by takie czujniki nie tylko pracowały w sposób niezawodny, ale również by ich praca była oparta na obowiązujących standardach bezpieczeństwa. Metodyka Common Criteria pozwala na uzyskanie wiedzy o poziomie bezpieczeństwa certyfikowanego obiektu, jak również umożliwia standaryzację procedur dotyczących projektowania, produkcji i serwisowania każdego urządzenia, które przeznaczone jest do pracy w środowiskach wymagających wysokiego poziomu bezpieczeństwa.

Przeprowadzenie analizy problemu bezpieczeństwa przykładowego czujnika gazometrycznego MCX pozwoliło zespołowi projektowemu wzbogacić wiedzę z zakresu metodyki Common Criteria, co w najbliższej przyszłości umożliwi wprowadzenie zasad obowiązujących w standardzie do procesu projektowania nowych rozwiązań sprzętowych i informatycznych. W czasach obecnych kładzie się duży nacisk na efektywność i bezpieczeństwo produktów, a dzięki coraz bardziej popularnej normie i certyfikacji CC możliwe jest osiągnięcie wysokiego poziomu wiarygodności zabezpieczeń. Dlatego też wynikiem wszystkich prac związanych z projektem CCMODE ma być wprowadzenie standardu CC do procesu produkcji wszystkich rozwiązań oferowanych przez Instytut EMAG.

Literatura

1. Common Criteria for IT Security Evaluation, version 3.1, 2009; Common Criteria Member Organizations, Part 1-3
2. MCX 1.0 – Mikroprocesorowy czujnik gazometryczny w wykonaniu iskrobezpiecznym – Security Target, ITI EMAG 2011, niepublikowane.
3. *Śpiechowicz K., Broja A., Mirek G., Małachowski M., Szczurek A., Cała D.*: Możliwość zastosowania metodyki Common Criteria do projektowania czujników gazometrycznych (case study). Konferencja „Środowisko rozwojowe produktów i systemów informatycznych o podwyższonych wymaganiach bezpieczeństwa. Instytut Technik Innowacyjnych EMAG 2009.
4. Strona internetowa ITI EMAG; http://www.emag.pl/, 03.2011.
5. Materiał dowodowy ADV_ARC mikroprocesorowego czujnika gazometrycznego w wykonaniu iskrobezpiecznym MCX.1.0. ITI EMAG 2011, niepublikowane.
6. *Białas A.*: Konstruowanie zabezpieczeń produktów i systemów informatycznych posiadających mierzalny poziom uzasadnionego zaufania. Mechanizacja i Automatyzacja Górnictwa 2009, nr 1.
7. *Białas A.*: Informatyczne produkty sprzętowe, oprogramowanie oraz systemy o zadanym poziomie uzasadnionego zaufania. Mechanizacja i Automatyzacja Górnictwa 2009, nr 12.
8. *Białas A.*: Wspólne Kryteria do projektowania i oceny zabezpieczeń (Common Criteria, ISO/IEC 15408). Autorskie szkolenie wprowadzające dla odbiorców certyfikowanych produktów informatycznych, niepublikowane.

Recenzent: dr inż. Andrzej Białas