PROCES CERTYFIKACJI ZINTEGROWANEGO STEROWNIKA AUTOMATYKI I BEZPIECZEŃSTWA BUDYNKÓW iSKD-4[1]

CERTIFICATION PROCESS OF THE INTEGRATED BUILDING AUTOMATION AND SECURITY CONTROLLER iSKD-4

Grzegorz HAYDUK, Paweł KWASNOWSKI, Grzegorz WRÓBEL
Łukasz TYRCHA, Radosław ŹREBIEC
ZDANIA Sp. z o.o.

Streszczenie: *W artykule przedstawiono tematykę badań i certyfikacji zintegrowanego sterownika automatyki i bezpieczeństwa iSKD-4. Sterownik łączy funkcje systemów Kontroli Dostępu, Sygnalizacji Włamania i Napadu z funkcjami automatyki pomieszczeniowej – sterowania z uzależnieniem od stanu zajętości pomieszczenia (wykrycia obecności). Sterownik został zaprojektowany zgodnie z wymaganiami stosownych norm dla systemów alarmowych i poddany badaniom, co zostało potwierdzone stosownym Świadectwem Kwalifikacyjnym stwierdzającym jego klasę zabezpieczenia.*
Przedstawiono dostępne programy certyfikacji oferowane w ramach Programów Certyfikacji LonMark, jak i cały proces certyfikacji sterownika iSKD-4 w zakresie zgodności z wymaganiami zapisanymi w LonMark Interoperability. Pokazano sam proces certyfikacji, jak również problemy związane z doborem profilu funkcjonalnego oraz zmiennych sieciowych. Poprzez realizację wymienionych powyżej certyfikacji sterownika iSKD-4 wykazano możliwość wprowadzenia na rynek automatyki budynków sterowników, które integrują w sobie funkcjonalności systemów automatyki i systemów bezpieczeństwa. Dzięki takiej integracji na poziomie indywidualnych pomieszczeń uzyskuje się łatwość wdrażania systemów automatyki spełniających wymagania normy EN 15323 w zakresie indywidualnego sterowania w zależności od zapotrzebowania na energię w pomieszczeniu.

Słowa kluczowe: kontrola dostępu, sygnalizacja włamania i napadu, automatyka pomieszczeniowa, integracja, LonWorks, certyfikacja, LonMark, świadectwo kwalifikacyjne, badania EMC, dyrektywa LVD

Abstract: *The paper deals with conformance testing and certifications of integrated building automation and security controller iSKD-4. It integrates functions of Access Control and Intruder Hold-Up & Alarm Systems with room automation functions – control according to room occupancy state. The controller was designed according to requirements of suitable standards for alarm systems, was tested and received certificate which confirms its security class.*
The paper presents also LonMark Certification Programs and complete certification process of the iSKD-4 controller for compliance with the LonMark Interoperability Guidelines was shown. Also problems with functional profile selection and network variables selection were shown. Through above mentioned certifications of the iSKD-4, the possibility of introduction to the building automation market of controllers which integrate automation and security, was proven. The integration on the level of single rooms results in simpler implementation of automation systems which fulfill requirements of EN 15232 standard in the field of individual control according to energy demand in individual rooms.

Keywords: access control, intruder & hold-up alarm system (I&HAS), room automation, integration, LonWorks, certification, LonMark, conformance certificate, EMC audit, LVD directive

[1] Artykuł przedstawia część wyników prac współfinansowanych w ramach projektu POIG.01.04.00-12-105/11 pt. "Opracowanie platformy technologicznej dla zintegrowanych sterowników automatyki i bezpieczeństwa budynków"

1 WPROWADZENIE

Celem dla współczesnych systemów automatyki jest zapewnienie wysokiej efektywności wykorzystania energii i ścisłej kontroli jej wykorzystania, przy jednoczesnym zapewnieniu wymaganego stopnia komfortu. Nie mniej ważną funkcją pełnioną przez te systemy jest zapewnienie bezpieczeństwa użytkowników jak i bezpieczeństwa mienia znajdującego się w budynku, poprzez realizację kontroli dostępu uprawnionych użytkowników do wydzielonych, kontrolowanych stref budynku, jak i systemu alarmowego – systemu sygnalizacji włamania i napadu. Realizacja wszystkich wymienionych funkcji w czasie rzeczywistym i bez sztucznych ograniczeń (np. niekompatybilności struktur danych wynikających ze stosowania różnych zamkniętych protokołów komunikacyjnych i konieczności integracji na poziomie centralek, systemów nadrzędnych, itp.) możliwa jest tylko poprzez integrację tych systemów na poziomie obiektowym, w jednej spójnej sieci sterowania.

W artykule zaprezentowano sterownik iSKD-4, zaprojektowany z myślą o zintegrowaniu funkcji kontroli dostępu, sygnalizacji włamania i napadu oraz automatyki pomieszczeniowej. Wszystkie te funkcje zostały zaprojektowane i zrealizowane zgodnie z wymaganiami odpowiednich norm i wytycznych, a sterownik został przebadany i uzyskał stosowne certyfikaty i świadectwa. Sterownik wyposażony jest w interfejs dla sieci LonWorks, stąd jednym z wymagań jest spełnienie stosownych Profili Funkcjonalnych organizacji LonMark. W dalszej części przedstawiono również wytyczne oraz problemy certyfikacji LonMark jak i wymagania związane z systemami alarmowymi zabezpieczenia mienia, również przebadane i pozytywnie spełnione przez sterownik iSKD-4.

2 STEROWNIK AUTOMATYKI I BEZPIECZEŃSTWA ISKD-4

iSKD-4 to sterownik przystosowany do obsługi pojedynczego pomieszczenia w zakresie kontroli dostępu, kontroli obecności i energooszczędnego sterowania oświetleniem oraz sygnalizacji włamania i napadu. Kontrola dostępu obsługuje zarówno przejścia 1-stronne jak i 2-stronne. Funkcjonalność SWiN obsługuje pojedynczą chronioną strefę (np. pojedyncze pomieszczenie, korytarz), z możliwością łączenia grup pomieszczeń w większe strefy podlegające ochronie.

Fizyczne wejścia i wyjścia sterownika iSKD-4 zapewniają obsługę pełnego osprzętu przejścia, tzw. APAS (Access Point Actuators and Sensors) w sposób zgodny z wymaganiami normy PN-EN 50133-1. W skład obsługiwanego APAS (osprzętu przejścia) wchodzą:

- czytniki kart i klawiatury z sygnalizacją trybu pracy przejścia i akceptacji karty/kodu,
- parametryzowane czujki ruchu,
- elektrozaczep (sterowanie, monitoring i opcjonalne zasilanie),

- przycisk wewnętrzny normalnego otwarcia drzwi,
- przycisk wewnętrzny do awaryjnego otwarcia drzwi,
- styk alarmu pożarowego (monitoring),
- przycisk zgłoszenia napadu,
- sygnalizatory optyczny i akustyczny napadu i włamania (nieuprawnionej obecności),
- kontaktrony sygnalizacji otwarcia drzwi oraz otwarcia okna,
- sygnalizacja dla zewnętrznych systemów faktu otwarcia drzwi.

W celu zapewnienia integralności systemu jak i wymaganego przez normy poziomu zabezpieczenia mienia, dla sterownika iSKD-4 objęte kontrolą sabotażu (styki tamper) zostały następujące elementy systemu:

- czujki ruchu,
- sygnalizatory optyczny oraz akustyczny,
- czytniki kart i kodów,
- kontaktrony,
- przycisk napadu,
- obudowa (otwarcie) i połączenia wewnętrzne.

Poprzez pomiar napięć, prądów czy rezystancji oraz kontrolę transmisji cyfrowej z określonymi elementami systemu, sterownik iSKD-4 wykrywa uszkodzenia:

- czujek ruchu,
- sygnalizatorów optycznego i akustycznego,
- czytników kart i klawiatur,
- zwarcia elektrozaczepu.

Normy dotyczące kontroli dostępu oraz sygnalizacji włamania i napadu (PN-EN 50133 i PN-EN 50131), określają również wymagania względem obudowy sterownika, dostępu do zacisków oraz:

- zasilania podstawowego (z sieci zasilającej) oraz rezerwowego (akumulatora),
- połączeń wewnętrznych (w obwodzie drukowanym),
- logicznych połączeń zewnętrznych (komunikacja z oprogramowaniem zarządzającym)

Spełnienie powyższych wymagań w zakresie norm, pozwala sklasyfikować system oparty na sterowniku iSKD-4 pod kątem funkcjonalności kontroli dostępu (klasa dostępu i klasa rozpoznania) oraz sygnalizacji włamania i napadu (stopień zabezpieczenia). Również jako urządzenie elektroniczne, wprowadzone do obrotu, musi spełniać wymagania w zakresie kompatybilności

elektromagnetycznej (EMC), bezpieczeństwa przeciwporażeniowego (tzw. dyrektywy nisko-napięciowe LVD). Zatem w zakresie kontroli dostępu, sterownik spełnia klasę rozpoznania "2" (identyfikator lub biometryka) i klasę dostępu "B" (wykorzystanie siatki czasowej i rejestracji zdarzeń). W zakresie systemu włamania i napadu sterownik zapewnia stopień zabezpieczenia "2" wg normy PN-EN 50133-1:2009 (ryzyko małe do ryzyka średniego tzn. intruzi lub włamywacze będą mieć ograniczoną znajomość systemu i będą korzystać z narzędzi w zakresie podstawowym i z przyrządów ręcznych), będący odpowiednikiem klasy "C" wg PN-93/E-08390-14:1993. Sterownik znajduje się w klasie środowiskowej "II" (środowisko wewnętrzne ogólne).

2.1 SYSTEM KONTROLI DOSTĘPU I SYGNALIZACJI WŁAMANIA I NAPADU X-SKD

System Kontroli Dostępu i Sygnalizacji Włamania i Napadu X-SKD dedykowany jest do zastosowań w budynkach biurowych lub dydaktycznych, wymagających wdrożenia kontroli dostępu oraz sygnalizacji włamania i napadu w wielu przejściach. Dodatkową zaletą ze stosowania niniejszego systemu jest możliwość integracji na poziomie obiektowym z automatyką budynkową oraz możliwość realizacji systemu nadrzędnego przy pomocy tych samych środków technicznych dla wszystkich funkcji budynku.

System kontroli dostępu i sygnalizacji włamania i napadu składa się ze:

- sterowników iSKD-4,
- osprzętu przejść (APAS: czytników kart bezstykowych, przycisku wyjścia, przycisku awaryjnego otwarcia drzwi, czujniku otwarcia drzwi - kontaktronu i elektrozaczepu),
- urządzeń serwerów kontroli dostępu xSerwer,
- oprogramowania konfiguracyjnego i diagnostycznego,
- opcjonalnie systemu nadrzędnego.

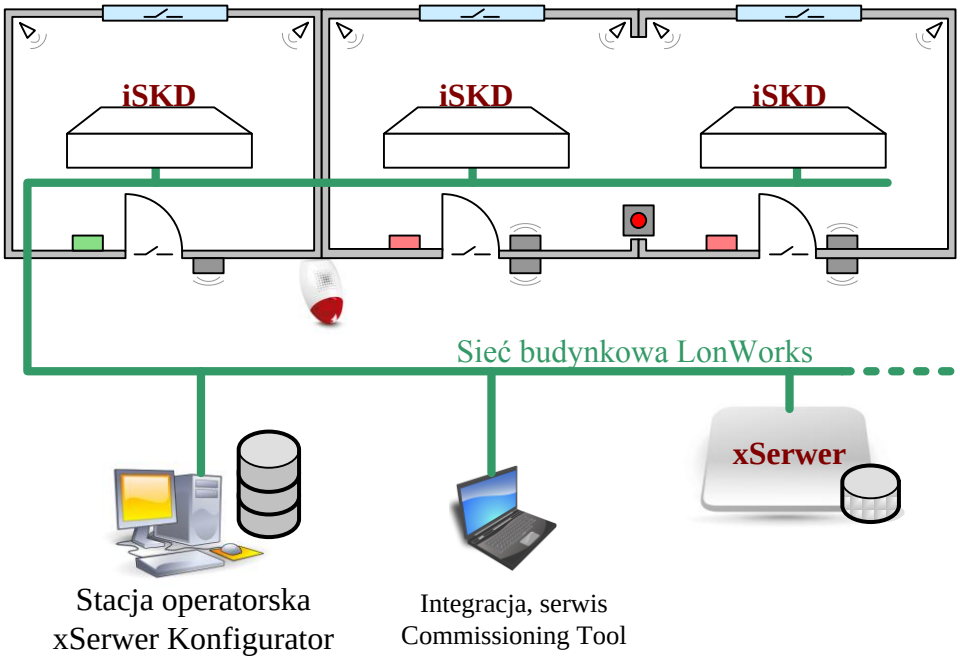
Sterownik iSKD-4 jest podstawą systemu X-SKD, natomiast urządzenie xSerwer obsługuje maksymalnie osiem przejść (sterowników iSKD-4) i pełni rolę bazy danych w której zapamiętywane są dane nt. uprawnionych kart dostępowych i ich siatki czasowej oraz rejestrowane są wszystkie wymagane zdarzenia. Dane przechowywane są w pamięci nieulotnej o pojemności wielokrotnie większej niż wymagana do przechowywania zdarzeń z 30 dni z 8 przejść.

Do konfiguracji, monitorowania i diagnostyki urządzeń xSerwer dostępne jest dedykowane oprogramowanie xSerwer Konfigurator. Umożliwia również odczyt zarejestrowanych logów zdarzeń oraz automatyczną i ręczną synchronizację czasu. Zawiera bazę danych z konfiguracjami wszystkich urządzeń xSerwer dla danego budynku. W przypadku konieczności wymiany urządzenia xSerwer, jego konfiguracja może zostać odtworzona z bazy danych programu xSerwer

Konfigurator. Umożliwia również tworzenie kopii zapasowej całej konfiguracji, co sprowadza się do wykonania kopii zapasowej bazy danych programu xSerwer Konfigurator.

Architektura systemu przedstawiona została na poniższym rys. 1. Obejmuje ona sterowniki iSKD-4 dla każdego przejścia oraz xSerwer. Przejście w mniejszym pomieszczeniu jest 1-stronne, wyposażone w przycisk otwarcia drzwi od wewnętrznej strony przejścia oraz czytnik kart od strony zewnętrznej. Przejście oraz okno chronione są przy pomocy kontaktronów. Dwa przejścia w dużym pomieszczeniu są przejściami dwustronnymi z przyciskami awaryjnego otwarcia drzwi (typu "Zbij szybkę"). Pomieszczenie wyposażone jest w przycisk napadowy, podłączony do dowolnego ze sterowników iSKD-4.

Dla mniejszych instalacji wszystkie elementy systemu X-SKD mogą komunikować się z wykorzystaniem samej sieci TP/FT-10 (łącznie z konfiguracją kart, siatki czasowej i logów zdarzeń), a większe instalacje mogą wykorzystywać szybkie połączenie IP pomiędzy sterownikami xSerwer a komputerem z oprogramowaniem xSerwer Konfigurowator. Komunikacja pomiędzy sterownikami xSerwer a iSKD-4 zawsze odbywa się przy pomocy sieci TP/FT-10. Jest ona wykorzystywana również do integracji niskopoziomowej z innymi elementami systemu automatyki pomieszczeniowej, umożliwiając sterowanie odbiornikami energii na podstawie sygnału z obecności ze sterownika iSKD-4.



Rys. 1. Architektura systemu X-SKD

Ostatnim elementem systemu może być system nadrzędny, na bieżąco monitorujący sterowniki iSKD-4 pod kątem stanu i trybu pracy przejść, alarmów kontroli dostępu oraz sygnalizacji włamania i napadu. Pełni on funkcje zdalnego centrum odbiorczego systemu alarmowego (ARC).

Ponieważ system oparty jest na interfejsach komunikacyjnych TP/FT-10 i wykorzystuje tylko standardowe możliwości technologii LonWorks, jest w pełni otwarty, a jego konfiguracja i integracja możliwa jest z zastosowaniem standardowych narzędzi dla tej technologii, tj. oprogramowania LonMaker, Commissioning Tool lub NL220.

3 WYMAGANIA DLA SYSTEMÓW BEZPIECZEŃSTWA

Jak zostało wspomniane w poprzednim rozdziale, system bezpieczeństwa ma integrować funkcjonalności kontroli dostępu oraz sygnalizacji włamania i napadu. Wymagania dla funkcjonalności kontroli dostępu zebrane zostały w normie PN-EN 50133:2007 pt. "Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia", natomiast dla funkcjonalności sygnalizacji włamania i napadu jest to norma PN-EN 50131:2009 pt. "Systemy alarmowe – Systemy sygnalizacji włamania i napadu".

Dodatkowo norma PN-EN 50130:2012 pt. "Systemy alarmowe" odwołuje się w arkuszu nr 4 do wymagań w zakresie kompatybilności elektromagnetycznej (PN-EN 61000-4-2 do -4-6, 4-11 w zakresie odporności na zaburzenia elektromagnetyczne i PN-EN 55022 w zakresie emisji zaburzeń elektromagnetycznych) oraz w arkuszu nr 5 do prób środowiskowych.

W normie PN-EN 50133 określono klasę zabezpieczenia jako kombinację klasy rozpoznania i klasy dostępu. Klasa rozpoznania (od najniższej 0 do najwyższej 3) określa czynniki, na podstawie których rozpoznany zostaje użytkownik, z uwzględnieniem ryzyka udostępnienia swoich praw osobie trzeciej. Sposoby rozpoznania użytkowników obejmują takie techniki jak przycisk, detektor ruchu, zapytanie o hasło, osobisty identyfikator niemożliwy do odczytania wizualnie (karty dostępu, klucze elektroniczne), dane biometryczne jak również kombinację tych czynników w celu ograniczenia możliwości błędnego rozpoznania.

Drugi składnik klasy zabezpieczenia – klasa dostępu – określa sposób przyznawania dostępu do chronionej strefy i rejestrację tego faktu. Najniższa klasa A nie wymaga ani implementacji siatki czasowej ani rejestracji uzyskania dostępu, klasa Ba wprowadza siatkę czasową, a najwyższa klasa B wymaga zarówno siatki czasowej jak i rejestracji operacji dostępu.

Z kolei klasa środowiskowa określa odporność elementów systemu na warunki zewnętrzne – temperaturę, wilgotność lub dodatkowo inne warunki atmosferyczne, a więc dopuszczalne miejsce zastosowania elementów systemu: od wnętrz typu pomieszczenia biurowe, wnętrz typu magazynowego, korytarzy, środowisk zewnętrznych osłoniętych aż do najwyższej klasy środowisk zewnętrznych nieosłoniętych.

3.1 WYMAGANIA SZCZEGÓŁOWE

W niniejszym podrozdziale podano szczegółowe najważniejsze wymagania w zakresie omawianych funkcjonalności bezpieczeństwa. Można przeprowadzić ich podział ze względu na przetwarzanie danych, ochronę przed sabotażem, ochronę przed zmianami w programie, rozpoznanie, sterowanie kontrolowanym przejściem, anonsowanie, rejestrację oraz komunikację z innymi systemami. Ponieważ dla sterownika wybrano określone klasy rozpoznania, dostępu i stopień zabezpieczenia, podane w rozdziale 2, poniżej podano wymagania właśnie dla tych klas KD i stopnia bezpieczeństwa SWiN. Są to zatem również cechy systemu X-SKD.

W grupie "ochrona przed sabotażem", wymaga się aby osoba nieuprawniona nie mogła uzyskać dostępu do systemu bez użycia narzędzi.

W grupie "przetwarzanie danych", wymaga się zapewnienie możliwości:

- przypisywania użytkownikom czasowych siatek dostępu,
- przypisywania użytkownikom poziomów dostępu,
- przetwarzania danych poza czytnikiem.

W grupie "reguły przetwarzania", wymaga się aby system:

- posiadał co najmniej dwa czasy odblokowania elektrozaczepu (5min i 60s) i co najmniej dwa czasy dozwolonego otwarcia przejścia (każdy sterownik iSKD-4 może posiadać indywidualnie ustawiane czasy),
- posiadał wbudowany zegar o minimalnym cyklu tygodniowym i maksymalnym błędzie 5sek/dzień,
- zapewniał siatkę czasową o minimalnej rozdzielczości dzień tygodnia + minuta doby.

W grupie "ochrona przed zmianami w programie", system ma:

- uniemożliwiać nieuprawnione zmiany zaprogramowanych zasad (kodów dostępu, haseł, siatki czasowej) – np. dodatkowe kody dostępu,
- umożliwiać administratorowi zmianę haseł,
- zapewniać minimalną liczbę kombinacji na poziomie 10000 (4-cyfrowy PIN).

W grupie "rozpoznanie", wymaga się:

- zapewnienia możliwości przypisania do użytkownika niepowtarzalnej w systemie cechy identyfikacyjnej (karty dostępowe mają unikalne identyfikatory),
- przynajmniej 1000000 kodów rozpoznawczych (stosowane de-facto karty zapewniają 10^{10} kombinacji),
- zapewnienia aby odsetek fałszywych akceptacji był nie większy niż 0,01%, a fałszywych odrzuceń nie większy niż 1%,
- nie stosowania identyfikatorów z kodem widocznym gołym okiem (kod nie może stanowić całości numeru identyfikacyjnego).

W grupie "sterowanie kontrolowanym przejściem", system:

- musi bezpośrednio sterować osprzętem przejść i kontrolować stan jego zabezpieczenia,

- musi dozorować stan otwarcia lub zamknięcia przejścia (kontaktron drzwiowy),
- posiadać złącza do kontrolowanego przejścia wewnątrz obudowy z kontrolą otwarcia obudowy,
- musi zapewniać wyjście sterujące przejściem zrealizowane izolowanym galwanicznie przełącznikiem o obciążeniu co najmniej 30VA,
- ma aktywować wyjście sterujące przejściem w chwili przyznania dostępu i kasować go po zaprogramowanym czasie lub wykryciu stanu otwarcia,
- ma zapewnić brak dostępu do złącz od strony o niższym poziomie zabezpieczenia (wymaganie musi zostać spełnione również po stronie projektanta konkretnej instalacji).

W grupie "anonsowanie", wymaga się:

- przedstawienia alertu w przypadku: wykrycia sabotażu, otwarcia kontrolowanego przejścia bez przyznania dostępu, wykrycia stanu otwarcia po upływie dozwolonego czasu od przyznania dostępu (stąd wynikają typy alarmów przejścia w systemach kontroli dostępu),
- zapewnienia opóźnienia alertu nie dłuższego niż 10 sekund (system działa zdarzeniowo z ustawianymi powtórzeniami transmisji).

W grupie "rejestracja", wymaga się zarejestrowania faktu:

- wykrycia sabotażu (z jego lokalizacją),
- programowania systemu,
- otwarcia przejścia bez przyznania dostępu,
- wykrycia stanu otwarcia po dozwolonym czasie po przyznaniu dostępu,
- transakcji przyznawania oraz odmowy dostępu (wraz z identyfikatorem i lokalizacją zdarzenia).

Opóźnienie zapisu rejestrowanych zdarzeń do pamięci nieulotnej musi być nie większe niż 60s, zawierać informację o dacie, czasie i typie zdarzenia. System musi mieć możliwość rejestracji co najmniej 500 zdarzeń przez 30 dni (wymaganie spełnione z dużym nadmiarem z uwagi na pojemność dostępnych kart pamięci).

W grupie "komunikacja z innymi systemami", system:

- dla każdego przejścia ma udostępniać wyjście informacji o uprawnionym dostępie,
- nie może przyznawać dostępu przy zmianie statusu komunikacji (łączność nawiązana/utracona).

W zakresie zasilania osprzętu przejścia, nie wymaga się dostarczania zasilania przez sterownik. Ma to szczególne znaczenie przy zasilaniu rezerwowym i stosowaniu elektrozaczepów rewersyjnych, które w stanie zamknięcia wymagają ciągłego zasilania. Mimo to, w urządzeniu integrującym funkcje kontroli dostępu i sygnalizacji włamania i napadu, jednym z głównych technicznych wyzwań jest spełnienie wymagania dotyczącego zasilania rezerwowego. W tabelach 23. i 24. normy PN-EN 50131-1:2006 podano minimalny okres gotowości zasilacza rezerwowego

i czas potrzebny na doładowanie. Dla sterownika iSKD-4 zastosowano zasilanie typu A, tj. sieć elektroenergetyczna i rezerwowe doładowywane źródło zasilania (akumulator). Różnica pomiędzy stopniami zabezpieczenia 1, 2 a 3 i 4 jest 5-krotna dla minimalnego okresu gotowości (12h dla stopni 1 i 2 oraz 60h dla stopni 3 i 4) oraz 3-krotna dla okresu doładowania (72h dla stopni 1 i 2 oraz 24h dla stopni 3 i 4).

4 PROGRAMY CERTYFIKACJI LONMARK

LonMark International jest organizacją międzynarodową, która opracowała i prowadzi programy certyfikacji, promujące i wspierające rozwój kompetencji i oferty urządzeń automatyki zgodnych z międzynarodowym i europejskim standardem ISO/IEC 14908 / EN 14908 / ANSI/CEA 709.1. Należą do nich program certyfikacji kwalifikacji zawodowych oraz program certyfikacji urządzeń. W ramach kwalifikacji zawodowych, po weryfikacji stosownej wiedzy, osoba może uzyskać tytuł LonMark Certified Professional, a instytucja tytuł LonMark Certified System Integrator. Natomiast w programie certyfikacji urządzeń weryfikuje się zgodność urządzeń z wytycznymi służącymi zapewnieniu współdziałania urządzeń automatyki różnych producentów (bez urządzeń pośredniczących).

4.1 CERTYFIKACJA ZAWODOWA

Program certyfikacji kwalifikacji zawodowych służy potwierdzeniu (poprzez poddanie się stosownym egzaminom) wiedzy niezbędnej do projektowania, instalacji, integracji i uruchamiania systemów opartych na technologii LonWorks. Poprawne wdrożenie rozproszonego systemu automatyki jak również jego dalsze utrzymanie i konserwacja, wymaga stosownej wiedzy. Można ją nabyć, a przede wszystkim zweryfikować w laboratorium AutBudNet AGH. Jest to jedyne miejsce w Europie, gdzie taka możliwość została zapewniona. Dalszym krokiem certyfikacji jest program LonMark Certified System Integrator, w ramach którego instytucja, organizacja lub firma świadcząca usługi w zakresie doradztwa, projektowania i wdrażania systemów automatyki na bazie technologii LonWorks, może uzyskać potwierdzenie swoich kompetencji. Instytucja taka musi zatrudniać co najmniej dwie osoby legitymujące się tytułem LonMark Certified Professional oraz posiadać kompetencje techniczne i wykazać się doświadczeniem potwierdzonym wykonanymi projektami integracji systemów automatyki.

4.2 CERTYFIKACJA URZĄDZEŃ

Drugą możliwością certyfikacji jest program certyfikacji urządzeń, w ramach którego weryfikowana jest zgodność urządzenia poddawanego badaniom z wytycznymi zapisanymi w dokumentach LonMark Interoperability Guidelines. Są to dwa dokumenty określające zachowanie każdej z warstw protokołu LonTalk oraz (co najważniejsze) zestawy zmiennych i parametrów sieciowych używanych przez urządzenie pełniące określoną funkcję automatyki. Producent chcący poddać urządzenie certyfikacji musi wykazać i udokumentować znajomość wytycznych oraz ich zastosowanie w konstrukcji urządzenia. Interfejs sieciowy urządzenia i jego oprogramowanie poddawane są dwuetapowym badaniom poprzez dwie aplikacje do certyfikacji. Pierwsza z nich pracuje w siedzibie organizacji LonMark, a wybrane jednostki organizacyjne mają zapewniony zdalny dostęp do tej aplikacji. Po przejściu pierwszego etapu badań, jednostka certyfikująca otrzymuje drogą elektroniczną kolejną aplikację, badającą rzeczywistą komunikację z urządzeniem. Po spełnieniu przez urządzenie wymagań formalnych i zweryfikowaniu zgodności z wytycznymi LonMark Interoperability Guidelines, producent urządzenia otrzymuje certyfikat potwierdzający zgodność pracy urządzenia z wytycznymi LonMark, prawo do umieszczania na urządzeniu oznaczenia LonMark, a wpis o urządzeniu umieszczony zostaje w międzynarodowym, ogólnodostępnym w sieci Internet katalogu organizacji LonMark, zawierającym urządzenia różnych producentów z całego świata. Urządzenie jest również prezentowane na łamach czasopisma LonMark Magazine, jako promocja nowego urządzenia spełniającego wymagania interoperacyjności. Dzięki zawarciu porozumienia pomiędzy AGH a LonMark International, również ten rodzaj certyfikacji dostępny jest w laboratorium AutBudNet AGH.

4.3 CERTYFIKACJA LONMARK INTERFEJSU SIECIOWEGO STEROWNIKA ISKD-4

Sterownik iSKD-4 posiada fizyczny interfejs komunikacyjny dla sieci TP/FT-10 (skręcona para przewodów) z zaimplementowanym protokołem LonTalk. Umożliwia on przesyłanie dowolnych wiadomości, w tym wartości dowolnych zmiennych sieciowych. Aby sterownik mógł wymieniać dane z innymi sterownikami, należy użyć określonego zestawu zmiennych sieciowych, o określonych typach danych (SNVT – ang. Standard Network Variable Type). Zestaw zmiennych sieciowych i parametrów konfiguracyjnych, pogrupowanych w bloki funkcjonalne, zgodne z tzw. profilem funkcjonalnym, nazywany jest interfejsem sieciowym urządzenia i zapisywany jest w formacie XIF (ang. eXternal Inteface File).

Plik XIF zawiera również unikalny identyfikator aplikacji sterownika (tzw. ProgramID). Zawiera on następujące informacje:

- identyfikator producenta nadawany przez LonMark International,
- identyfikator głównego profilu funkcjonalnego urządzenia,
- obszar zastosowań sterownika,
- typ fizycznego interfejsu sieciowego,
- wersję aplikacji.

Aplikacja sterownika może mieć zaimplementowanych wiele funkcjonalności należących do kilku profili funkcjonalnych. Każdy z nich będzie definiował zbiór zmiennych sieciowych i parametrów konfiguracyjnych, o statusie obowiązkowych oraz opcjonalnych. Każdy profil funkcjonalny ma przypisany indywidualny identyfikator. W identyfikatorze ProgramID zamieszcza się tylko identyfikator dla profilu, który będzie uznawany za podstawowy.

Należy nadmienić, że każdy producent zarządza listą swoich numerów ProgramID, zapewniając ich pełną unikalność. Każda aplikacja różniąca się zestawem zmiennych (plikiem XIF), musi posiadać unikalny ProgramID.

Następnym krokiem jest utworzenie tzw. zasobów (ang. ResourceFiles). Definiują one użyte w sterowniku typy bloków funkcjonalnych, typy wyliczeniowe producenta oraz typy zmiennych sieciowych i parametrów konfiguracyjnych producenta (ang. manufacturer specific). Zasoby grupują definicje typów w różnych zakresach (ang. scope), przypisanych np. producentowi lub w węższym zakresie - określonej klasie jego urządzeń. Można w ten sposób zdefiniować np. ogólno-firmowe typy wyliczeniowe lub specyficzne tylko dla danej klasy urządzeń.

W kolejnym kroku opracowuje się aplikację sterownika, tworząc kod programu w środowisku NodeBuilder w języku NeuronC, wykorzystując uprzednio zdefiniowane w zasobach typy bloków funkcjonalnych i typy zmiennych sieciowych. Pierwsza część programu zawiera m.in. deklaracje zmiennych sieciowych. Podczas kompilacji powstaje kod wynikowy aplikacji oraz plik z interfejsem sieciowym XIF. Kompilator oprócz błędów uniemożliwiających wygenerowanie kodu wynikowego, podaje również ostrzeżenia w zakresie niezgodności z wytycznymi procesu certyfikacji. Przykładowo, użycie wycofanego typu zmiennej sieciowej SNVT_lev_disc spowoduje wygenerowanie ostrzeżenia, że aplikacja nie uzyska certyfikatu LonMark.

Mając przygotowane zasoby i interfejs sieciowy oraz aplikację, można przystępować do certyfikacji. Po wniesieniu opłat członkowskich LonMark, uzyskuje się dostęp do członkowskiej części portalu LonMark oraz do narzędzia SCT (ang. Self-Certification Tool). Jest to aplikacja webowa, dzięki której część procesu certyfikacji jest obsługiwana przez producenta urządzenia. Czynności wykonywane w SCT są następujące:

1. Założenie projektu certyfikacji z podaniem danych kontaktowych producenta urządzenia, jego opisu, innych uzyskanych certyfikatów, identyfikatora ProgramID.
2. Otrzymanie aktywacji projektu przez LonMark International (zwykle następnego dnia).
3. Udzielenie odpowiedzi na maksymalnie 60 pytań w zakresie spełnienia wymagań dokumentów LonMark Layer 1-6 Interoperability Guidelines i LonMark Application-Layer Interoperability Guidelines (ponad 170 stron) w zakresie warstw protokołu LonTalk i wykorzystywanych w urządzeniu sposobów komunikacji (odpowiedź na jedno pytanie może wyłączyć z zestawu pytań inne pytania, np. jeżeli nie jest używany koprocesor, nie odpowiada się na pytania z nim związane).
4. Wysłanie kompletu plików zasobów (zasoby producenta, klasy urządzenia, itd.) oraz ich walidacja. W przypadku wykazania błędu, konieczna jest ponowna edycja zasobów, przekompilowanie aplikacji, wysłanie i walidacja plików zasobów.
5. Wysłanie pliku interfejsu sieciowego XIF oraz jego walidacja; w przypadku błędu niezgodności XIF z wytycznymi, konieczna jest korekta aplikacji, jej przekompilowanie i ponowne wysłanie i walidacja pliku XIF. Możliwa jest również sytuacja, gdy błąd w interfejsie XIF wynika z niezgodności z użytymi zasobami. Może być wówczas konieczny powrót do edytora zasobów i podjęcie kolejnej próby walidacji kompletu plików zasobów oraz interfejsu XIF.
6. Wykonanie testu fizycznej komunikacji ze sterownikiem. Wymaga to pobrania aplikacji Physical Test Utility i pobrania definicji testu fizycznego (plik XML pobierany na podstawie tokenu projektu). Po podłączeniu testowanego sterownika, testowane jest zachowanie urządzenia podczas komisjonowania, ustawiania trybu Online, resetu programowego oraz obsługa poleceń LonMark bloków funkcjonalnych urządzenia (Node Object oraz pozostałych zaimplementowanych w urządzeniu bloków funkcjonalnych) oraz odczytu zmiennych sieciowych.
7. Test fizycznej komunikacji ze sterownikiem jest ostatnią czynnością podczas której można jeszcze wprowadzić zmiany w certyfikowanym urządzeniu. Nawet gdy urządzenie pozytywnie przejdzie test fizyczny, można jeszcze zmienić pliki zasobów, aplikację, interfejs XIF i ponownie poddać urządzenie walidacji oraz testowi fizycznemu. Po uzyskaniu pozytywnych wyników wszystkich walidacji i testu fizycznego, należy zatwierdzić ten etap certyfikacji klikając przycisk "Certify".

Po wykonaniu wszystkich kroków przy pomocy aplikacji webowej Self-Certification Tool, proces certyfikacji przejmowany jest przez organizację LonMark International. Personel techniczny

weryfikuje przebieg auto-certyfikacji, dokonuje dodatkowych weryfikacji dostarczonych plików i jeżeli zajdzie taka potrzeba, kontaktuje się poprzez pocztę elektroniczną w celu udzielenia dodatkowych wyjaśnień. Gdy certyfikowane urządzenie nie budzi wątpliwości, wystawiany jest certyfikat zgodności z wymaganiami LonMark, z podaniem wersji wytycznych.

5 PODSUMOWANIE

Podczas projektowania sterownika iSKD-4 brano pod uwagę możliwość zintegrowania w sterowniku funkcji pełnionych przez systemy bezpieczeństwa z funkcjami automatyki pomieszczeniowej. Zaimplementowano w sterowniku funkcje kontroli obecności i sterowania oświetleniem z uzależnieniem od stanu zajętości pomieszczenia. Elementem koniecznym do sterownia oświetleniem jest jedynie zastosowanie modułu wyjść fizycznie sterujących oprawami oświetleniowymi oraz wejścia informującego o potrzebie załączenia oświetlenia (łącznika natynkowego, panelu dotykowego lub dowolnego innego interfejsu użytkownika). Z powodzeniem zaprojektowano interfejs sieciowy spełniający wymagania możliwości współdziałania (ang. interoperability) wg LonMark Interoperability Guidelines. Dla klasy urządzeń systemów kontroli dostępu, istnieją szczegółowo zdefiniowane profile funkcjonalne z określeniem zestawu zmiennych i znaczenia ich wartości (np. tryby pracy przejścia).

Jednak dla prawie połowy klas urządzeń (zastosowań), zdefiniowany jest jedynie identyfikator klasy, bez specyfikacji technicznej nazw zmiennych, ich znaczenia i wartości. Producenci muszą implementować swoje bloki funkcjonalne z własnymi zmiennymi sieciowymi, które nie będą zgodne ze zmiennymi innych producentów. Powoduje to, że w wielu zastosowaniach nie jest zapewniona możliwość współdziałania urządzeń różnych producentów.

Kolejny problem z certyfikacją interfejsu sieciowego dotyczy zmiennych wielostanowych. Typ zmiennej sieciowej SNVT_lev_disc został wycofany i nie może być używany w certyfikowanych urządzeniach. Zamiast niego oficjalna specyfikacja typów SNVT poleca używanie typu SNVT_switch, ten jednak nie definiuje konkretnych stanów, umożliwiając używanie np. dyskretnych wartości 0%-100% z rozdzielczością 0,5% na polu value. Z jednej strony daje możliwość zakodowania większej ilości stanów niż SNVT_lev_disc (6 stanów), jednak nie definiuje które wartości reprezentują wartość prawidłową, a które nie. Chcąc np. zdefiniować 5 trybów sterowania oświetleniem, można je przypisać do wartości value 0, 25, 50, 75, 100, a wartości pośrednie uznać za nieprawidłowe. Lepszym rozwiązaniem wydaje się zdefiniowanie własnego typu wyliczeniowego producenta i zmiennej sieciowej używającej tego typu. Wówczas

poszczególne stany można oznaczyć symbolami listy wyliczeniowej, np. LIGHT_OFF, LIGHT_OCC, LIGHT_PANEL, LIGHT_OCC_PANEL, LIGHT_ON.

Używanie sterownika w zastosowaniach wymagających potwierdzonego stopnia zabezpieczenia systemu SWiN lub klasy systemu KD możliwe jest dzięki zaprojektowaniu go zgodnie ze stosownymi normami, a co nie mniej ważne, zweryfikowaniu tej zgodności i potwierdzeniu jej przy pomocy stosownych badań, certyfikatów i świadectw kwalifikacyjnych. W zakresie systemów bezpieczeństwa, sterownik będący częścią systemu X-SKD uzyskał Świadectwo Kwalifikacyjne nr 01/15 wydane przez Zakład Rozwoju Technicznej Ochrony Mienia TECHOM. Posiadane przez system dokumenty potwierdzające zgodność z określonymi wymaganiami norm są na pewno elementem wyróżniającym go wśród wielu innych dostępnych na rynku. Problemem jest jednak adaptacja do aktualnego stanu norm – nadal często można spotkać klasyfikację wg normy PN-93/E-08390 z 1994 roku, zamiast stosowania norm PN-EN 50133 i PN-EN 50131.

Przeprowadzone prace wykazały możliwość i celowość wprowadzenia na rynek automatyki budynków zintegrowanych sterowników, które realizują zarówno funkcje systemów bezpieczeństwa, jak i funkcje systemów automatyki budynków ze sterowaniem energią w zależności od zapotrzebowania.