TECHNIKA TRANSPORTU SZYNOWEGO

Waldemar NOWAKOWSKI, Maksymilian SZCZYGIELSKI

ANALIZA BEZPIECZEŃSTWA TRANSMISJI W SYSTEMIE ZABEZPIECZENIA PRZEJAZDÓW SZP-1

Streszczenie

W artykule opisano nowy system zabezpieczenia przejazdów SZP-1, ze szczególnym uwzględnieniem problematyki bezpieczeństwa wymiany informacji. System SZP-1 został opracowany w ramach projektu ESTER jako ekonomiczna alternatywa w stosunku do obecnie stosowanych systemów sygnalizacji przejazdowej.

WSTĘP

Stopniowa dekapitalizacja infrastruktury kolejowej w Polsce wymaga zwiększenia poziomu prac modernizacyjnych. Pewną szansą rozwiązania tego problemu jest rosnąca dostępność pomocy strukturalnej po wstąpieniu naszego kraju do Unii Europejskiej. Zarządcy infrastruktury kolejowej oczekują od producentów systemów sterowania ruchem kolejowym nowych rozwiązań technicznych, które stanowiłyby ekonomiczną alternatywę w stosunku do obecnie stosowanych systemów. Przykładem takiego rozwiązania jest system zabezpieczenia przejazdów SZP-1, który został opracowany przez Zakłady Automatyki KOMBUD S.A. w ramach projektu: „ESTER – ekonomiczny system zdalnego sterowania i kierowania ruchem kolejowym". System SZP-1 przeznaczony jest do zabezpieczenia ruchu na przejazdach kolejowych kategorii „A", „B" i „C". SZP-1 może być stosowany na liniach kolejowych jednotorowych i dwutorowych (zelektryfikowanych i niezelektryfikowanych), z blokadą samoczynną, półsamoczynną oraz bez blokady, na których maksymalna prędkość pociągów nie przekracza 160 km/h.

1. ARCHITEKTURA SYSTEMU SZP-1

System zabezpieczenia przejazdów typu SZP-1 posiada strukturę systemu rozproszonego. W strukturze systemu SZP dla przejazdów kategorii „B" można wyróżnić m.in. następujące wyposażenie [1]:

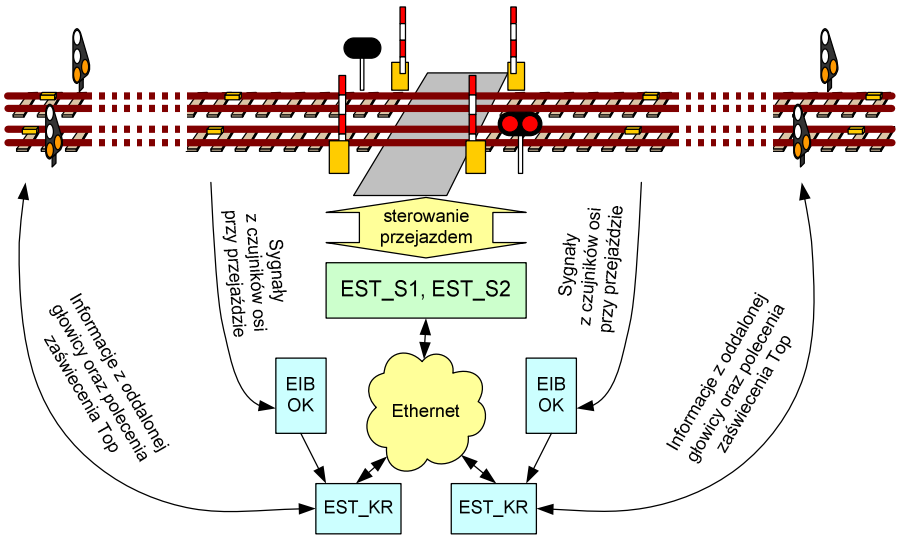
1. Podsystem urządzeń wykonawczych i kontrolnych (PUW):
   - napędy rogatkowe wraz z drągami i lampkami,
   - sygnalizatory drogowe,
   - sygnalizatory dźwiękowe (element opcjonalny),
   - MOZ –moduł zasilania,
   - układ kontroli zasilania.
2. Podsystem sterowania:

- karty sterowników decyzyjnych EST_S1, EST_S2,
- panel sterujący,
- ruter z funkcją firewall (element opcjonalny),
- przełączniki Ethernet.

3. Urządzenia zdalnej kontroli (UZK) jako element opcjonalny.
4. Układ zasilania kontenera.
5. Podsystem urządzeń oddziaływania PUO:
   - czujniki załączające,
   - czujniki wyłączające,
   - tarcze ostrzegawcze Top,
   - karty czujników i tarcz Top EST_G oraz czujników EST_GK,
   - moduł dopasowujący TEN-FRAU (element opcjonalny),
   - karty transmisyjne kryptograficzne: radiowe EST_KR, EST_KRG lub przewodowe EST_KK, EST_KKG,
   - karty kontroli zasilania EST_ACC,
   - układy zasilania głowic.
6. Podsystem urządzeń dodatkowych (ISZ).

2. BEZPIECZEŃSTWO TRANSMISJI W SYSTEMIE SZP-1

SZP-1 to systemem rozproszony, w którym poszczególne elementy systemu komunikują się ze sobą z wykorzystaniem otwartych układach transmisji danych (rys. 1). Dlatego też znaczący wpływ na bezpieczeństwo całego systemu mają metody zabezpieczenia procesu wymiany danych.



Rys. 1. Schemat wymiany informacji w systemie SZP-1

Za wypracowanie poleceń sterujących przejazdem odpowiedzialne są dwa sterowniki EST_S1 oraz EST_S2 działające pod systemem operacyjnym Linux [1]. Można je sobie wyobrazić jako most między urządzeniami specyficznymi dla SZP-1 (tj. czujniki osi, tarcze ostrzegawcze Top), a przejazdem. W takim przypadku musi być zapewniona integralność przekazywanych danych. Brak integralności danych mogłaby skutkować wystąpieniem sytuacji niebezpiecznej [2]. Z punktu widzenia bezpieczeństwa utrata danych nie jest tak groźna, gdyż system jako całość przechodzi do stanu bezpiecznego zmniejszając swoją

dostępność. Zachowanie integralności danych jest szczególnie istotne ze względu na zastosowanie transmisji radiowej. Jednym z zalecanych sposobów zabezpieczenia integralności przesyłanych danych jest stosowanie skrótu informacji dołączanego najczęściej na końcu przesyłanego telegramu (np. kodu CRC). W literaturze , które wiążą ze sobą takie wielkości jak: odległość bitowa (Hamminga), długość telegramu i prawdopodobieństwo niewykrytego przekłamania [3] (tab.1 i tab 2).

Tab. 1. Najlepsze wielomiany typu CRC32sub8 [3]

Odległość Hamminga	Wielomian	Długość telegramu
8	0x000001D7 $x^{32}+x^8+x^7+x^6+x^4+x^2+x^1+x^0$ {1,1,5,25}	197
7	0x00000179 $x^{32}+x^8+x^6+x^5+x^4+x^3+x^0$ {2,30}	270
6	0x000001ED $x^{32}+x^8+x^7+x^6+x^5+x^3+x^2+x^0$ {1,10,21}	2048
6	0x000000E5 $x^{32}+x^7+x^6+x^5+x^2+x^0$ {1,1,3,4,23}	4145

Tab. 2. Najlepsze wielomiany typu CRC32sub16 [3]

Odległość Hamminga	Wielomian	Długość telegramu
12	0x0001DA97 $x^{32}+x^{16}+x^{15}+x^{14}+x^{12}+x^{11}+x^9+x^7+x^4+x^2+x^1+x^0$ {1,2,11,18}	62
11	0x00015A67 $x^{32}+x^{16}+x^{14}+x^{12}+x^{11}+x^9+x^6+x^5+x^2+x^1+x^0$ {3,5,8,16}	65
10	0x00018AD5 $x^{32}+x^{16}+x^{15}+x^{11}+x^9+x^7+x^6+x^4+x^2+x^0$ {1,1,11,19}	106
9	0x00008D35 $x^{32}+x^{15}+x^{11}+x^{10}+x^8+x^5+x^4+x^2+x^0$ {32}	116
8	0x0000B3E1 $x^{32}+x^{15}+x^{13}+x^{12}+x^9+x^8+x^7+x^6+x^5+x^0$ {1,8,9,14}	313
7	0x00002979 $x^{32}+x^{13}+x^{11}+x^8+x^6+x^5+x^4+x^3+x^0$ {5,9,9,9}	516
6	0x00003551 $x^{32}+x^{13}+x^{12}+x^{10}+x^8+x^6+x^4+x^0$ {1,5,13,13}	8220+

Obok sterowników decyzyjnych EST_S1 i EST_S2 istotnymi elementami systemu są także sterowniki EST_KR, których zadaniem jest dostarczanie wiarygodnych danych. Sterowniki te nie posiadają dużej mocy obliczeniowej, gdyż zajmują się jedynie zbieraniem informacji z kart czujników oraz szyfrowaniem, deszyfrowaniem i przygotowywaniem danych dla potrzeb transmisji radiowej. Bezpośredni wpływ na bezpieczeństwo systemu mają jednak sterowniki decyzyjne EST_S1 i EST_S2. Dlatego też system zrealizowano jako

dwukanałowy, pracujący w układzie „2z2” co oznacza, że do poprawnego funkcjonowania niezbędna jest prawidłowa i zgodna praca obu kanałów.

Ze względu na otwarty układ transmisyjny wymiana informacji w systemie SZP-1 narażona jest na następujące zagrożenia [2]:

- skasowanie telegramu,
- wprowadzenie do systemu telegramu przez nieautoryzowanego nadawcę,
- zmianę kolejności telegramów,
- opóźnienie w odebraniu telegramu,
- podszycie się innego systemu (maskaradę).

W celu ograniczenia zagrożeń ze strony otwartego układu transmisyjnego wzięto pod uwagę następujące warunki:

- autentyczność telegramów,
- integralność telegramów,
- określony czas przesyłania telegramów,
- kolejność telegramów.

oraz przyjęto następujące funkcje zabezpieczenia informacji w systemie:

- numerowanie telegramów - zabezpieczenie przed takimi zagrożeniami jak: powtórzenie, skasowanie, brak autoryzacji czy zmiana kolejności,
- kody integralności - pozwalają zabezpieczyć przed uszkodzeniem telegramu, przypadkowymi błędami pozwalając na wykrycie pojedynczych lub seryjnych błędów,
- czas oczekiwania na odpowiedź - pozwala zapobiec opóźnieniom w transmisji,
- szyfrowanie i stosowanie kodów bezpieczeństwa - zabezpieczenie przed nielegalnym dostępem i modyfikacją telegramów.

Zaproponowana architektura systemu SZP-1 oraz rozwiązania przepływu informacji uwzględniają wymagania zawarte w normie PN EN 50159. Telegramy wykorzystują techniki kryptograficzne z kluczem tajnym. Dane wysyłane (drogą radiową) uzupełnianie są kodem CRC-16 szyfrowane algorytmem AES z kluczem 128-bitowym, a następnie dla zapewnienia integralności danych całość uzupełniana jest kodem CRC-32. Transmisja lokalna po magistrali SPI również chroniona jest przed przekłamaniem kodem CRC-32.

Oprócz kodowania wprowadzono dodatkowe zabezpieczenia podwyższające poziom bezpieczeństwa transmitowanych danych, w tym:

- zmienna częstotliwość wysyłania pakietów, w celu kontroli przez sterowniki czy transmisja jest przerwana,
- wprowadzenie kryteriów czasowych kontroli poprawności pakietu w określonym czasie.

PODSUMOWANIE

Zakłady Automatyki „KOMBUD” S.A. opracowały nowy system sterowania i kierowania ruchem kolejowym – ESTER. Jednym z rozwiązań wchodzących w skład projektu ESTER jest zaprezentowany w artykule system zabezpieczenia przejazdów SZP-1. System ten jest ekonomiczną alternatywą w stosunku do obecnie stosowanych m.in. dzięki zastosowaniu nowoczesnych technologii, w tym: transmisji radiowej oraz niekonwencjonalnych źródeł energii elektrycznej, co eliminuje potrzebę budowy kosztownych linii kablowych.

Innowacyjne podejście w zakresie otwartego układu transmisyjnego w systemie SZP-1 wymusiło konieczność zabezpieczenia procesu wymiany danych, zgodnie z wymogami zawartymi w normie PN EN 50159. Dlatego też, w systemie SZP-1 zastosowano metody, które wpływają na zapewnienie wymaganego poziomu nienaruszalności bezpieczeństwa.

TRANSMISSION SECURITY ANALYSIS IN CROSSING PROTECTION SYSTEM SZP-1

Abstract

The article describes a new railway crossing protection system SZP-1, with particular emphasis safety-related information exchange. SZP-1 system was developed under the project ESTER as the economic alternative to the current crossing protection systems.

BIBLIOGRAFIA

1. Nowakowski W., Kornaszewski M.: *Innowacyjny system zabezpieczenia przejazdów SZP-1*, XV Międzynarodowa Konferencja „TransComp", Zakopane 2011r.
2. Łukasik Z., Nowakowski W.: *Wymiana informacji w systemach związanych z bezpieczeństwem*, XII Międzynarodowa Konferencja „TransComp", Zakopane 2008r.
3. Ray J., Koopman P.: *Efficient high hamming distance CRCs for embedded applications*, International Conference on Dependable Systems and Networks, Philadelphia 2006r.

Autorzy:
dr inż. Waldemar NOWAKOWSKI – Zakłady Automatyki KOMBUD S.A. w Radomiu
dr inż. Maksymilian SZCZYGIELSKI - Zakłady Automatyki KOMBUD S.A. w Radomiu