Zagrożenia przewodowych i bezprzewodowych systemów transmisji danych w systemach zarządzania i sterowania ruchem kolejowym z uwzględnieniem cyberataków i ataków terrorystycznych

The threats of wire and wireless data transmission systemsin rail traffic and management systems including cyber and terroristic attacs

Andrzej Lewiński

Prof. dr hab. inż.

Uniwersytet Technologiczno-Humanistyczny im. K. Pułaskiego w Radomiu

a.lewinski@uthrad.pl

Streszczenie: Praca ma na celu przedstawienie aktualnego stanu zabezpieczeń w obecnie eksploatowanych rozproszonych, komputerowych systemów zarządzania i sterowania ruchem kolejowym, ale też systemów przyszłościowych związanych z wdrażaniem w kolejnictwie polskim opartych na standardach bezprzewodowych też związanych z ERTMS/ETCS.

Słowa kluczowe: *Przewodowa i bezprzewodowa transmisja danych*

Abstract: The paper deals with presentation of up to date state of protection in dissipated, computer railway control and management systems, including the future systems implemented in Polish State Railways based on wireless standards with regard the ETMS/ETCS solutions.

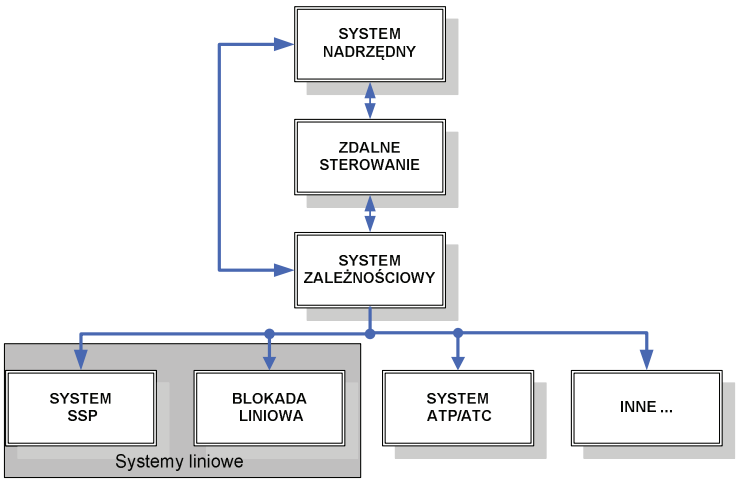
Keywords: *Wired and wireless data transmission*

Systemy sterowania to głównie nadmiarowe (2 z 2, 2 z 3) sterowniki komputerowe o bardzo niskiej intensywności uszkodzeń z szybką (rzędu 0.001 – 0.1 sek.) reakcją na wykrytą pojedynczą usterkę w systemie, co zapewnia spełnienie obowiązujących w UE (także w kolejnictwie polskim) wymagań bezpieczeństwa SIL (ang. Safety Integrity Level). Typowy, obecnie eksploatowany system zarządzania i sterowania ruchem kolejowym jest rozproszonym systemem komputerowym o strukturze przedstawionej na rys. **1**.

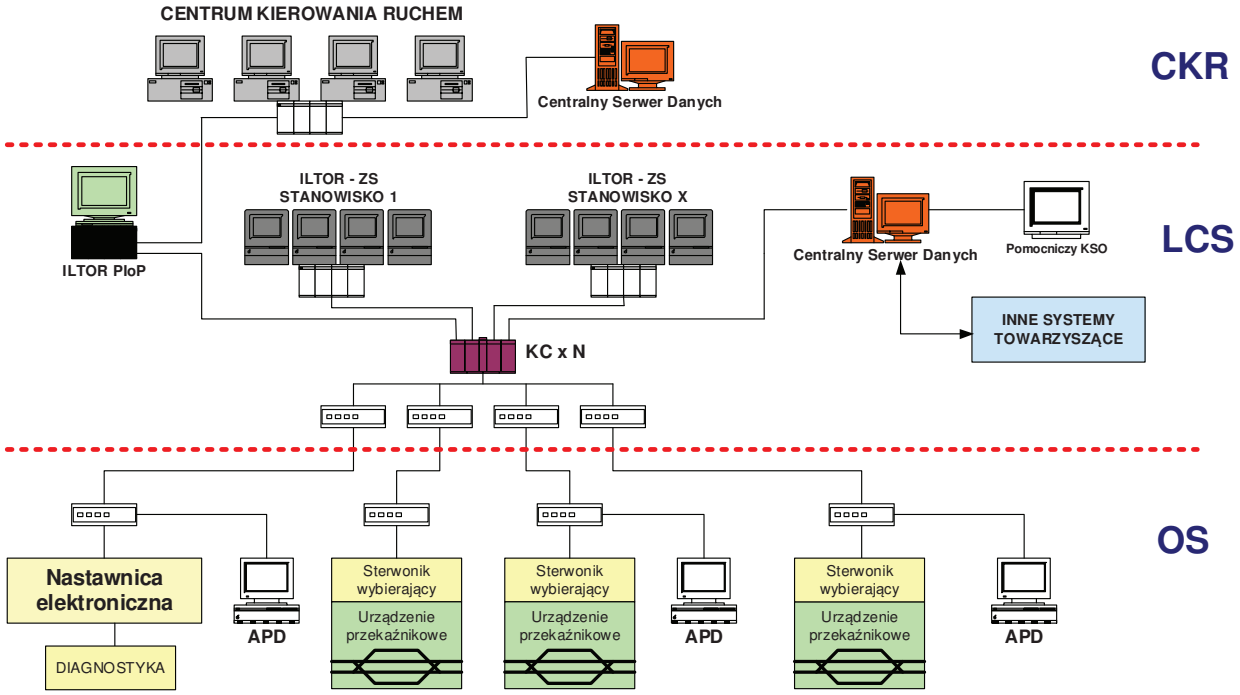
Pomiędzy podsystemami jest sieć transmisyjna narażona na zakłócenia ale też na ataki (hakerskie, terrorystyczne) mogące ingerować w proces sterowania zagrażając bezpieczeństwu. Typowym przykładem systemu zarządzania i sterowania ruchem kolejowym może być system ILTOR 2 [1], [23] powszechnie stosowany w UE (w tym w Polsce), w którym zainstalowano jest wiele terminali, oraz serwery i rutery pracujące w sieci lokalnej (ETHERNET). Struktura systemu będącego rozproszonym komputerowym systemem sterowania którego podsystemy (oraz urządzenia) komunikują się poprzez standardy sieciowe, została przedstawiona na rys. **2**. System NSRK obejmuje

- systemy nadrzędne,
- systemy zależnościowe,
- systemy zdalnego sterowania,
- systemy liniowe (ssp, blokady liniowe),
- ATP/ATC.

Od ponad 40 lat są w UE eksploatowane komputerowe systemy zarządzania i sterowania ruchem kolejowym (ZSRK) . Są to komputerowe systemy rozproszone o strukturze hierarchicznej (dyspozytorski system nadrzędny, systemy zależnościowe obejmujące stacje oraz blokady liniowe, a także systemy lokalne – sterowniki obiektowe przypisane do zwrotnic i sygnalizatorów oraz systemy samoczynnej sygnalizacji przejazdowej,



1*. Typowa struktura systemu zarządzania i sterowania ruchem kolejowym [1]*



***2**. Współczesne centrum sterowania ruchem kolejowym – ILTOR-2 [23]*

kontroli nie zajętości torów itp.) . Podstawą poprawnego funkcjonowania jest efektywna transmisja przekazująca stan kontrolowanych obiektów oraz polecenia sterujące.

Jednak problem odporności systemów transmisji danych pomiędzy podsystemami i elementami na zagrożenia spowodowane próbami przejęcia i zmiany przesyłanych informacji nie został do tej pory poruszony. Systemy zarzadzania i sterowania ruchem kolejowym muszą spełniać rygorystyczne normy dotyczące organizacji systemu (EN-PN 50 126) [10], konfiguracji sprzętu (EN-PN 50 129) [12] , oprogramowania (EN-PN 50 128) [11] i transmisji (EN-PN 50 159) [13], ale do tej pory brak jest badań pod kątem oceny odporności tych systemów na zagrożenia spowodowane próbami ataków.

Bezpieczeństwo transmisji w systemach nadzoru i sterowania ruchem kolejowym

Od 2005 roku (wejście Polski do struktur UE) zasady transmisji są uregulowane przez obowiązujące normy (CENELEC). Podstawą była norma EN 50159.1, która regulowała transmisję przewodową w systemach NSRK, ale jej stosowanie nie dotyczyło systemów już eksploatowanych gdzie producenci mogli stosować własne rozwiązania, niekoniecznie zgodne z wymaganiami normy.

Wspomniana norma PN-EN 50 159-2011 dopuszcza możliwość stosowania bezprzewodowych standardów transmisji pod warunkiem, że zapewniony jest ten sam poziom funkcjonalności i bezpieczeństwa, co w dotychczasowych realizacjach wykorzystujących transmisję kablową. Dotyczy to zarówno przewodowych, jak też bezprzewodowych standardów transmisji. Podstawowym kryterium jest zapewnienie dopuszczalnego poziomu ryzyka (THR) zgodnie z obowiązującymi normami PN-EN 50 126 i PN-EN 50 129 [5-8]. Oznacza to, że wskaźnik THR [2] dla systemów srk zaliczonych do danego poziomu bezpieczeństwa SIL nie powinien przekroczyć przewidzianej dla tego poziomu maksymalnej wartości.

Realizacja transmisji informacji musi być przeprowadzona w taki sposób, aby możliwa była 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.

W systemach transmisji otwartej transmisja prowadzona jest z wykorzystaniem sieci radiowej, sieci Internet lub poprze 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.

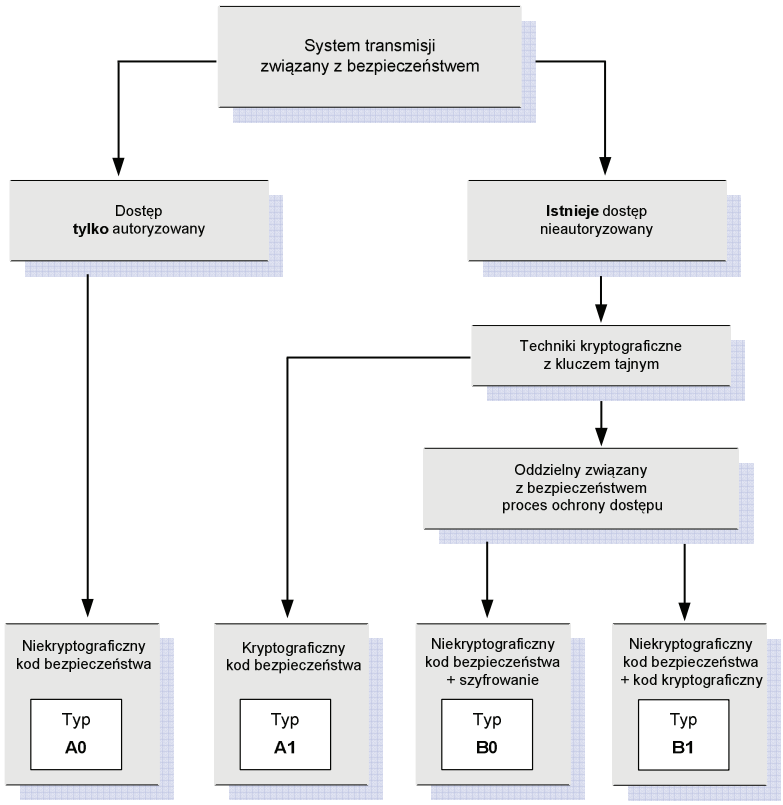
Otwarty, ale też zamknięty system transmisji narażony jest na następujące typy zagrożeń:

1. Maskarada,
2. Wstawienie,
3. Powtórzenie,

4. Usunięcie,
5. Zmiana kolejności,
6. Opóźnienie.

Zastosowano też w systemach NSRK następujące sposoby zabezpieczenia przesyłania informacji przed wymienionymi zagrożeniami:

1. Maskarada, czyli celowe lub niecelowe „podszycie się" innego systemu pod system srk. Zgodnie z normą zaleca się użycie technik kryptograficznych poprzez zastosowanie algorytmów szyfrujących oraz kluczy uwierzytelniających. W proponowanej koncepcji, aby zachować wymagany poziom bezpieczeństwa zastosowano szyfrowane tunele VPN z protokołami IPsec, algorytmy szyfrujące DES (ang. Data Encryption Standard), 3DES i AES (ang. Advanced Encryption Standard). Natomiast zastosowanie algorytmu uzgadniania kluczy Diffiego-Hellmana eliminuje możliwości przechwycenia pakietów poprzez podsłuch kanału komunikacyjnego.
2. Wstawienie, czyli ataki związane z uzyskaniem dostępu do przesyłanych informacji lub podsyłaniem przetworzonych pakietów. W proponowanym rozwiązaniu zastosowano tryb tunelowania, wykorzystując protokół IPsec (ang. 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.
3. Powtórzenie. Aby zapobiec powtarzalności pakietów zastosowano nagłówek IPsec – ESP w ruchu pakietów (ang. Encapsulating Security Payload), który zapewnia uwierzytelnianie, identyfikację oryginalności oraz integralności danych. Dodatkową ochronę przed powtarzaniem pakietów zapewnia dołączenie kolejnego numeru do każdego pakietu.
4. Usunięcie. Ochrona przeciw atakom usuwania, modyfikacji, powtórzeń lub przekierowania telegramów do innych odbiorców realizowana jest poprzez mechanizmy kryptograficzne ISAKMP (ang. Internet Security Association and Key Management Protocol), min 3DES, SHA-1 lub MD5, DH2 zgodnie z zaleceniami norm.
5. (oraz 6.) Zmiana kolejności, opóźnienie. Zmiana kolejności i opóźnienia telegramów została rozwiązana poprzez zastosowanie protokołu IPsec (tunel IPsec oraz format pakietów ISAKMP), a także kontrolę czasu.



***3**. Klasyfikacja zabezpieczeń transmisji dla systemów transmisji otwartej [13]*

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.

Przyjmując zalecenia norm przyjęto w koncepcji wykorzystania sieci otwartych strukturę telegramu transmisji, model typu B0 (rys. **3** i **4**). Zapewniono tym samym wymaganą postać informacji oraz odpowiedni proces jej przetwarzania, stosując metody zabezpieczeń przed wymienionymi zagrożeniami transmisji w sieci STO.

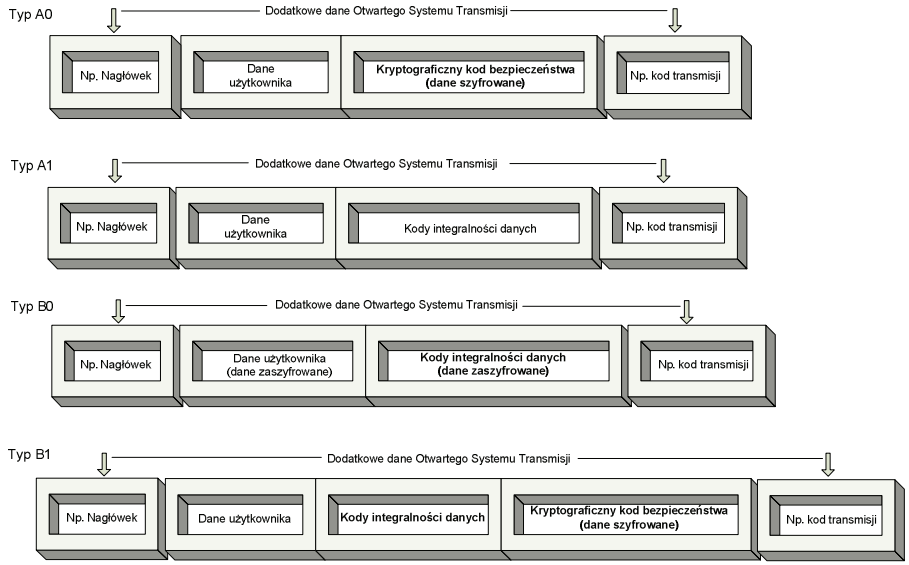
Zgodnie przyjętą klasyfikacją systemów powiązanych z bezpieczną transmisją przyjęto poniżej określoną klasyfikację grup transmisji:

- A0 – tylko autoryzowany dostęp, nie jest stosowany kryptograficzny kod bezpieczeństwa,
- A1 – bez wykluczenia nieautoryzowanego dostępu, zaleca się stosowanie kryptograficznego kodu bezpieczeństwa,
- B0 – bez wykluczenia nieautoryzowanego dostępu, nie jest stosowany kryptograficzny kod bezpieczeństwa, wymagane jest szyfrowanie,
- B1 – bez wykluczenia nieautoryzowanego dostępu, nie jest stosowany kryptograficzny kod bezpieczeństwa, wymagany jest kod kryptograficzny.

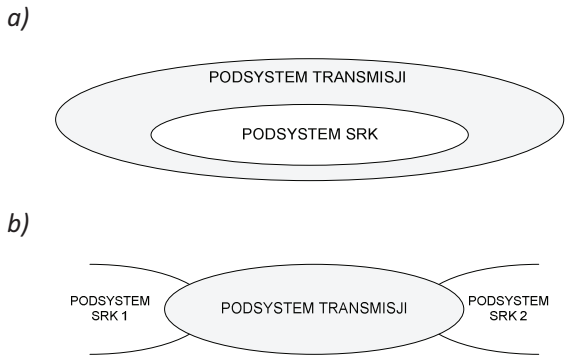
Postać informacji dla każdego typu bezpiecznej transmisji przedstawiają schematy pokazane na rys. **4** .

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

Właściwie przeprowadzona analiza dotycząca oceny wpływu zastosowanego systemu transmisji na parametry niezawodności i bezpieczeństwa syste-



***4**. Struktura informacji w systemach bezpiecznej transmisji zgodnie z normą PN-EN 50159-2 [13]*



***5**. a.) Struktura systemu z transmisją otwartą wpisaną w system nadmiarowy b.) Szeregowa struktura systemu jednokanałowej transmisji otwartej*

mu srk wymaga indywidualnej analizy odnoszącej się do konkretnego typu aplikacji. Oznacza to, iż każdorazowe zastosowanie systemu transmisji w urządzeniach srk wymaga, zgodnie z obowiązującymi w tym zakresie normami, wymaganiami i zaleceniami [10 – 20], zastosowania odpowiedniej procedury postępowania, której etapy są zdefiniowane następująco:

1) aplikacja,
2) analiza zagrożeń,
3) redukcja ryzyka,
4) przypisanie systemu do poziomów bezpieczeństwa SIL,
5) specyfikacja wymagań bezpieczeństwa.

Każdy z wyżej wymienionych punktów wymaga odrębnego uzasadnienia i stosownego udokumentowania. W odniesieniu do systemów srk szczególną uwagę należy położyć na oszacowanie poziomu ryzyka (norma PN-EN 50126). Intensywność uszkodzeń dla ustalonego poziomu SIL określają normy: PN-EN 50126, PN-EN 50128, PN-EN 50129. Na przykład dla systemów sterowania ruchem kolejowym odpowiedzialnych za bezpieczeństwo przyjmuje się wartość z przedziału $10^{-9} \leq THR < 10^{-8}$ dla poziomu SIL 4.

Przeważnie proponowane systemy transmisji są systemami jednokanałowymi, w związku z tym tolerowany poziom ryzyka THR (ang. Tolerable Hazard Rate) [2],[27] jest równy intensywności uszkodzeń. Dla poziomu SIL4 powinien zawierać się w granicach $10^{-9} \div 10^{-8}$ [h^{-1}]. W przypadku, gdy dotyczy systemów dwu- lub trzykanałowych istotny staje się czas wykrycia usterki, co pozwala na większe intensywności usterek w kanałach transmisyjnych. Schematycznie zależność podsystemu transmisji i srk w systemie z transmisją otwartą pokazano na rysunku **5**.

W przypadku zastosowania jako medium transmisji bezprzewodowej, należy dodatkowo uwzględnić charakterystyczne wskaźniki dotyczące transmisji, zabezpieczenie czy kodowanie. Ważnym w tym przypadku staje się długość kodu zabezpieczającego CRC (ang. *Cyclic Redundancy Code*).

Typowym zabezpieczeniem integralnosci danych jest cykliczny kod nadmiarowy CRC-32 (ang. *Cyclic Redundancy Code*) o założonym odstępie Hamminga. Prawdopodobieństwo błędnej transmisji PF wynosi wtedy [1], [4],

$$P_F = \sum_{i=D}^{N} \frac{N!}{i!*(N-i)!} * p^i * (1-p)^{N-i} \quad (1)$$

gdzie : D – odległość Hamminga,
N – długość słowa kodowego,
p – bitowe prawdopodobieństwo przekłamania (przyjmuje się typową wartość 10^{-4} dla transmisji radiowych [107]).

Dla telegramów o długości 500B i 1000B, prawdopodobieństwo błędnej transmisji wynosi odpowiednio:

$$P_{F500} = 6.98x10^{-11}, P_{F1000} = 1.74x10^{-8} \quad (2)$$

a prawdopodobieństwo poprawnie przesłanego telegramu:

$$P_S = (1 - BER)^N \quad (3)$$

gdzie : N – długość telegramu,
BER – bitowa stopa błędu (obliczona ze wzoru). Prawdopodobieństwo poprawnej transmisji telegramów 500 i 1000B przedstawia tabela **1**.

Przykłady transmisji bezpiecznej w systemach NSRK i odporności na zagrożenia

W kolejnictwie polskim od wielu lat są eksploatowane rozproszone systemy nadzoru i sterowania ruchem, w których integralną część stanowi transmisja danych. Zabezpieczenia zgodne z wymaganiami norm CENELEC są podstawą dopuszczenia tych systemów do eksploatacji (do badań eksploatacyjnych w przypadku systemów stosujących standardy bezprzewodowe).

Rozproszony system komputerowy z transmisją przewodową

Podstawą bezpiecznego i niezawodnego realizowania procesów sterowania

ruchem kolejowym jest zapewnienie bezpiecznego i właściwego przepływu informacji pomiędzy systemami biorącymi udział w tym procesie. W systemach srk transmisja jest związana z przekazywaniem pomiędzy urządzeniami rozkazów sterujących (polecenia, zezwolenia na jazdę,…) oraz potwierdzeń ich realizacji (meldunki, raporty o położeniu,…).

Bezpieczna transmisja danych zarówno w zamkniętych, jak i otwartych systemach srk musi spełniać wymagania i zalecenia określone w wymienionych wcześniej obowiązujących normach. Za system transmisji zamkniętej uważany jest system w którym [1]:

- dozwolony jest tylko autoryzowany dostęp,
- znana jest maksymalna liczba uczestników podłączenia,
- medium transmisyjne (najczęściej przewód miedziany lub światłowód) jest znane i podłączone na stałe do komunikujących się urządzeń.

W takim przypadku prawdopodobieństwo nieuprawnionego dostępu można uznać za znikomo małe, chociaż w sieci może pracować zarówno sprzęt zabezpieczony, jak i niezabezpieczony.

Dobrym przykładem systemu bezpiecznej transmisji jest powiązanie elementów scentralizowanego systemu zależnościowego MOR-3 (produkcji KOMBUD S.A. [21], [22] przedstawionego na rys. **6** (system ten może współpracować z systemem nadrzędnym MOR-1, lub innym tego typu systemem, np. EBISCREEN produkcji BOMBARDIER TRANSPORTATION ZWUA S.A.) Na prezentowanym schemacie wyróżnione zostały podstawowe warstwy funkcjonalne: poziom interfejsu użytkownika (MOR-1), komputerowych urządzeń stacyjnych oraz obwodów wykonawczych (MOR-3).

W systemie zostały wyróżnione wymienione warstwy funkcjonalne:

- Interfejs użytkownika – elektroniczny pulpit nastawczy – urządzenia warstwy obsługi i wizualizacji służą do zobrazowania stanu urządzeń srk oraz sytuacji ruchowej w nadzorowanym okręgu.
- System zależnościowy – system odpowiedzialny za bezpieczeństwo nastawiania i zwalniania przebiegów, oraz kontrolę stanu urządzeń sterowanych. Komunikuje się z urządzeniami przytorowymi poprzez zespół wejść i wyjść oraz z warstwą interfejsu użytkownika (pulpitem nastawczym).
- Warstwę urządzeń i systemów przytorowych – napędy zwrotnicowe, obwody torowe, sygnalizatory itp.

Tab. 1. Prawdopodobieństwo poprawnej transmisji w funkcji bitowej stopy błędów BER [2]

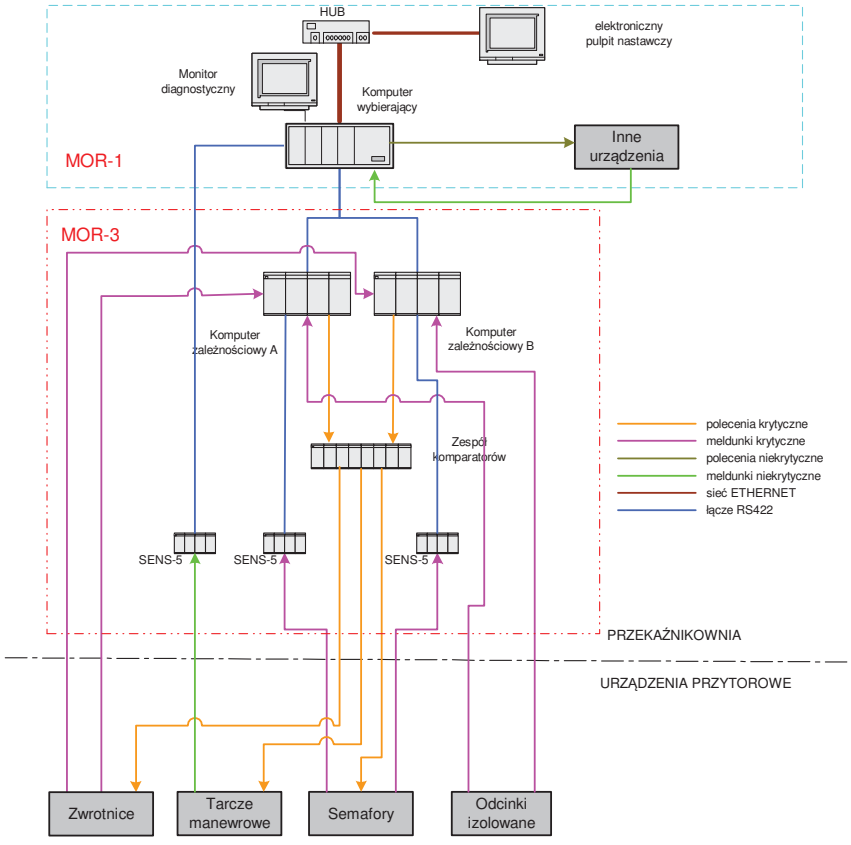
Prawdopodobieństwo poprawnej transmisji telegramu PS	BER – bitowa stopa błędu (telegram 500B)	BER – bitowa stopa błędu (telegram 1000B)
1	0	0
0.9	0.00021	0.000105
0.8	0.00044	0.000221
0.7	0.00071	0.000356
0.6	0.00102	0.000510
0.5	0.00138	0.000692
0.4	0.00183	0.000915
0.3	0.00240	0.001203
0.2	0.00321	0.001608
0.1	0.00459	0.002299

Na prezentowanym schemacie wyróżnione zostały podstawowe warstwy funkcjonalne: poziom interfejsu użytkownika (MOR-1), komputerowych urządzeń stacyjnych oraz obwodów wykonawczych (MOR-3).

W praktyce system MOR-3 rozumiany jest jako system urządzeń stacyjnych składający się z komputerów zależnościowych oraz elementów wykonawczych z zastosowaniem komparatorów bezpiecznych.

Informacje z układu pomiarowego typu SENS przekazywane są do komputerów za pośrednictwem łączy szeregowych RS422, a poszczególne komputery połączone są siecią Ethernet. Również sieć Ethernet wykorzystana jest do powiązania komputerowych urządzeń stacyjnych z elektronicznym pulpitem nastawczym.

Telegram rozkazowe do sterownika zależnościowego są wysyłane przez sterownik wybierający stanowiący element interfejsu użytkownika. Wyróżnio-



6. System transmisji w systemie zależnościowym MOR-3 [21], [22]

no następujące grupy rozkazów:
- rozkazy do zwrotnicy,
- rozkazy do semafora,
- rozkazy do tarczy manewrowej,
- rozkazy do odcinka izolowanego,
- rozkazy do elementu uniwersalnego,
- rozkazy do elementu związanego ze sterowaniem obszarem.

System transmisji ma istotny wpływ na bezpieczną pracę systemu MOR-3. Zakłócenia w transmisji, traktowane jako usterki na poziomie sprzętu (norma PN-EN 50120-1), mogą potencjalnie doprowadzić do nieprawidłowego działania systemu lub nawet do stanów niebezpiecznych. Dlatego też w oprogramowaniu transmisji MOR-3 zastosowano wiele zabiegów mających na celu niedopuszczenie do powstania sytuacji niebezpiecznej.

Podstawowym zabezpieczeniem transmisji jest kod integralności danych CRC (ang. *Cyclic Redundancy Code*). Przyjmuje się, że dodatkowy nadmiar o długości n bitów powoduje istotne zmniejszenie intensywności uszkodzeń λ_N do poziomu λ_{NT} w sposób:

$$\lambda_{NT} = \lambda_N 2^n \qquad (4)$$

Oznacza to, że dla n=32 intensywność niebezpiecznych przekłamań maleje 4 109 razy.

W systemie MOR -3 zastosowano:
- Cykliczny Kod Nadmiarowy CRC 32 bitowy, zapewniający odstęp Hamminga D = 4 dla obszaru kodowanego o długości do 4000 bajtów, stosowany do zabezpieczania całości telegramu.
- Cykliczny Kod Nadmiarowy CRC 8-bitowy z wielomianem generacyjnym zapewniającym odstęp Hamminga D = 4, dla obszaru kodowanego o długości kilku bajtów. Używany do dodatkowego kodowania nagłówka telegramu.

Do innych zabezpieczeń należy zaliczyć takie metody, jak kodowanie ważnych (wrażliwych) informacji w ciele telegramu, tj.: znacznik typu telegramu, znacznik rodzaju polecenia (rozkazu); zostały dobrane specjalne zbiory kodów tak, aby odstęp Hamminga dla danego zbioru kodów był maksymalny.

Oprócz kodowania wprowadzono też zabezpieczenia podwyższające poziom bezpieczeństwa transmisji:
- zróżnicowanie nagłówków telegramów dla kanałów A i B oraz różnego miejsca występowania telegramu,
- zróżnicowanie długości i treści poszczególnych telegramów wraz z nadmiarem informacyjnym,
- kryterium czasu powodujące, że brak poprawnego telegramu w czasie około 1s jest interpretowane jako przerwa w transmisji i powoduje przejście systemu do stanu bezpiecznego,
- uszkodzenie kabli transmisyjnych, kart transmisji i zasilania powodując przerwę w transmisji i bezpieczną reakcję systemu.

Istotnym zabezpieczeniem jest tzw. „Telegram życia". Sterownik wybierający powinien co około 5 sekund wysyłać do sterownika zależnościowego telegram życia. Brak telegramu życia przez ponad 10 sekund powoduje praktyczne przejście systemu w stan awaryjny, a po kolejnych 10 sekundach następuje ustawienie wszystkich semaforów i tarcz manewrowych na stój.

Autorzy systemu oszacowali, że zastosowane zabezpieczenia zapewniają, że prawdopodobieństwo niewykrycia przekłamania telegramu jest mniejsze od $2{,}39*10^{-14}$, co jest wskaźnikiem znacznie korzystniejszym niż prawdopodobieństwo uszkodzenia sprzętu – komputera w pojedynczym kanale (liczonym dla całego czasu eksploatacji systemu).

Przyszłościowy system z otwartą transmisją bezprzewodową

W koncepcji systemu bezpiecznej transmisji zaproponowanej przez firmę KOMBUD S.A. Radom [21] (rys. **7**) zastosowano kanał radiowy (otwarty system transmisji) do przekazywania informacji w podsystemie urządzeń oddziaływania (występującymi w przejazdach kategorii B i C) sterownikami transmisji radiowej EST_KRG (informacje z głowic oraz polecenia dla Top) a odpowiadającym mu w kontenerze sterownikiem EST_KR (informacje rozsyłane w lokalnej sieci kontenerowej).

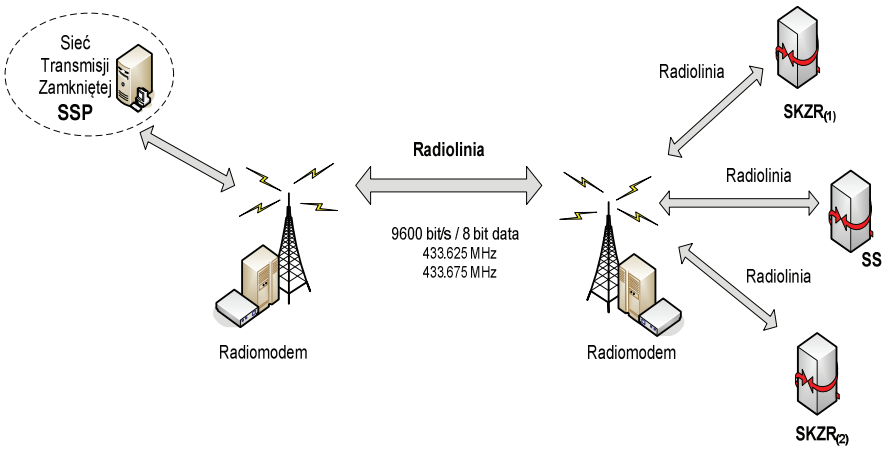
Zaznaczone na rysunku podsystemy to: SKZR (system kontroli zajętości), system sterowania na stacji (SS) i system sygnalizacji przejazdowej (SSP). W tej koncepcji systemu bezpiecznej transmisji zastosowany został kanał radiowy (otwarty) do przekazywania informacji w podsystemie urządzeń oddziaływania. Kanał radiowy wykorzystywany jest do przekazywania informacji między sterownikami współpracującymi z czujnikami koła a sterownikami systemu ssp. Taka konfiguracja pozwala na wyeliminowanie konieczności wykonywania połączeń kablowych od oddalonych od przejazdu punktów oddziaływania – czujników. W obecnej fazie badań eksperymentalnych połączenia radiowe traktowane są jako kanały rezerwowe, transmisja podstawowa wykorzystuje istniejące połączenia kablowe, światłowodowe i skrętki miedziane.

System transmisji otwartej oparty jest na radiolinii zapewniającej kontrolę autoryzacji dostępu. Do celów łączności wybrane zostały radiomodemy 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, co zostało potwierdzone odpowiednim certyfikatem.

Przyjmując, że poziom niezawodności zarówno dla transmisji zamkniętej, jak i otwartej charakteryzowany intensywnością uszkodzeń λ_N jest rzędu 10-4, pozwala to oszacować intensywność uszkodzeń niebezpiecznych (przy założeniu niewykrycia przekłamania w zastosowanym kodzie integralności CRC32) na takim samym poziomie jak w systemach zamkniętych z transmisją kablową (4), czyli $10^{-4}*2^{-32} = 4*10^{-13}$, co daje podstawę do zaliczenia podsystemu transmisji do poziomu SIL 4. Należy jednak przyjąć, że jest to minimalna intensywność uszkodzeń, a uwzględnienie w praktyce zakłóceń, przerw oraz usterek sprzętu i zaprogramowanych protokołów może znacznie podwyższyć tę wartość.

W koncepcji systemu ESTER (ESTER-ekonomiczny system zdalnego sterowania i kierowania ruchem kolejowym) 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 za-

szyfrowanych 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, które zabezpiecza przed przypadkowymi błędami, pozwalając na wykrycie pojedynczych lub seryjnych błędów.



7. Struktura systemu sterowania ruchem kolejowym z transmisją radiową [21]

Odporność systemów NSRK na zagrożenia hakerskie i terrorystyczne

Wspomniana norma PN- EN 50 159 uwzględniała awarie (uszkodzenia i błędy) transmisji spowodowane niewłaściwy działaniem systemów i urządzeń, nie zakładało się celowego, destrukcyjnego działania człowieka. W ostatnich czasach zaistniały sytuacje, gdy celowa ingerencja w system polegająca na przejęciu sterowania na linii kolejowej, lub związane z tym uszkodzenie urządzeń wykonawczych może w oczywisty sposób prowadzić do sytuacji krytyczne, dużej w skutkach katastrofy. Takie sytuacje nie były przewidywane 20 – 30 lat temu, kiedy wdrażano pierwsze systemy komputerowe o strukturze rozproszonej z transmisją kablową. Z kolei dopuszczone do użytkowania otwarte, bezprzewodowe systemy transmisji wprawdzie koncentrują się na kontrolowanej autoryzacji dostępu oraz kontroli integralności przesyłanych telegramów, to nie uwzględniają możliwości specjalizowanych ataków hakerskich typowych np. dla zaawansowanego Internetu (np. zmasowany atak olbrzymiej ilości telegramów blokujących serwery).

W przypadku obecnie eksploatowanych systemów z transmisją kablową można wymienić następujące zagrożenia będące skutkiem aktu terrorystycznego:

- Celowe uszkodzenie kabli transmisyjnych z możliwością ingerencję w sterowanie.
- Ingerencja w sterowniki i inne układy (kart transmisji i zasilania) powodująca zmianę programu sterowania. Dotyczy to niepowołanego dostępu do szaf sterowniczych i innych urządzeń zewnętrznych systemu.
- Niepowołany dostęp do centrum dyspozytorskiego (system nadrzędny, lokalne centrum sterowania, posterunek dyżurnego ruchu). Istnieje wtedy zarówno próba zmiany oprogramowania i związane z tym celowe błędne i katastrofalne w skutkach polecenia (nie kontrolowane przez dopuszczone i obecnie stosowane oprogramowanie kontrolujące poprawną pracę dyspozytorów).

Aby skutecznie zapobiec powyższym zagrożeniom należy:

- Skutecznie kontrolować integralność kabli transmisyjnych, poza „telegramami życia" należy dodatkowo kontrolować dynamicznie stan odcinków, sygnalizatorów i napędów zwrotnicowych zgodnie z zadanym przez dyspozytora sterowaniem. Wydaje się celowe skrócenie poniżej 0.5s. czasu „telegramu życia" co praktycznie wykluczy mechaniczne ingerencje. Przerwy w transmisji (np. poniżej 0.5s) powinny inicjować procedury awaryjne powiązane z pełną kontrolą stanu systemu.
- Zalecane jest inne kodowanie telegramów życia, np. przez wprowadzenie zabezpieczeń kryptograficznych (np. standard B0 wymieniony w normie).
- Wszystkie szafy sterownicze i obudowy urządzeń zewnętrznych powinny posiadać system alarmowy informujące służby ochrony o próbie ingerencji. Związana jest z tym autoryzacja serwisu i odpowiednie procedury kontrolne wraz z rejestracją dostępu do takich obiektów w centrum dyspozytorskim. (Można wprowadzić stosowaną obecnie w innych podobnych systemach bezpiecznych mobilną autoryzację obsługi wyłącznie w czasie dokonywania czynności serwisowych.)
- Właściwa polityka bezpieczeństwa w centrach dyspozytorskich, lokalnych centrach sterowania, posterunkach dyżurnych ruchu i nastawniach. Wprowadzenie monitoringu A/V i pełnej autoryzacji pracowników i ich czynności.
- Wszystkie usługi informatyczne związane z serwisem sterowników komputerowych we wszystkich obiektach powinny uwzględniać odpowiednie procedury bezpieczeństwa (tylko zaufane i wiarygodne firmy, informatycy z certyfikatem, monitoring i rejestracja wszystkich czynności zwłaszcza tych związanych z oprogramowaniem)

Większość z podanych zagrożeń i metody ich przeciwdziałania uwzględniają systemy przyszłościowe, bezprzewodowe standardy otwarte (przerwa w transmisji bezprzewodowej powinna generować te same procedury co przerwanie kabla). Dopuszczenie systemu z bezprzewodową transmisją otwarta wymaga odniesienie i przeciwdziałanie wszystkim wymienionym w Rozdziale 2 zagrożeniom.

Wnioski

Aby potwierdzić bezpieczną transmisję bezprzewodową (również otwartą) w podobny sposób, należy poddać analizie inne systemy obecnie i w przyszłości eksploatowane w kolejnictwie polskim, a zwłaszcza systemy zamknięte z pełną autoryzacją dostępu:

- Istniejące systemy komunikacji „tor – pojazd" (SHP, KHP, SOP)

- Systemów przyszłościowe związane ze standardem ETRMS/ETCS wykorzystujące bezprzewodową transmisję do/od pojazdu.

W pracy pokazano, że właściwą ochronę przed zagrożeniami terrorystycznymi i hakerskimi może zapewnić odpowiednia wprowadzona polityka bezpieczeństwa, zarówno w systemach z instalacjami kablowymi jak tych z systemami bezprzewodowymi (również ze standardami otwartymi, gdzie tego typu ingerencje są bardziej prawdopodobne).

Dodatkowo można przeprowadzić analizę teoretyczna w celu oszacowania wpływu zagrożeń na bezpieczeństwo transmisji uwzględniając przy tym modele analityczne zalecane w tym celu przez wspomniane normy CENELEC i UIC takie jak procesy Markowa, weryfikowane przez metody symulacyjne (MATLAB/SIMULINK).

Konieczne wydaje jednak się przeprowadzenie badań doświadczalnych z próbami włamania się do komputerów sterujących i poddanie systemowej analizie (statystycznej) uzyskanych wyników badań doświadczalnych (laboratoryjnych i eksploatacyjnych) przeprowadzone na obiektach udostępnionych przez Instytut Kolejnictwa w Warszawie oraz zainteresowane firmy automatyki kolejowej.

Tego typu praca pracy badawcza pokaże ilościowe i jakościowe wskaźniki odporności systemów zarządzania i sterowania ruchem w transporcie kolejowym na utratę łączności, przekłamania i możliwość błędnego sterowania. Wskaźniki te zostaną wypracowane zarówno drogą analityczną (modele systemów i ich weryfikacja), jak też na bazie wyników badan laboratoryjnych i eksploatacyjnych. ◄

Materiały źródłowe

[1] Lewiński A., „Nowoczesne systemy telematyki kolejowej", Wydawnictwo Politechniki Radomskiej, Radom, 2012, ISBN 978- 83- 7351-506-2

[2] Lewiński A., Perzyński T.: „Akceptowalny poziom ryzyka jako kryterium bezpieczeństwa w transporcie kolejowym", prace konferencji Wydziału Transportu Politechniki Radomskiej Logi-Trans 2007

[3] A. Lewiński, T. Perzyński, A. Toruń: „The Analysis of Open Transmission Standards in Railway Control and Management", materiały Międzynarodowej Konferencji TRANSPORT SYSTEMS TELEMATICS TST 2012, 10-13.10.2012, Communications in Computer and Information Science 329), Springer-Verlag Berlin Heidelberg 2012

[4] A. Lewiński, L. Bester:„The Analysis of Transmission Parameters in Railway Cross Level Protection Systems with Additional Warning of Car Drivers", materiały Międzynarodowej Konferencji TRANSPORT SYSTEMS TELEMATICS TST 2012, 10-13.10.2012, Communications in Computer and Information Science 329), Springer--Verlag Berlin Heidelberg 2012

[5] Lewiński A., Toruń A.:„The efficiency analysis of train monitoring system applying the Changeable Block Distance method", 23-26.10.2013, materiały Międzynarodowej Konferencji TRANSPORT SYSTEMS TELEMATICS TST2013, monografia, COMMUNICATIONS IN COMPUTER AND INFORMATION SIENCE (395), Springer-Verlag Berlin Heidelberg 2013

[6] Lewiński A., Łukasik Z., Perzyński T., Ukleja P:: „The Future Generation of Railway Control Systems For Regional Lines Including New Telematic Solutions". Archives of Transport Systems Telematics, volume 7, issue 3, 2014. (s. 13-17). ISSN 1899-8208

[7] Lewiński A., Łukasik Z., Toruń A.:„The application of public radio transmission standards in innovative railway automation systems". Journal of KONBiN 2(26) 2013, s. 123-136, ISSN 1895-8281

[8] Lewiński A., Perzyński T., Toruń A.: "Risk Analysis as a Basic Method of Safety Transmission System Certification". Communications In Computer and Information Science no. 239. Springer 2011.

[9] Grant MNiSW pt:„Wpływ nowych technologii informacyjnych na poprawę funkcjonalności i bezpieczeństwa ruchu pociągów" nr 4T12C00529. Politechnika Radomska 2006.

[10] 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.

[11] Norma PN-EN 50128:2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Oprogramowanie dla kolejowych systemów sterowania i zabezpieczenia.

[12] Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.

[13] Norma PN-EN 50159: 2010. Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania.

[14] Norma PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów. Porcedura analizy rodzajów i skutków uszkodzeń (FMEA).

[15] Norma PN-EN 61025:2007 Analiza drzewa niezdatności (FTA).

[16] Norma PN-EN 61078:2006 Techniki analizy niezawodności – Metoda schematów blokowych niezawodności oraz metody boolowskie.

[17] Norma PN-IEC 60300-3-9:1999 Analiza ryzyka w systemach technicznych.

[18] Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym – DG PKP KA nr KA2b-5400-01/98 z dnia 06.02.1998r.

[19] Instrukcja, konserwacji, przeglądów oraz napraw bieżących urządzeń sterowania ruchem kolejowym le-12 (E-24) PKP PLK S.A. Warszawa, 2005r.

[20] Instrukcja WTB-E10 – Wytyczne techniczne budowy urządzeń sterowania ruchem kolejowym w przedsiębiorstwie PKP stanowiące załącznik do zarządzenia nr 43 Zarządu PKP z dnia 09.09.1996r z późniejszymi zmianami.

[21] KOMBUD S.A. – materiały Zakładu Automatyki KOMBUD S.A. w Radomiu

[22] KONTRON S.A. – materiały Kontron East Europe sp. z o.o

[23] SIMIS-W. Sterowanie Ruchem Kolejowym, materiały seminaryjne firmy Siemens Technika Transportowa, Zakopane 2000.