Powszechnie przyjęte rozwiązania - sposób zapewnienia cyberbezpieczeństwa w produkcie

Code of practice - method for assuring cybersecurity in product

Marek Kuciński

Mgr inż.

voestalpine Signaling Poland Sp. z o. o.

marek.kucinski@voestalpine.com

Mariusz Buława

Dr inż.

voestalpine Signaling Poland Sp. z o. o.

mariusz.bulawa@voestalpine.com

Streszczenie: Wdrożenie cyberbezpieczeństwa w systemach sterowania ruchem kolejowym nie jest zadaniem łatwym. Zgodnie ze zdefiniowanymi procesami bezpiecznego wytwarzania produktów (w szczególności zdefiniowanymi w IEC62443-4-1 i TS50701) wymagane jest podjęcie zadań takich jak: analiza zagrożeń, definicja wymagań, projekt i implementacja, weryfikacja i testowanie. Proces ten można znacząco uprościć wykorzystując powszechnie przyjęte rozwiązania (ang. c*ode of practice*). W artykule przedstawiono przykładowe wykorzystanie tej możliwości w kontekście sterownika obiektowego zgodnego z wymaganiami EULYNX.

Słowa kluczowe: *Cyberbezpieczeństwo; EULYNX; Sterownik Obiektowy; TS50701; IEC62443*

Abstract: Introducing cybersecurity in railway traffic command and control systems is not an easy task. Conforming to defined processes of secure product development (especially defined in IEC62443-4-1 and TS50701) there are required tasks to be done such as: threat analysis, requirements definition; design and implemmentation, verification and testing. This process could be significantly simplified with utilization of the industry approved codes of practice. In the article an example showing this possibility was given based on the EULYNX compliant Object Controller.

Keywords: *Cybersecurity; EULYNX; Object Controller; TS50701; IEC62443*

Wstęp

Wzrastający poziom zagrożeń, zarówno lokalnych jak i globalnych, powoduje, że wdrożenie cyberbezpieczeństwa w produktach staje się nie tylko tematem ważnym, ale i obowiązkowym. Nadchodzące wejście w życie wymogów dyrektywy NIS2 [1] nałoży na wiele podmiotów z branży transportu szereg wymogów tak formalnych jak i technicznych. Odkładanie w wielu firmach inwestycji w obszarze cyberbezpieczeństwa spowodowało, że dystans do nadrobienia jest znaczny. Powoduje to potrzebę stosowania efektywnych i adekwatnych metod w celu jak najszybszego osiągnięcia pożądanego poziomu cyberbezpieczeństwa.

Cyberbezpieczeństwo na kolei a normy

W szczególności systemy sterowania ruchem kolejowym, ze względu na ich rolę w całym systemie kolejowym, wymagają szczególnej uwagi. Potencjalne błędne zadziałanie może doprowadzić do utraty zdrowia i życia wielu ludzi lub szkód materialnych w znacznym rozmiarze. Stąd wiele z tych systemów musi zapewnić poziom integralności bezpieczeństwa SIL-4.

Dotąd stosowane metodyki związane z bezpieczeństwem funkcjonalnym, zdefiniowane przez CENELEC w grupie norm EN50126, EN50128 czy EN50159, nie zapewniają wystarczającego poziomu ochrony przed intencjonalnymi próbami naruszenia integralności systemów. Stąd konieczość sięgnięcia do opracowań definijących kompleksowe podejście do cyberbezpieczeństwa w produkcie. Dobrym punktem odniesienia jest zespół norm IEC62443, w szczególności części -4-1 [2] i -4-2 [3]. Pierwsza z nich definiuje wymagania procesowe i organizacyjne dla dostawców komponentów i podsystemów. Druga grupuje i wymienia konkretne wymagania techniczne, które powinny być zaimplementowane w komponentach i podsystemach. Dobór właściwych i adekwatnych rozwiązań bazujących jedynie na powyższych normach jest zadaniem trudnym, obarczonym znacznym ryzykiem.

Trudność ta została już zauważona przez ekspertów z branży kolejowej. W celu usprawnienia zrozumienia potrzeb a następnie właściwej ich implementacji opracowana została specyfikacja techniczna TS50701 [4], której celem jest wdrożenie wymagań i rekomendacji związanych z wdrożeniem cyberbezpieczeństwa na kolei. Prezentuje ona odniesienie pomiędzy implementacją cyberbezpieczeństwa i bezpieczeństwa funkcjonalnego zgodnie z modelem V. Procesy zostały podzielone na fazy, które są jasno zdefiniowane i następują po sobie.

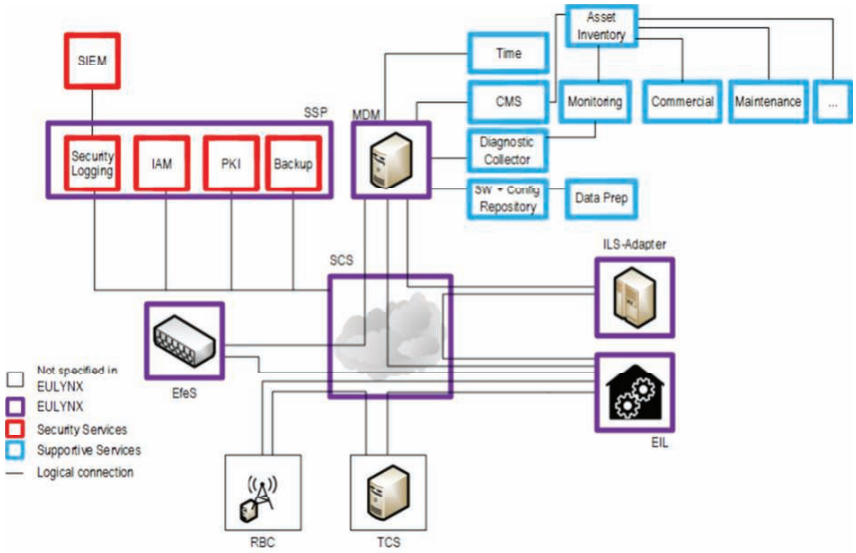
1. Dr inż. Mariusz Buława, Prezes Zarządu voestalpine Signaling Poland podczas prezentacji na Międzynarodowej Konferencji naukowo-technicznej „IT/OT w transporcie szynowym" w Warszawie

2. Mgr inż. Marcin Kuciński z voestalpine Signaling Poland prezentujący „Powszechnie przyjęte praktyki a wdrożenie cyberbezpieczeństwa w produkcie" podczas Międzynarodowej Konferencji naukowo-technicznej „IT/OT w transporcie szynowym" w Warszawie

Inicjatywa EULYNX

Przykładem praktycznego podejścia do zapewnienia cybersecurity w systemach sterowania ruchem kolejowym są wymagania opracowane w ramach inicjatywy EULYNX. Pierwszym krokiem, od którego należy zacząć jest zidentyfikowanie systemu i jego otoczenia (ang. System Definition) oraz podzieleniu go na strefy bezpieczeństwa połączone konduktami [5]. Przykładowe podejście zaprezentowano na rys. **3**. Tak zdefiniowana jest architektura systemu w kontekście cyberbezpieczeństwa w specyfikacjach EULYNX [7].

W kontekście sterowników obiektowych (EfeS) widoczne są dwa połączenia (kondukty) – pierwszy do cyfrowego interlockingu (EIL) a drugi do systemu monitoringu, diagnostyki i utrzymania (MDM). Dla każdej strefy i konduktu należy przeprowadzić analizę zagrożeń. Składa się ona z dwóch kluczowych elementów podlegających ocenie: prawdopodobieństwa (ang. likelihood) oraz znaczenia (ang. severity). Korzystając z tych dwóch określonych współczynników można przystąpić do przypisywania rozwiązań adekwanych do ryzyk, których poziom nie jest akceptowalny, względem przyjętych założeń.



3. Architektura systemu w kontekście cyberbezpieczeństwa w EULYNX [7]

Kodeks postępowania

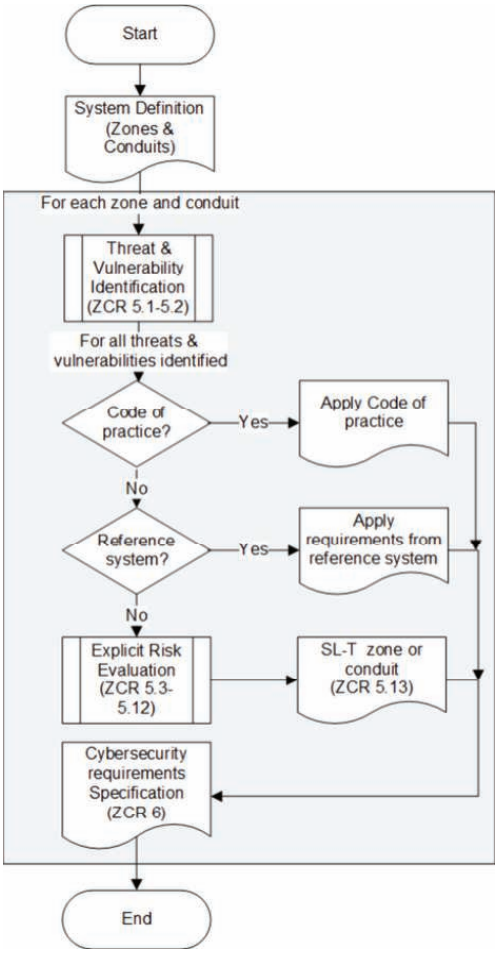
W normie TS50701 szczególnie interesująca jest zaproponowana metodyka szczegółowej oceny ryzyka (rys. **4**). Wskazano dwie możliwości uproszczenia analizy ryzyka z wykorzystaniem kodeksu postępowania lub systemu referencyjnego. Skorzystanie z tych możliwości pozwala znacząco uprościć proces doboru właściwych rozwiązań. Szczególnie korzystne jest wykorzystanie powszechnie przyjętych przez ekspertów branżowych rozwiązań tzw. kodeksów postępowania. Warto przytoczyć tu definicję [4]:

3.1.21 kodeks postępowania
<w cyberbezpieczeństwie> spisany zestaw reguł, zatwierdzony przez grupę ekspertów, który jeśli zostanie poprawnie zastosowany, może zostać wykorzystany do ograniczenia jednego lub więcej zagrożeń
3.1.21 code of practice
<in cybersecurity> written set of rules, validated by a group of experts, that, when correctly applied, can be used to control one or more specific threats

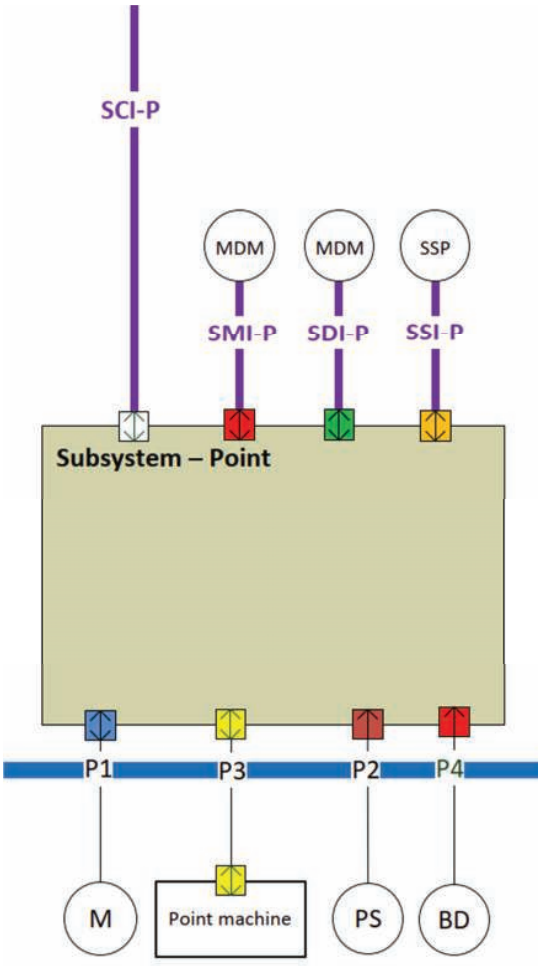
Sterownik obiektowy i jego interfejsy

Dobrym przykładem wykorzystania tej możliwości jest specyfikacja EULYNX Baseline 4 Release 2 (najnowsza aktualnie dostępna). W architekturze dla każdego komponentu (np. sterowników obiektowych) zdefiniowano komplet interfejsów. Przykładowo dla sterownika obiektu typu rozjazd (ang. point) wskazano m.in. interfejsy SCI-P, SDI-P, SMI-P i SSI (rys. **5**). Aby nie przeprowadzać szczegółowej analizy względem wszystkich zagrożeń dla interfejsów zdecydowano się na wybranie powszechnie uznanego za bezpieczny interfejsu TLS w wersji 1.3 (rys. **6**) [7]. Dobór tego protokołu pozwolił ograniczyć do pomijalnego poziomu m.in. poniższe zagrożenia:

1) Naruszenie poufności – cała komunikacja jest szyfrowana kluczem symetrycznym, który jest negocjowany unikalnie dla każdej sesji.
2) Naruszenie integralności – każda wiadomość posiada zabezpieczenie w postaci MAC (ang. Message Authentication Code) co umożliwia wykrycie usunięcia lub podmiany w treści przesyłanej informacji.
3) Podszywanie i zaprzeczalność – połączenia nawiazywane są z wy-



***4**. Diagram szczegółowej analiza ryzyka [4]*



***5**. Definicja interfejsów dla sterownika obiektu typu rozjazd [6]*

***6**. Połączenie między sterownikiem obiektowym a cyfrowym interlockingiem [7]*

korzystaniem kryptografii asymetrycznej. Dzięki temu uczestnicy komunikacji mogą być pewni, że partnerzy są tymi, za których się podają.

4) Atak powtórzenia – ramki są podpisywane przez MAC z uwzględnieniem numeru sekwencyjnego (który nie jest przesyłany w wiadomości) stąd usunięcia czy powtórzenia są wykrywalne.

Dzięki powyższym cechom połączenie przez interfejsy prowadzone konduktami chronionymi przez TLS 1.3 można uznać za odpowiednio zabezpieczone.

Podsumowanie

Przed dostawcami systemów sterowania ruchem kolejowych stoi duże wyzwanie w postaci zapewnienia zgodności z wymaganiami cyberbezpieczeństwa. Zagadnienie jest złożone zarówno organizacyjnie jak i technicznie a jednocześnie ważne i pilne. Tym samym szczególnego znaczenia nabiera dobór właściwych i adekwatnych metod pozwalających ograniczać zidentyfikowane ryzyka. Jednym z nich jest stosowanie kodeksów postępowania tzn. powszechnie przyjętych rozwiązań technicznych, zamiast szczegółowej analizy ryzyka. Wykorzystanie tej możliwości znacząco skraca czas projektowania i wprowadzenia na rynek. ◄

Materiały źródłowe

[1] European Parliament; Dyrektywa NIS2; Directive (EU) 2022/2555
[2] IEC 62443-4-1:2018; Security for industrial automation and control systems Part 4-1: Secure product development lifecycle requirements; ISBN 978-2-8322-5239-0
[3] IEC 62443-4-2:2019; Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components; ISBN 978-2-8322-6597-0
[4] PD CLC/TS 50701:2023; Railway applications - Cybersecurity; ISBN ISBN 978 0 539 20855 9
[5] IEC62443-3-2:2020; Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design; ISBN 978-2-8322-8501-5
[6] EULYNX System Definition – Appendix A1; Eu.Doc.7 A1 v4.2.
[7] EULYNX Security Concept; Eu-.Doc.15 v2.1