Transmisja otwarta w systemach srk,
Bezpieczeństwo systemów srk
Transmisja bezpieczna

Andrzej LEWIŃSKI[1]
Andrzej TORUŃ[2]
Lucyna BESTER[3]

SPOSOBY REALIZACJI TRANSMISJI OTWARTEJ W SYSTEMACH STEROWANIA RUCHEM KOLEJOWYM

W artykule przedstawiono uwarunkowania związane z wdrożeniem systemów transmisji otwartej w wybranych systemach sterowania ruchem kolejowym. Obowiązująca w UE norma PN-EN50159-2 dopuszcza możliwość stosowania bezprzewodowych standardów transmisji pod warunkiem, że zapewniony jest ten sam poziom funkcjonalności i bezpieczeństwa, co w dotychczasowych realizacjach wykorzystujących transmisję kablową. W pracy omówiono sposoby realizacji bezpiecznej transmisji opartej na zaleceniach wspomnianej normy oraz przykłady realizacji takiej transmisji na potrzeby kolejnictwa polskiego.

METHODS OF IMPLEMENTATION OF THE OPEN TRANSMISSION IN RAILWAY CONTROL SYSTEMS

The article presents the conditions to implementation of the open transmission systems in selected railway control systems. Existing EU standard PN-EN50159-2 allows the use of wireless transmission standards, with respect to condition that the same level of functionality and security may be assured in comparison to cable transmission. The paper discusses how to implement secure transmission based on the recommended standard to polish railways requirements.

1. PODSTAWOWE WARUNKI BEZPIECZNEJ TRANSMISJI W SYSTEMACH SRK

Bezpieczna transmisja w systemach sterowania ruchem kolejowym musi spełniać wymagania i zalecenia określone w obowiązujących właściwych normach PN-EN 50159-1: 2002, PN-EN 50159-2: 2002 [1,2]. Bezpieczeństwo transmisji jest analizowane na

[1] Politechnika Radomska, Wydział Transportu i Elektrotechniki; 26-600 Radom, ul. Malczewskiego 29
Tel. +48 48 361-77-20, Fax: +48 48 361-77-42, E-mail: a.lewinski@pr.radom.pl
[2] Instytut Kolejnictwa, Zakład Sterowania Ruchem i Teleinformatyki; 04-275 Warszawa; ul. Chłopickiego 50,
Tel. +48 22 47-31-490, Fax: +48 22 47-31-036 E-mail: atorun@ikolej.pl
[3] Politechnika Radomska, Wydział Transportu i Elektrotechniki; 26-600 Radom, ul. Malczewskiego 29
Tel. +48 48 361-77-22, E-mail: l.bester@pr.radom.pl

poziomie systemu sterowania jako jego element (norma PN-EN50126) oraz jest istotnie związana ze sprzętem i oprogramowaniem, co uwzględniają obowiązujące dla systemów kolejowych normy PN-EN 50129, PN-EN 50128.

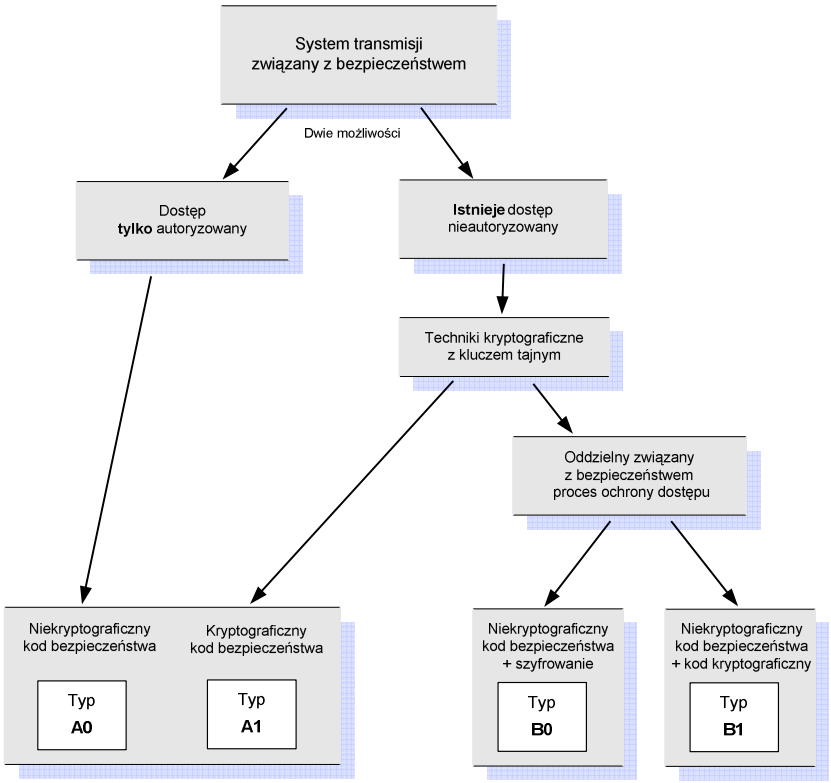
Realizacja transmisji informacji musi być przeprowadzona w taki sposób, aby możliwa była możliwie jak najszybsza detekcja błędnych informacji, a przerwa w łączu transmisyjnym musi spowodować przejście systemu do „stanu bezpiecznego" zgodnie z procedurą określoną dla rozpatrywanego systemu srk. Stan ten jest definiowany dla poszczególnych typów systemów indywidualnie i tak np. „stan bezpieczny" w systemach zliczania osi oznacza sygnalizację stanu „odcinek zajęty", dla sygnalizacji przejazdowej „stan bezpieczny" może oznaczać załączenie ostrzegania o zbliżaniu się pociągu, a w systemach sygnalizacji wymuszenie wyświetlenia na semaforze „sygnału zabraniającego S1". Dlatego też w celu zapewnienia prawidłowego działania systemu srk należy zastosować odpowiednie środki zabezpieczające przed przekłamaniem lub utratą informacji będących skutkiem zakłóceń bądź nieświadomej lub celowej (nieuprawnionej) działalności obsługi. W przypadku bezpiecznych systemów transmisji informacje muszą być zabezpieczone dodatkowymi bitami lub zakodowane. Dopuszcza się stosowanie innych środków zabezpieczających, o ile będą one zapewniać wymagany poziom bezpieczeństwa.
Wprowadzany system transmisji otwartej wykorzystującej publiczne sieci radiowe powinien zapewnić dotychczasowy poziom bezpieczeństwa (zgodny z klasyfikacją SIL, wynikający z norm PN-EN 5012x) oraz nie gorszy od poziomu funkcjonalności w istniejących systemach (dotyczy to zwłaszcza opóźnień i przerw w transmisji).
W systemach transmisji otwartej transmisja prowadzona jest z wykorzystaniem sieci radiowej, sieci Internet lub poprzez łącza współdzielone o publicznym dostępie. Oznacza to, że informacje przesyłane są przez system transmisji dostępny dla nieuprawnionych użytkowników, przez co przesyłane dane mogą być narażone na ataki takie jak np usunięcie lub podszycie się nadawców pod urządzenia srk pracujące w sieci. Zgodnie z obowiązującymi normami PN-EN 50159-2 otwarty system transmisji narażony jest na następujące typy zagrożeń:

A. Maskarada, czyli celowe lub niecelowe „podszycie się" innego systemu pod system srk.
B. Wstawienie, związane z atakami w celu uzyskania dostępu do przesyłanych informacji lub podsyłanie przetworzonych pakietów.
C. Powtórzenie telegramów.
D. Usunięcie, modyfikacja, lub przekierowanie telegramów,
E. Zmiana kolejności telegramów,
F. Opóźnienia telegramów

W przedstawionej koncepcji wykorzystania sieci otwartych w systemach srk zaproponowano typ transmisji B0 (rys.1), z wymaganą dla tego typu strukturą informacji oraz odpowiedni proces przetwarzania zapewniając metody zabezpieczeń przed wymienionymi zagrożeniami transmisji w sieci. Zgodnie z normą zaproponowany sposób transmisji został zaliczony do klasy 7 (media transmisyjne o ograniczonym zaufaniu np. Internet).

1.1 Klasyfikacja typów telegramów w układach transmisji otwartej

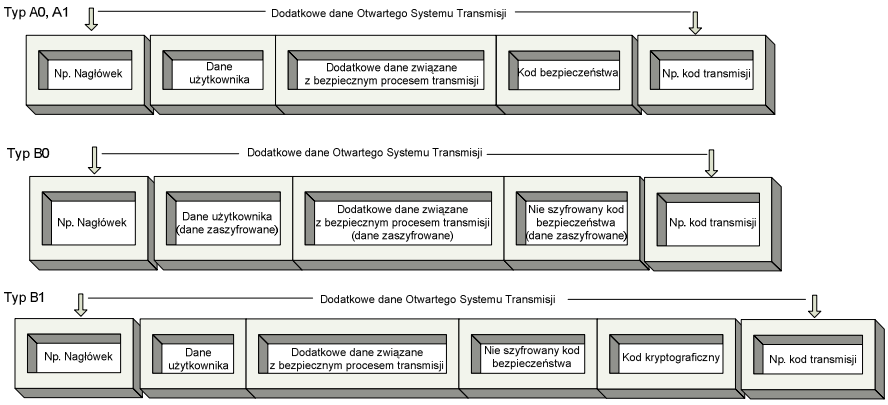
W systemach transmisji otwartej (STO) dla systemów sterowania ruchem kolejowym zostały określone podstawowe zasady przesyłania informacji oraz metody ich zabezpieczania. Zgodnie przyjętą klasyfikacją systemów powiązanych z bezpieczną transmisją przyjęto poniżej określoną klasyfikację grup transmisji.



Rys. 1. Klasyfikacja zabezpieczeń transmisji dla systemów transmisji otwartej

- A0 – dostęp tylko autoryzowany, wymagany jest kod integralności danych, nie musi być stosowany kryptograficzny kod bezpieczeństwa,
- A1 – nie wyklucza się zastosowania nieautoryzowanego dostępu, wymagane jest stosowanie kryptograficznego kodu bezpieczeństwa,
- B0 – nie wyklucza się zastosowanie nieautoryzowanego dostępu, wymagane jest szyfrowanie, nie jest wymagany kryptograficzny kod bezpieczeństwa,
- B1 – nie wyklucza się zastosowanie nieautoryzowanego dostępu, wymagany jest kod kryptograficzny, nie musi być stosowany kryptograficzny kod bezpieczeństwa.

Jak widać na rysunku 1 postać informacji A0 jest taka sama dla systemu z autoryzowanym dostępem jak też dla systemu otwartego bez autoryzowanego dostępu.
Postać informacji dla każdego typu bezpiecznej transmisji przedstawiają schematy przedstawione na rysunku 2.



Rys. 2. Struktura informacji w systemach bezpiecznej transmisji zgodnie z normą PN-EN 50159-2

Aby uniknąć zagrożeń transmisji konieczne jest utworzenie tunelu szyfrowanego VPN (Virtual Private Network) pomiędzy segmentami sieci zamkniętej, zakończonego urządzeniami szyfrującymi bramami VPN, co zapewnia bezpieczne połączenia pomiędzy tymi sieciami. Zgodnie z normą [1] zaleca się użycie technik kryptograficznych poprzez zastosowanie algorytmów szyfrujących oraz kluczy uwierzytelniających.

Ad. A. W proponowanej koncepcji, aby zachować wymagany poziom bezpieczeństwa zastosowano szyfrowane tunele VPN z protokołami IPsec, algorytmy szyfrujące DES (Data Encryption Standard), 3DES i AES (Advanced Encryption Standard). Natomiast zastosowanie algorytmu uzgadniania kluczy Diffiego-Hellmana eliminuje możliwości przechwycenia pakietów poprzez podsłuch kanału komunikacyjnego.

Ad. B. Zastosowano tryb tunelowania wykorzystując protokół IPsec (Internet Protocol Security), dzięki czemu chronione są wszystkie pakiety wysyłane pomiędzy hostami. Protokół IPSec zapobiega wszelkim modyfikacjom pakietów oferuje bezpieczną, silną kryptografię i uwierzytelnianie na poziomie IP. Zastosowanie algorytmu uzgadniania kluczy Diffiego-Hellmana eliminuje możliwości przechwycenia pakietów poprzez podsłuch kanału komunikacyjnego.

Ad. C. Aby zapobiec powtarzalności pakietów zastosowano nagłówek IPsec - ESP w ruchu pakietów (Encapsulating Security Payload), który zapewnia uwierzytelnianie, identyfikację oryginalności oraz integralności danych. Dodatkową ochronę przed powtarzaniem pakietów zapewnia dołączenie kolejnego numeru do każdego pakietu.

Ad. D. Ochrona przeciw atakom usuwania, modyfikacji, powtórzeń lub przekierowania telegramów do innych odbiorców realizowana jest poprzez mechanizmy kryptograficzne ISAKMP (Internet Security Association and Key Management Protocol), min 3DES, SHA-1 lub MD5, DH2 zgodnie z zaleceniami norm [2].

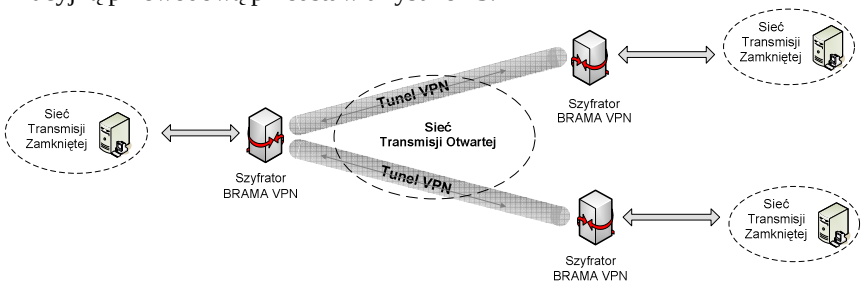
Ad. E, F. Zmiana kolejności i opóźnienia telegramów została rozwiązana poprzez zastosowanie protokołu IPsec (tunel IPsec oraz format pakietów ISAKMP) oraz kontrolę czasu. Proponowane w koncepcji rozwiązania umożliwiają dodatkowo wyeliminowanie innych zagrożeń takich jak: Zjawisko ukrytej lub odkrytej stacji, Efekt przechwytywania, Przekłamanie danych pakietu, Przekłamanie sumy kontrolnej CRC telegramu.

2. KONCEPCJA ZASTOSOWNIA SYSTEMU TRANSMISJI OTWARTEJ W WYBRANYCH SYSTEMACH SRK

Aktualnie opracowane są przez różne firmy produkujące urządzenia srk rozwiązania stosujące transmisję otwartą, głównie opartą na bezprzewodowych standardach radiowych.

2.1 Koncepcja systemu opartego o tunel VPN.

Ogólny model sieci z zaznaczeniem kanału zastępującego dotychczasową sieć komunikacyjną przewodową przedstawia rysunek 3.



Rys. 3. Architektura transmisji z wykorzystaniem sieci otwartych w systemach srk

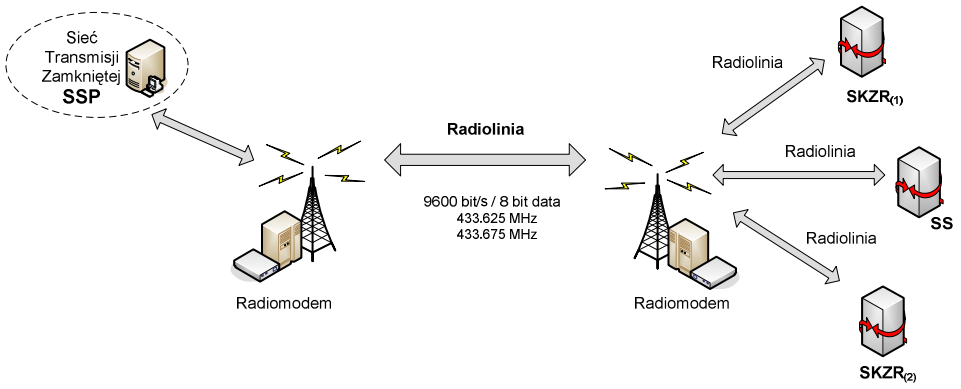
Analizując wpływ zmiany sposobu transmisji na poziom bezpieczeństwa systemu srk zostały przeprowadzone badania porównawcze parametrów dla przykładowej aplikacji systemu blokady liniowej stosowanej na PKP PLK S.A., zaliczonej do systemów poziomu SIL 4. Analiza prowadzona była przy założeniu ograniczenia i zminimalizowania poziomu usterek transmisji. W celu osiągnięcia niskiego poziomu usterek przyjęto, że zastosowane będą dodatkowe środki techniczne tj. redundancja CRC, uzupełnienie telegramu o dodatkowe dane w postaci znaczników czasu oraz inne zabezpieczenia wynikające z zastosowanych protokołów transmisji.

Analiza miała na celu potwierdzenie możliwości wykorzystania transmisji w sieciach otwartych w zastosowaniach kolejowych. W tym celu dokonano porównania parametrów dla dwóch typów transmisji w systemie blokady liniowej.. Pierwszy z nich dotyczy transmisji zamkniętej realizowanej poprzez linię kablową (model referencyjny

dopuszczony do stosowania w aplikacjach kolejowych na PKP PLK S.A. np. systemu SHL-12), drugi jest propozycją systemu transmisji otwartej realizowanej poprzez tunel VPN.
Kanał transmisji opartej o tunel VPN został zamodelowany w oparciu o dane katalogowe standardowych bram VPN dostępnych na rynku (firm tj. Cisco, NETGEAR, Westermo), dla którego przyjęto średnie czasy MTBF na poziomie 500 000h. Pozostałe elementy systemu mające wpływ na bezpieczeństwo transmisji zależą istotnie od charakterystyki sieci operatora i czynników niedeterministycznych trudnych do określenia na etapie budowy koncepcji systemu, przy czym zgodnie z wymaganiami określone zostały minimalne parametry sieci gwarantujące zachowanie przyjętych dla systemu sterowania poziomów bezpieczeństwa SIL.
Zakładając, że systemy z transmisją zamkniętą (dopuszczone do eksploatacji w UE i Polsce) spełniają wymagania norm PN-EN 50129, PN-EN 50128, PN-EN 50159-1 należy zauważać, że przyjęte rozwiązania systemów z transmisją otwartą opartą o zalecenia normy PN-EN 50159-2 powinny zapewnić analogiczny poziom bezpieczeństwa. Co daje podstawę da zaliczenia podsystemu transmisji radiowej do poziomu SIL 4.

2.2 Koncepcja systemu oparta o kanał radiowy (radiomodemy)

W tej propozycji koncepcji systemu bezpiecznej transmisji zastosowany został kanał radiowy (otwarty system transmisji) do przekazywania informacji w podsystemie urządzeń oddziaływania. Analiza prowadzona była w odniesieniu do systemu zabezpieczenia przejazdu kolejowego. W przyjętym modelu kanał radiowy wykorzystywany jest do przekazywania informacji między sterownikami współpracującymi z czujnikami koła a sterownikami systemu ssp umieszczonymi w kontenerze. Taka konfiguracja pozwala na wyeliminowanie konieczności wykonywania połączeń kablowych od oddalonych od przejazdu punktów oddziaływania (czujników).
W tym przypadku, jak przy analizie opisywanej wcześniej przyjęto metodę porównania standardowych parametrów charakteryzujących system ssp oparty o system wymiany telegramów siecią w układzie zamkniętym (sieć kablowa) – systemy takie są powszechnie eksploatowane na sieci PKP PLK S.A. – oraz wyznaczenia parametrów dla sieci transmisji w układzie otwartym (tak, aby możliwe było stwierdzenie czy nie został naruszony, obniżony, poziom SIL).
W rozpatrywanym przypadku kanał transmisji otwartej oparty został na wydzielonej radiolinii, co zapewnia m.in. kontrolę autoryzacji dostępu. Do obliczeń przyjęto parametry techniczne radiomodemów typu Satellar firmy Satel. Transmisja odbywa się w kanale 433.725 MHz (odstęp sąsiednio-kanałowy 25 kHz) z prędkością w kanale radiowym do 19200 bit/s. Zastosowany sprzęt transmisyjny charakteryzuje się wysoką niezawodnością – MTBF około 525600 h.
Na rys. 4 przedstawiono podobne radiolinie do komunikacji ze sterownikami stacyjnymi (SS) i systemem zajętości torów (SKZR).



Rys. 4. Przykład łączności radiowej pomiędzy podsystemami

W modelu przyjęto telegramy zgodne z typem transmisji B0, wykorzystując techniki kryptograficzne z kluczem tajnym oraz szyfrowanie danych w całości łącznie z kodem integralności danych. Jako algorytm szyfrowania przyjęto standard AES z kluczem 128-bitowym, do tak zaszyfrowanych danych dołączanych jest dodatkowy kod integralności danych, który pozwala na odrzucenie przekłamanych telegramów oraz zabezpiecza przed ich rozszyfrowaniem. Natomiast w celu kontroli integralności danych wykorzystano technikę kodowania nadmiarowego CRC (Cyclic Redundancy Check), które zabezpieczają przed przypadkowymi błędami pozwalając wykrycie pojedynczych lub seryjnych błędów.

3. WNIOSKI

Oba analizowane rozwiązania transmisji otwartej są zgodne z zaleceniami obowiązującej normy PN-EN 50159-2, regulującej takie zastosowania w systemach sterowania ruchem kolejowym.

Zaproponowane rozwiązania otwartej transmisji radiowej, powinny zapewnić ten sam poziom bezpieczeństwa, co produkowane (i eksploatowane w kolejnictwie polskim) przez obie firmy systemy zamknięte, w których stosowana jest transmisja kablowa.

W pierwszym przykładzie rozwiązanie wykorzystuje dostępne na rynku bramy VPN wraz z odpowiednimi protokołami zabezpieczającymi dane przed przekłamaniem, utratą bądź nieuprawnionym dostępem.

W drugim alternatywnym rozpatrywanym przypadku zaproponowano rozwiązanie oparte o radiolinie z licencjonowanym pasmem z autoryzowanym dostępem tylko dla potrzeb systemu, wraz z zabudową specjalizowanych radiomodemów, posiadających wbudowane mechanizmy zabezpieczające dane przed przekłamaniem, utratą bądź nieuprawnionym dostępem.

W wyniku przeprowadzonych analizy stwierdzono, iż w obu przypadkach zastosowana transmisja otwarta zapewnia parametry porównywalne ze stosowanymi standardami w sieciach zamkniętych. (nie zostały obniżone poziomy SIL w ujęciu systemów, jako całości).

Ponieważ zastosowanie transmisji otwartej nie może spowodować sytuacji, gdzie dany system srk przestanie spełniać zdefiniowane dla niego wymagania bezpieczeństwa lub nastąpi obniżenie tych parametrów poniżej przyjętego poziomu SIL, dla każdego zastosowania transmisji otwartej w danym typie systemu srk np. blokada liniowa, sygnalizacja przejazdowa, zdalne sterowanie lub w przypadku zmiany rodzaju sieci transmisji otwartej (np. transmisja bezprzewodowa, Internet), należy przeprowadzić analizę i ocenę bezpieczeństwa uwzględniając typowe dla rozpatrywanego systemu srk parametry takie jak: dostępność, przepustowość czy opóźnienia, proces ten musi zostać udokumentowany odpowiednimi dowodami potwierdzającymi spełnienie wymagań dla konkretnego typu aplikacji (systemu srk) zgodnie z obowiązującymi w tym zakresie wymaganiami norm kolejowych serii PN-EN 50 xxx.

4. BIBLIOGRAFIA

[1] Norma PN-EN 50159-2:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 2 Łączność systemów bezpiecznych w układach otwartych.
[2] Norma PN-EN 50159-1:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 1 Łączność systemów bezpiecznych w układach zamkniętych.
[3] Jaźwiński J., Ważyńska – Fiok K.: „Bezpieczeństwo i niezawodność systemu sterowania ruchem kolejowym", Zeszyt 95, WKiŁ Warszawa 1982
[4] Szopa T.: „Niezawodność i bezpieczeństwo". Oficyna Wydawnicza Politechniki Warszawskiej. Warszawa 2009