TECHNIKA TRANSPORTU SZYNOWEGO

Andrzej LEWIŃSKI Tomasz KALBARCZYK

BEZPIECZNA TRANSMISJA W SYSTEMACH SRK NA PRZYKŁADZIE ROZWIĄZAŃ FIRMY KOMBUD S.A.

Streszczenie

W artykule przedstawione zostały wymagania dla transmisji cyfrowej stosowanej w bezpiecznych systemach srk zdefiniowane w obowiązujących normach. Artykuł zawiera wprowadzenie do zagadnienia i praktyczną realizację na przykładzie wybranych systemów sterowania ruchem kolejowym produkowanych przez KOMBUD S.A.

WSTĘP

Współczesne systemy sterowania ruchem kolejowym w transporcie są systemami komputerowymi. W układach tych mamy do czynienia ze współpracą systemu dyspozytorskiego i zcentralizowanego, systemu zależnościowego z małymi systemami stacyjnymi, systemami sygnalizacji przejazdowej i blokady liniowej, a także z systemami automatycznego prowadzenia pociągu. Systemy takie, z punktu widzenia bezpieczeństwa i niezawodności, są realizowane poprzez tworzenie specjalnych struktur. Wszystkie obecnie produkowane komputerowe systemy srk posiadają poprzez swoje interfejsy możliwość komunikowania się pomiędzy sobą za pomocą standardów kablowych i bezprzewodowych.

Polska norma z 1991 roku „Bezpieczeństwo systemów sterowania ruchem" PNZN-91/MTiGM-CBP-12, dotyczyła głównie systemów przekaźnikowych i nie dawała możliwości poprawnej implementacji urządzeń komputerowych w systemach sterowania ruchem kolejowym.

Wraz z wejściem Polski do UE obowiązujące stały się normy oznaczone: **PN-EN 50126** [1], **PN-EN 50128** [2], **PN-EN 50129** [3] oraz **PN-EN 50159** [4].

Na podstawie zaleceń CENELEC dotyczących niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa całego systemu zawartych w projektach norm w 1997 roku w Zakład Sterowania Ruchem i Zasilania CNTK opracował „Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym" [5]. Opracowanie to od lutego 1998r. jest obowiązujące dla projektantów systemów sterowania ruchem kolejowym w kolejnictwie polskim.

Norma **PN-EN 50126** określa niezawodność, gotowość, dostępność i bezpieczeństwo (RAMS - *Reliability, Availability, Maintainability and Safety*), jako proces oparty o cykl życia systemu (*ang. system life-cycle*). Zidentyfikowane zostały poszczególne etapy systemu i procedury związane z zatwierdzaniem przed przejściem do następnego etapu.

Norma **PN-EN 50128** określa procedury i wymagania techniczne dla projektowania oprogramowania bezpiecznego systemu elektronicznego dla sterowania i zabezpieczenia na kolei.

Norma **PN-EN 50129** definiuje wymagania dotyczące projektowania, testowania, odbioru i zatwierdzania elektronicznych systemów, podsystemów i urządzeń sygnalizacji związanych z bezpieczeństwem w zastosowaniach kolejowych.

Norma **PN-EN 50159** określa wymagania konieczne do osiągnięcia bezpiecznej komunikacji w systemach sterowania ruchem kolejowym połączonych poprzez interfejsy transmisyjne.

Jedną z często stosowanych technik analizy bezpieczeństwa systemów są drzewa niezdatności FTA (Fault Tree Analysis FTA) [6]. Technika ta polega na identyfikacji sytuacji niebezpiecznych, tzw. niezdatności. Niezdatnością nazywamy taką sytuację, która bezpośrednio lub poprzez zainicjowanie zdarzeń pośredniczących może doprowadzić do wypadku. W szczególności, niezdatnością może być dwa pociągi jadące jednym torem naprzeciw siebie.

Koncepcja bezpiecznych systemów komputerowych stosowanych w kolejnictwie zakłada bardzo małą intensywność usterek, co przy całkowitej niezależności kanałów przetwarzania gwarantuje znikome prawdopodobieństwo wystąpienia usterki podwójnej lub wielokrotnej – decydującej o uszkodzeniu katastroficznym (krytycznym). Podstawą analizy jest akceptowalny, dopuszczalny poziom ryzyka (*THR - Tolerable Hazard Rate*), określony z zależności.(bezpieczeństwo systemu zależy nie tylko od intensywności uszkodzeń, ale od czasu detekcji uszkodzeń pojedynczych i podwójnych):

$$THR = \prod_{i=1}^{n} \frac{\lambda_i}{t_{d_i}^{-1}} \cdot \sum_{i=1}^{n} t_{d_i}^{-1} \tag{1}$$

gdzie: λ_i – intensywność uszkodzeń dla kanału i, $t_{d_i}^{-1}$ – czas reakcji systemu na błąd dla kanału *i*.

Wartość THR szacowana jest na podstawie charakterystyk niezawodnościowych producenta sprzętu i decyduje o bezpieczeństwie (zgodnie z normą PN-EN 50129) poprzez Poziomem Integralności Bezpieczeństwa SIL (*safety integrity level* SIL), który umownie określa nienaruszalność bezpieczeństwa dla systemów bezpiecznych:

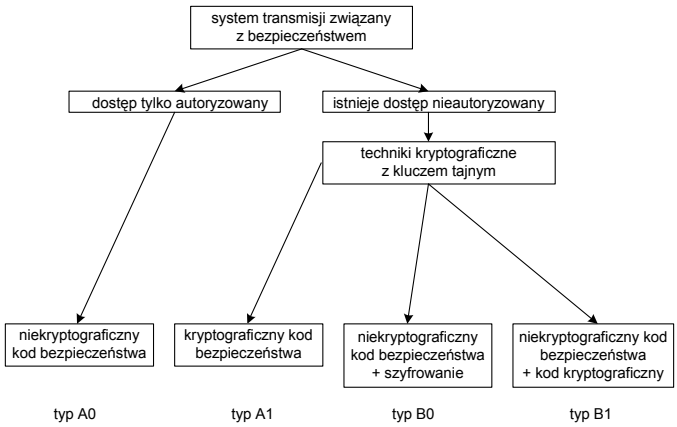
Tab. 1. Dopuszczalne wartości THR

THR	SIL
$10^{-9} \le THR < 10^{-8}$	4
$10^{-8} \le THR < 10^{-7}$	3
$10^{-7} \le THR < 10^{-6}$	2
$10^{-6} \le THR < 10^{-5}$	1

1. TRANSMISJA BEZPIECZNA W ZAMKNIĘTYCH SYSTEMACH SRK

1.1. Ogólne zasady

Wymagania dla bezpiecznych systemów transmisyjnych zostały opracowane przez CENELEC i ujęte w normie **PN-EN 50159:2011**. Zdefiniowane zostały cztery modele transmisji związane z bezpieczeństwem (rys. 1).



Rys. 1. Metody zabezpieczenia transmisji dla systemów związanych z bezpieczeństwem

Norma **PN-EN 50159-1** ma zastosowanie w zamkniętych systemach transmisyjnych (model A0), w których:

a) Dostęp do medium transmisyjnego jest autoryzowany
b) Znana jest maksymalna liczba użytkowników
c) W całym cyklu życia systemu medium transmisji jest niezmienne

W myśl normy **PN-EN 50159-1** bezpieczny system transmisji jest zdefiniowany, jako składający się z:

a) Niezaufanego systemu transmisji
b) Funkcji bezpieczeństwa

Każdej formie wymiany danych cyfrowych mogą towarzyszyć błędy. Zachodzi wtedy konieczność implementacji mechanizmów pozwalających określić integralność odebranego strumienia danych. Do wykrywania i korekcji błędów w torze transmisyjnym stosuje się kilka metod. Wprowadzają one pewną nadmiarową informację do przesyłanej wiadomości. Pozwala to na określenie czy odebrany strumień różni się od wysłanego.

Jedną z najbardziej popularnych metod wykorzystywanych do wykrywania błędów w zbiorach danych jest suma kontrolna CRC (Cyclic Redundancy Check). Jest to rodzina kodów przeznaczonych do zapewniania integralności danych cyfrowych. Pozwala wykryć błędy wynikające z istnienia szumów kanału (przekłamanie bitu) lub zaniku sygnału (utraty jednego lub więcej bitów). Kod taki generuje pewną liczbę dodatkowych bitów, które są dodawane do przesyłanej wiadomości. W zależności od doboru współczynników wielomianu generacyjnego uzyskujemy różne możliwości wykrywania błędów. Przykładowy wielomian generacyjny (tzw. CRC-32):

$$G\ (x) = x^{32} + x^{25} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10}\ x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1 \qquad (2)$$

Pozwala na wykrywanie:

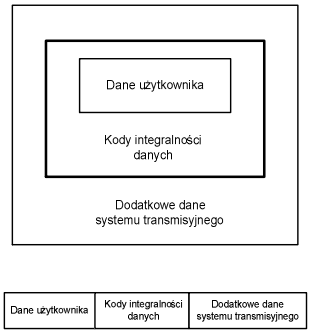
a) wszystkich błędów pojedynczych i podwójnych;
b) wszystkich błędów polegających na przekłamaniu nieparzystej liczby bitów;
c) wszystkich błędów seryjnych o długości serii nie przekraczającej 32.
d) Prawdopodobieństwo nie wykrycia błędu seryjnego 33-bitowego wynosi 2^{-31}.

Natomiast prawdopodobieństwo nie wykrycia błędu seryjnego 34-bitowego lub dłuższego – wynosi 2^{-32}

1.2. Charakterystyka bezpiecznej transmisji w wybranych systemach firmy KOMBUD S.A.

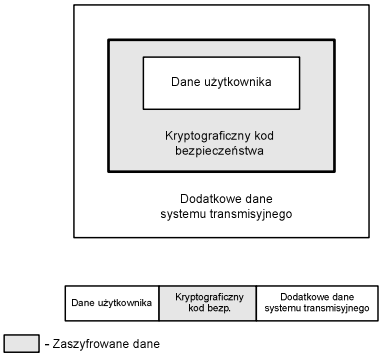
Bezpieczna transmisja w systemach sterowania ruchem kolejowym musi spełniać wymagania i zalecenia określone w obowiązujących właściwych normach PN-EN 50159: 2011. Bezpieczeństwo transmisji jest analizowane na poziomie systemu sterowania, jako jego element (norma PN-EN50126) oraz jest istotnie związane ze sprzętem i oprogramowaniem, co uwzględniają obowiązujące dla systemów kolejowych normy PN-EN 50129, PN-EN 50128.

Przy założeniu, że sieć transmisyjna jest zabezpieczona przed nieautoryzowanym dostępem model telegramu przyjmuje postać jak na rys. 2. Taką formę firma KOMBUD stosuje w systemach stacyjnych w przypadku konieczności powiązania z urządzeniami innych firm np. blokada SHL.



Rys. 2. Model telegramu z kodem integralności danych (typ A0)

Inne podejście należy zastosować, gdy przyjmiemy założenie braku pewności wykluczenia nieautoryzowanego dostępu. Wówczas zaleca się stosowanie technik kryptograficznych z użyciem tajnego klucza. Norma przewiduje w tym przypadku wykorzystanie technik kryptograficznych. Jednym z rozwiązań jest dodanie kryptograficznego kodu bezpieczeństwa np. w postaci zaszyfrowanego kodu integralności. Mówimy wówczas o telegramie typu A1. Model takiego telegramu dla tej metody przedstawiono na rys. 3.



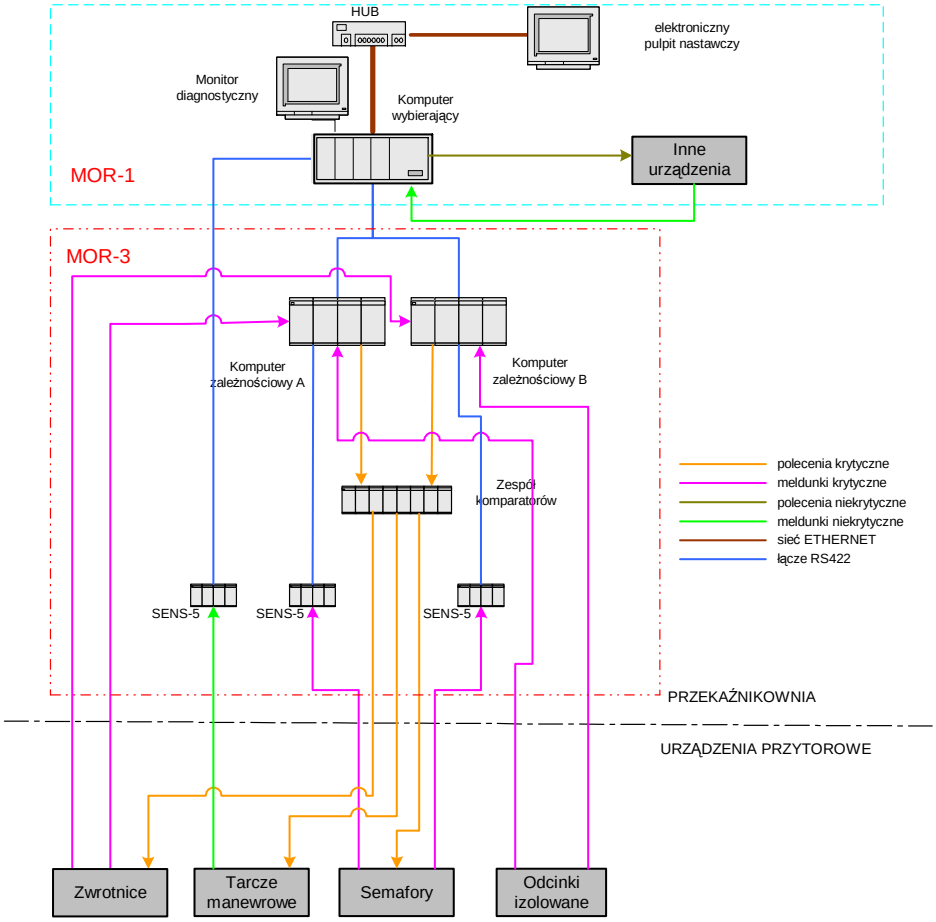
Rys.3. Model telegramu z kryptograficznym kodem bezpieczeństwa (typ A1)

Taki model transmisji wykorzystywany jest w systemach firmy KOMBUD w zakresie sterowania pojedynczym obiektem jak również w przypadku obszarowego sterowania (Mor-2lcsr).

Firma KOMBUD S.A. oferuje własne oryginalne rozwiązania systemów komputerowych. Głownie są to systemy stacyjne typu MOR, do których należą: komputerowy sterownik zależnościowy (MOR-3) (rys. 4), system nadrzędny współpracujący poprzez zdalne

sterowanie z urządzeniami zależnościowymi (Mor-2lcsr), komputerowe zobrazowanie i sterowanie istniejących systemów przekaźnikowych typu E (MOR-1), system kontroli zajętości (SKZR).

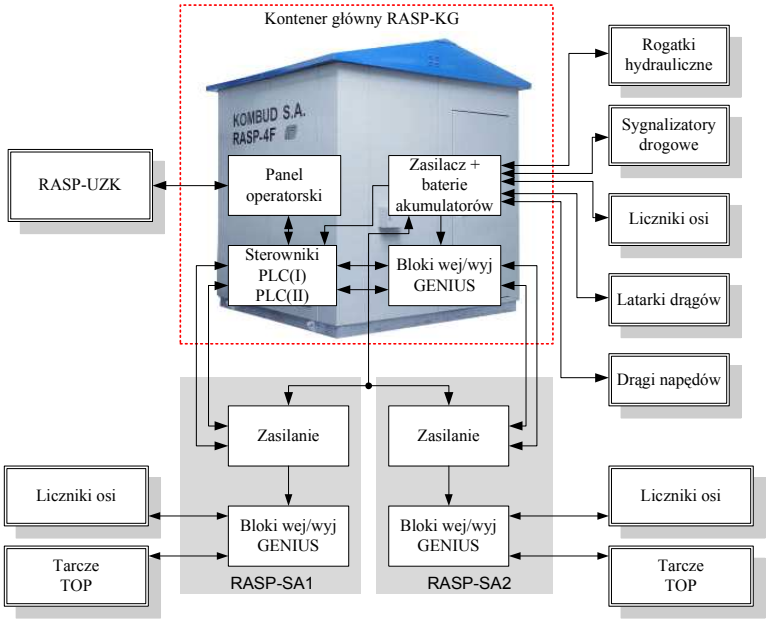
Transmisja danych pomiędzy systemami została zorganizowana w taki sposób, aby maksymalnie zwiększyć wykrywalność błędów przez kod CRC. Oznacza to zastosowanie kilku kodów CRC dla poszczególnych bloków danych. Dzięki temu oprócz zwiększenia wykrywalności przekłamań możliwe jest odczytanie nieprzekłamanych danych (błędny fragment jest ignorowany) i podjęcie odpowiedniej reakcji, co podnosi dostępność systemu.



Rys. 4. Schemat powiązań systemu MOR-3 (architektura systemu dla małej stacji)

Oprócz systemów stacyjnych KOMBUD produkuje systemy sygnalizacji przejazdowej typu RASP. Systemy SSP realizowane są w strukturze dwukanałowej („2 z 2”), co można zauważyć w przypadku systemu RASP 4F produkowanego przez KOMBUD S.A.

Sterowniki PLC zbudowane są w oparciu o dwa identyczne zestawy zbudowane na kasetach tworząc dwa niezależnie działające sterowniki ze wzajemną wymianą danych i synchronizacją pracy poprzez magistralę Ethernet. Schemat systemu z podziałem na moduły i bloki funkcjonalne przedstawia rys.5.



Rys. 5. Schemat blokowy samoczynnej sygnalizacji przejazdowej RASP-4F

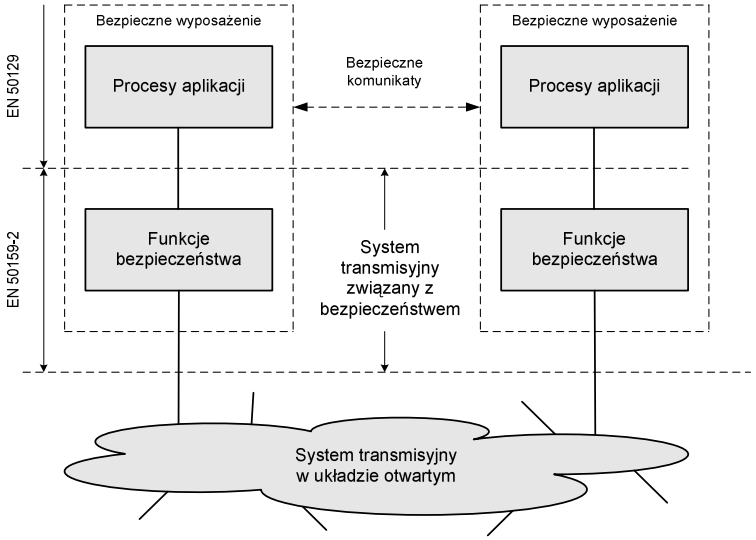
2. BEZPIECZNA TRANSMISJA OTWARTA

2.1. Ogólne zasady

Norma **PN-EN 50159-2** definiuje wymagania dotyczące bezpieczeństwa w układach otwartych łączności dla kolejowych systemów łączności, sygnalizacji i sterowania. W odróżnieniu od normy **PN-EN 50159-1** dostęp do kanału transmisyjnego jest możliwy przez nieuprawnionych użytkowników oraz liczba użytkowników i medium transmisyjne nie jest znane w całym cyklu życia (modele A1, B0, B1). Obydwie normy nie definiują systemu transmisyjnego i jego wyposażenia oraz nie rozróżniają, które dane są związane z bezpieczeństwem a które nie, natomiast zdefiniowane są zagrożenia i metody zapobiegania tym zagrożeniom.

Zgodnie z definicją w normie **PN-EN 50159-2** bezpieczny system transmisji (rys.6) składa się z:

a) Niezaufanego systemu transmisji
b) Funkcji związanych z bezpieczeństwem
c) Funkcji związanych z bezpiecznym dostępem



Rys. 6. Otwarty bezpieczny system transmisji wg PN-EN 50159-2

Zgodnie z normą, dla wiadomości transmitowanych w układach otwartych występuje siedem zagrożeń [6]:

a) powtórzenie wiadomości,
b) utrata wiadomości,
c) wstawienie nadmiarowej wiadomości,
d) nie zachowanie sekwencyjności,
e) uszkodzenie wiadomości,
f) opóźnienie dostarczenia wiadomości,
g) podszycie się pod wiadomość (maskarada).

Na podstawie normy PN-EN 50159-2 w tabeli 2 podano zestawienie zagrożeń i metod obrony (funkcji bezpieczeństwa).

Tabela 2. Zestawienie zagrożeń i metod obrony [10]

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**
Powtórzenie (*repetition*)	X	X						
Skasowanie (*deletion*)	X							
Brak autoryzacji (*insertion*)	X			X	X	X		
Zmiana kolejności (*resequence*)	X	X						
Uszkodzenie (*corruption*)							X	X
Opóźnienie (*delay*)		X	X					
Maskarada (*masquerade*)					X	X		X

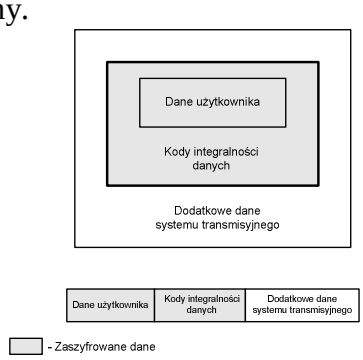
A. numerowanie telegramów (*sequence number*),
B. stosowanie w telegramach znaczników czasu (*time stamp*),
C. zdefiniowanie maksymalnego czasu oczekiwania na odpowiedź (*time-out*),
D. dodawanie do telegramów identyfikatora nadawcy i odbiorcy,
E. stosowanie komunikatów zwrotnych (*freedback message*),
F. wykorzystywanie procedur autoryzacji (*identification*),
G. stosowanie kodów bezpieczeństwa (*safety code*),
H. szyfrowanie danych (*cryptographics*).

2.2. Charakterystyka bezpiecznej transmisji otwartej w przyszłościowych systemach firmy KOMBUD S.A.

Zakładając, że systemy z transmisją zamkniętą (dopuszczone do eksploatacji w UE i w Polsce) spełniają wymagania norm PN-EN 50129, PN-EN 50128, PN-EN 50159 należy uważać, że systemy z transmisją otwartą opartą o zalecenia normy PN-EN 50159 powinny zapewnić analogiczny poziom bezpieczeństwa.

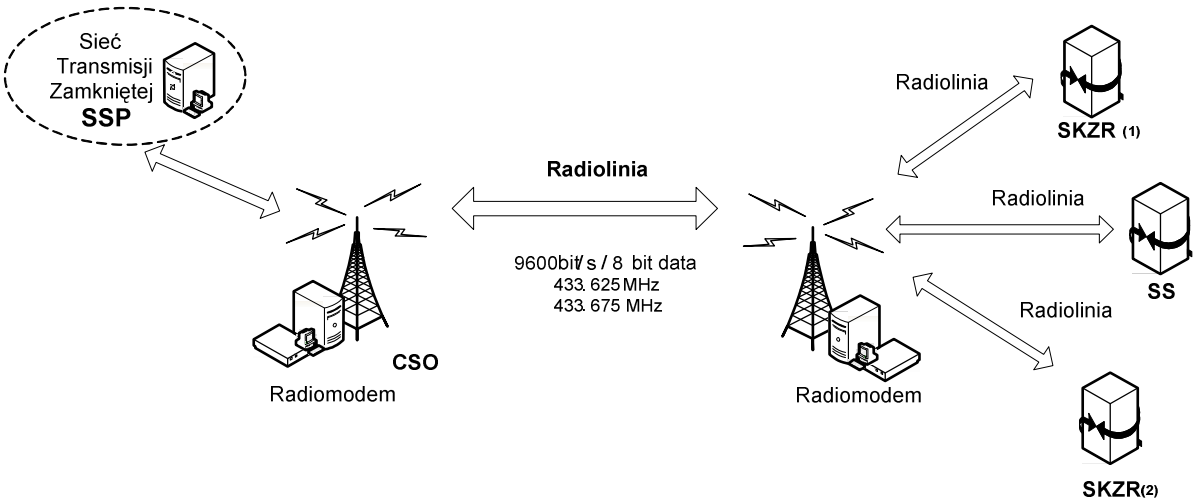
Wprowadzany system transmisji otwartej wykorzystującej publiczne sieci radiowe powinien zapewnić dotychczasowy poziom bezpieczeństwa (zgodny z klasyfikacją SIL, wynikający z norm PN-EN 50128, PN-EN 50129) oraz nie gorszy od poziomu funkcjonalności w istniejących systemach (dotyczy to zwłaszcza opóźnień i przerw w transmisji).

W innowacyjnych rozwiązania nowych systemów sterowania firma KOMBUD S.A. przyjęła model B0 dla układów z transmisją otwartą (rys. 7) kanałem radiowym wykorzystującym radiomodemy.



Rys. 7. Model telegramu z zaszyfrowaną wiadomością (typ B0)

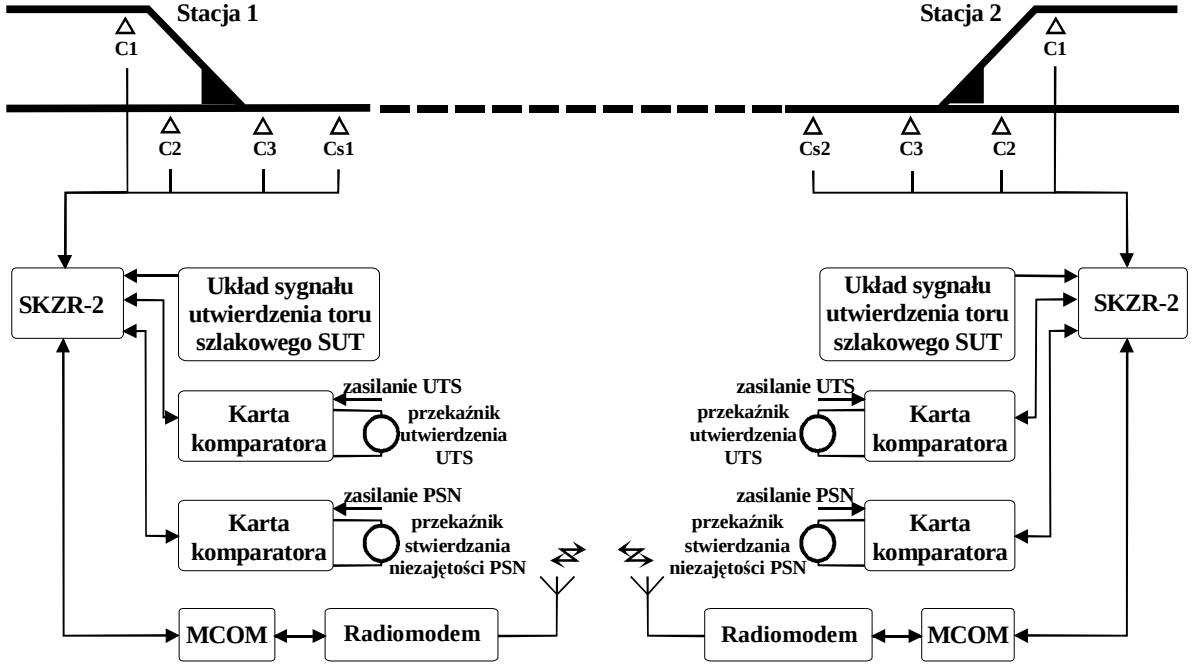
Kanał radiowy wykorzystywany jest do przekazywania informacji między sterownikami współpracującymi z czujnikami koła a sterownikami systemu ssp umieszczonymi w kontenerze. Taka konfiguracja pozwala na wyeliminowanie konieczności wykonywania połączeń kablowych od oddalonych od przejazdu punktów oddziaływania (czujników). W przypadku systemów stacyjnych (MOR) dodatkowy kanał radiowy przekazuje informacje o stanie urządzeń i polecenia pomiędzy stanowiskiem obsługi (CSO) a sterownikiem stacyjnym (SS). Taki kanał transmisyjny może być redundantny dla połączenia kablowego lub być podstawowym medium transmisji. Mając na uwadze dostępność systemu (awaria połączenia kablowego) firma KOMBUD S.A. wprowadziła odmianę systemu SKZR, który umożliwia kontrolę zajętości szlaków realizowaną poprzez kanał radiowy. W tak realizowanym obszarowo systemie sterowania (LCS) poszczególne systemy komunikują się poprzez wydzielone kanały transmisji radiolinii, co zapewnia m.in. kontrolę autoryzacji dostępu (rys. 8).



Rys. 8. Przykład łączności radiowej w obszarze LCS

W systemie przyjęto telegramy zgodne z typem transmisji B0 (rys. 7), wykorzystując techniki kryptograficzne z kluczem tajnym oraz szyfrowanie danych w całości łącznie z kodem integralności danych (standard AES z kluczem 128-bitowym oraz kod CRC32).

Odmiana SKZR-2 jest wersją wcześniejszego licznikowego systemu kontroli niezajętości typu SKZR, przystosowaną do łączności bezprzewodowej. SKZR-2 został wyposażony w dodatkowy mechanizm kontroli sekcji szlakowych w postaci interfejsu przekaźnikowego, który realizuje funkcję utwierdzenia sekcji w przebiegu wyjazdowym. System SKZR-2 udostępnia meldunki o stanie kontrolowanych sekcji (zwrotnica, układ zwrotnic, odcinek toru stacyjnego, odcinek toru szlakowego) za pośrednictwem interfejsu przekaźnikowego (rys. 9).



Rys. 9. Sposób kontroli niezajętości toru szlakowego przy wykorzystaniu transmisji radiowej do bezpiecznej komunikacji systemów SKZR-2.

Interesującym rozwiązaniem zastosowanym dla systemu Mor-2lcsr i SKZR-2 jest manager komunikacji (MCOM). MCOM umożliwia w pełni wykorzystanie radiowego kanału half-duplex eliminując kolizje i repetycje jednocześnie pozostając dla systemów sterowania

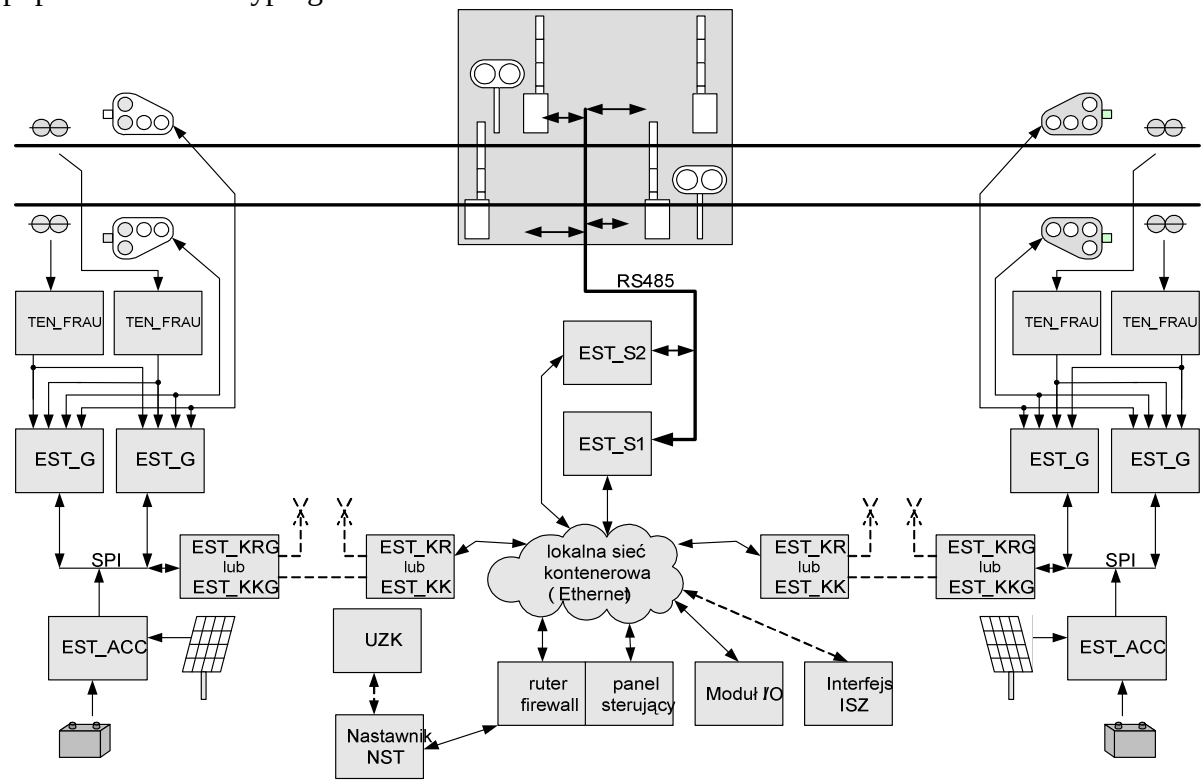
transparentnym. Dodatkowo możliwe jest szyfrowanie (AES-128) każdego połączenia (radiolinii rys. 8) innym kluczem.

Innym systemem, w którym wykorzystywany jest otwarty kanał transmisyjny jest system zabezpieczenia przejazdów SZP-1. SZP-1 (rys.10) przeznaczony jest do zabezpieczenia ruchu na przejazdach kolejowych kategorii „A", „B" i „C".

Podsystem sterowania zlokalizowany w kontenerze, odbiera i analizuje sygnały pochodzące od podsystemu urządzeń oddziaływania (PUO) oraz steruje i kontroluje elementami należącymi do podsystemu urządzeń wykonawczych i kontrolnych (PUW) tj.:

- sygnalizatory drogowe,
- rogatki,
- tarcze ostrzegawcze przejazdowe.

Podsystem sterowania może również sterować i kontrolować inne urządzenia, które tworzą podsystem urządzeń dodatkowych (PUD). Realizuje także, poprzez interfejs ISZ, powiązanie z systemami zależnościowymi (stacyjnymi) oraz zapewnia współpracę z urządzeniami zdalnej kontroli (UZK).Podsystem urządzeń oddziaływania (PUO) komunikuje się z podsystemem sterowania wykorzystując kanał transmisji bezprzewodowej. Urządzenia zdalnej kontroli (UZK) są opcjonalne dla każdej z kategorii przejazdów. W systemie SZP-1 UZK może być połączone z urządzeniami na przejeździe kanałem transmisji kablowym lub bezprzewodowym. Tak jak w przypadku systemu Mor-2lcsr i SKZR-2 tu również wykorzystany jest model B0 zdefiniowany w normie PN-EN 50159 zapewniający odpowiedni poziom bezpieczeństwa jak również ochronę przed nieautoryzowanym dostępem realizowaną poprzez techniki kryptograficzne.



Rys. 10. System zabezpieczenia przejazdów SZP-1 z transmisją radiową

PODSUMOWANIE

Bezpieczna transmisja w systemach sterowania ruchem kolejowym musi spełniać wymagania i zalecenia określone w obowiązujących właściwych normach PN-EN 50159: 2011 [25]. Bezpieczeństwo transmisji jest analizowane na 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.

Wprowadzany system transmisji otwartej wykorzystującej publiczne sieci radiowe powinien zapewnić dotychczasowy poziom bezpieczeństwa (zgodny z klasyfikacją SIL, wynikający z norm PN-EN 50128, PN-EN 50129) oraz nie gorszy od poziomu funkcjonalności w istniejących systemach (dotyczy to zwłaszcza opóźnień i przerw w transmisji).

Rozwiązania zastosowane przez firmę KOMBUD S.A. reprezentują aktualnie obowiązując standardy i zarówno pod względem funkcjonalnym, jak też bezpieczeństwa w niczym nie ustępują analogicznym systemom produkowanym obecnie w UE. Spełniają wszystkie obowiązujące normy w zakresie projektowania i eksploatacji komputerowych systemów srk. Dotyczy to systemów już eksploatowanych (gdzie wyniki oparto na analizie statystycznej danych eksploatacyjnych), systemów aktualnie produkowanych (gdzie do analizy zastosowano charakterystyki niezawodnościowe producenta stosowanych komponentów] oraz systemów aktualnie projektowanych i testowanych (gdzie zastosowano prognozowanie niezawodności).

Pod względem rozwiązań technicznych w zakresie systemów liniowych, stacyjnych i przejazdowych urządzenia te nie odbiegają od urządzeń innych firm, produkowanych w państwach UE. Przedstawione nowatorskie rozwiązania oparte o bezprzewodowe standardy *transmisji pokazują duże możliwości w zakresie innowacyjnej techniki sterowania ruchem kolejowym.

THE SAFETY TRANSMISSION IN RAILWAY CONTROL SYSTEMS ACCORDING TO KOMBUD S.A. SOLUTIONS

Abstract

The paper deals with requirements defined for digital transmission applied tor safety railway control systems according to existing standards. the paper contains the introduction to the presented problem and practical realization with respect to some railway control systems produced by KOMBUD S.A.

BIBLIOGRAFIA

1. Dokumenty firmy KOMBUD S.A.
2. Fault Tree Analysis (FTA), International Standard, IEC 61025:2006
3. Lewiński A., Bester L.: „Zastosowanie nowych standardów transmisji bezprzewodowej w systemach zarządzania i sterowania ruchem kolejowym" Prace Naukowe Politechniki Warszawskiej, Transport z.62, 2007, Stare Jabłonki 2007.
4. Lewiński A., Perzyński T.: „Akceptowalny poziom ryzyka, jako kryterium bezpieczeństwa w transporcie kolejowym", prace konferencji Wydziału Transportu Politechniki Radomskiej LogiTrans 2007.
5. Lewiński A., Toruń A., Bester L.: „ Sposoby realizacji transmisji otwartej w systemach sterowania ruchem kolejowym". Logistyka 3/2011.
6. Łukasik Z., Nowakowski W.: „Wymiana informacji w systemach związanych z bezpieczeństwem", XII Międzynarodowa Konferencja „TransComp", Zakopane 2008r.

7. Norma PN-EN 50126:2002 (U) Zastosowania kolejowe. Specyfikowanie i wykazywanie Nieuszkadzalności, Gotowości, Obsługiwalności i Bezpieczeństwa (RAMS). Część 1: Wymagania podstawowe i procesy ogólnego przeznaczenia.
8. Norma PN-EN 50128:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Oprogramowanie dla kolejowych systemów sterowania i zabezpieczenia.
9. Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.
10. Norma PN-EN 50159: 2010. Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania.
11. Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym – DG PKP KA nr KA2b-5400-01/98 z dnia 06.02.1998r.

Autorzy:
dr hab. inż. Andrzej LEWIŃSKI, prof. nadzw. UTH Rad. – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu
Tomasz KALBARCZYK - KOMBUD S.A.