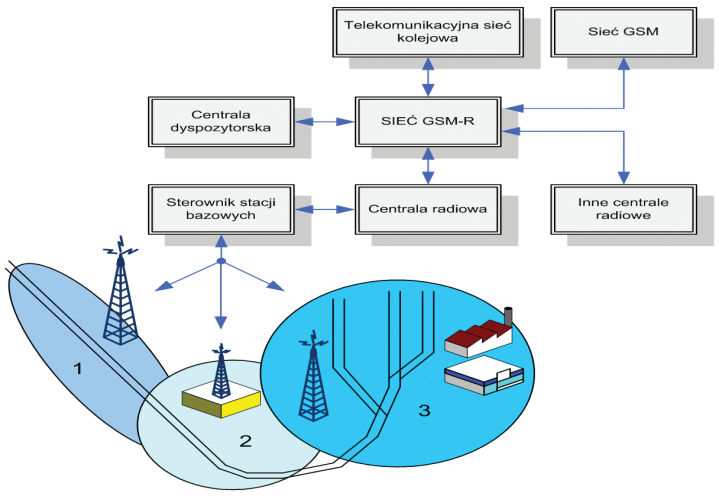
Andrzej Lewiński

Obecne i przyszłościowe systemy sterowania ruchem kolejowym

Znaczącym krokiem w rozwoju urządzeń zabezpieczenia ruchu pociągów było zastosowanie urządzeń elektrycznych (przekaźnikowych), których konstruowanie i wdrażanie rozpoczęto już w latach 40. XX w. Poprzedzone ono było fazą wdrożenia urządzeń hybrydowych (mechaniczno-elektrycznych), tj. urządzeń suwakowych z sygnalizacją świetlną [1, 5]. Współczesne systemy sterowania ruchem kolejowym w transporcie są systemami komputerowymi, komunikującymi się za pomocą standardów kablowych i bezprzewodowych.

Dobrym tego przykładem jest system ERTMS (ang. *European Rail Traffic Management System*), łączący w sobie dotychczasowe systemy sterowania nadrzędnego i scentralizowanego sterowania zależnościowego oraz systemy automatycznego prowadzenia pociągu (ATP/ATC) z wymaganiami interoperacyjności, realizowanymi między innymi przez bezprzewodowe struktury GSM-R (ang. *Global System for Mobile Communications - Railways*). Kolejowy człon sieciowy stacji GSM-R (rys. 1.) ma dodatkową bazę danych, związaną z adresowaniem funkcyjnym, oraz bardziej rozbudowane bazy połączeń grupowych i efektywne algorytmy zestawiania połączeń wysokopriorytetowych z czasami poniżej 1s. Połączenia między kolejowymi centralami radiowymi realizowane są poprzez kolejową sieć teletransmisyjną. W przypadku wykorzystania w procesie sterowania standardu GSM-R do sterowania ruchem kolejowym istnieje możliwość zestawienia dwóch kanałów transmisji (kanał rozmowy i kanał transmisji danych), co ma istotny wpływ na bezpieczeństwo transmisji. Na rysunku 1 przedstawiono również trzy typy komórek pokrycia przestrzennego przez system GSM-R:obsługujące tylko linie kolejowe (1), obsługujące linie kolejowe i tereny stacyjne (2), obsługujące inne tereny kolejowe (3).



Rys. 1. Typowa struktura GSM-R

Sieć radiowa składa się z radiowych kolejowych obszarów komórkowych. Rozproszone systemy kolejowe pracują w oparciu o standardy sieciowe, takie jak: WAN (Profibus) czy LAN (Ethernet, RS232). Profibus (*Process Field Bus*) jest siecią przeznaczoną do wykorzystania w rozproszonych systemach sterowania oraz nadzoru, jak również siecią odporną na zakłócenia, pracującą w standardzie EN 50170. Sieci komputerowe stosowane w systemach srk realizowane są jako :zamknięte lub otwarte, a sposób transmisji w obu przypadkach regulują odpowiednie normy PN-EN 50159: 2010 [10].

Systemy stosowane w transporcie kolejowym należą do grupy nowoczesnych wielokomputerowych systemów rozproszonych opartych na technologiach sieciowych i mających związek z decentralizacją sterowania. 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.

Kolejnym etapem jest wprowadzenie do systemów sterowania ruchem kolejowym systemów z transmisja otwartą, opartą na sieciach publicznych, przeważnie bezprzewodowych. Istotnym problemem jest w tych rozwiązaniach zapewnienia odpowiedniego bezpieczeństwa transmisji.

Bezpieczeństwo systemów srk – dawniej i obecnie

Bezpieczeństwo systemów przekaźnikowych

Przekaźnikowe systemy srk projektowane były jako systemy bezpieczne oparte na regule *fail-safe* – żadne pojedyncze uszkodzenie nie może prowadzić do błędnego wysterowania urządzeń zewnętrznych (sygnalizatora, zwrotnicy). Oznacza to, iż w przypadku przekaźnikowych urządzeń srk pojedyncze uszkodzenie musi wymuszać zmianę stanu systemu na taki, który zdefiniowany jest jako stan bezpieczny (np. uniemożliwienie wyświetlenia sygnału zezwalającego, wykluczenie możliwości nastawienia przebiegu, przestawienia zwrotnicy, ….). Osiągnięcie stanu bezpiecznego powoduje określone ograniczenia w dostępności systemu do sterowania, lecz nie powoduje sytuacji zagrożenia w ruchu kolejowym. Podstawowo bezpieczeństwo obwodów elektrycznych osiągane jest przez:

- zastosowanie odpowiednich elementów konstrukcyjnych obwodów, tj. przekaźniki zabezpieczeniowe określonej klasy, transformatory, przekładniki prądowe, dławiki, bezpieczniki,.
- odpowiednie ukształtowanie obwodu elektrycznego, zgodnie z opracowanymi przez uprawnione jednostki kolejowe albumy typowych układów dla poszczególnych systemów zabezpieczenia ruchu kolejowego.

Ze względu na sposób projektowania i montażu przekaźnikowe urządzenia sterowania ruchem kolejowym sklasyfikowane zostały na dwie podstawowe grupy:

- urządzenia projektowane indywidualnie (np. stacyjne typu E), dla których wykorzystywane były zasady projektowania oparte o albumy schematów typowych, a zasady bezpiecznego prowadzenia ruchu zdefiniowane były w zależności od układu torowego i charakterystyki ruchowej obiektu (stacji) w postaci tablicy zależności lub kart przebiegów (rys. 2) [5], [13],
- urządzenia geograficzne – zblokowane (budowane w strukturze modułowej, tj. JZH 111, CBP83, SUP-3, SUP-3M) definiowane jako graf powiązania typowych modułów funkcjonalnych (rys.3) [6], [12].

W pierwszym przypadku połączenia poszczególnych obwodów systemu typu E stanowią odwzorowanie układu torowego stacji i są one montowane bezpośrednio w terenie (na stacji), dla każdego zdefiniowanego przebiegu w sposób indywidualny. Praktycznie w systemie typu E wyróżniamy cztery podstawowe typy obwodów elektrycznych: nastawcze, sygnałowe, obwody utwierdzenia i zwolnienia przebiegów, obwody świateł. Układ torowy stacji wraz z przykładowymi zapisami zależności są przedstawione w tablicy zależności. Do zapewnienia bezpieczeństwa prowadzenia ruchu na posterunku dodatkowo oprócz kontroli stanu elementów dróg przebiegów, system na podstawie indywidualnie projektowanej dla każdego posterunku tablicy zależności wyklucza przebiegi sprzeczne oraz kontroluje warunki bezpiecznego nastawiania i zwalniania dróg przebiegów.

Drugi rodzaj to system przekaźnikowych urządzeń zblokowanych JZH 111, wyróżnia się w swojej budowie zastosowaniem określonych bloków przekaźnikowych (powtarzalnych) odpowiadających za obsługę i sterowania jednego określonego typu urządzenia na stacji (zwrotnicy, sygnalizatora, …) wykonanych w formie zamkniętego uniwersalnego i powtarzalnego, wieloprzekaźnikowego modułu, montowanego w fabryce.

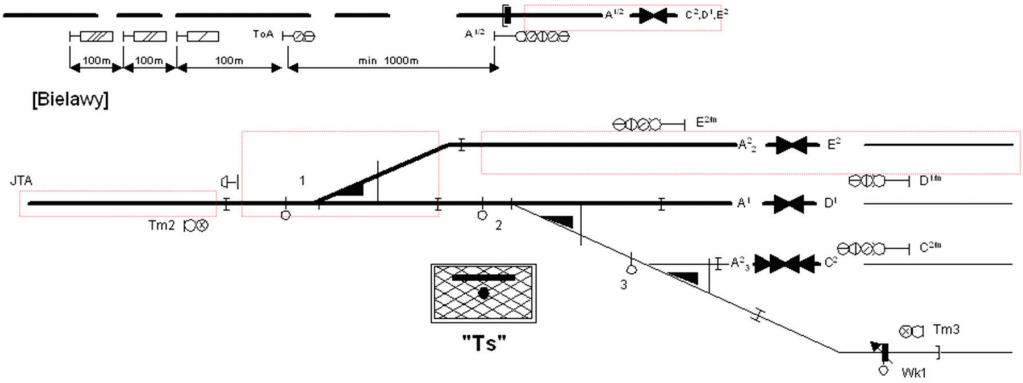
Poszczególne moduły łączone są między sobą odpowiednimi ścieżkami logicznymi. Przykładowe ścieżki logiczne, to: wybierania elementów drogi przebiegu, kontroli dostępu do modułu, poszukiwania ochrony bocznej, nastawiania elementów drogi przebiegu, utwierdzania modułów, kontroli prędkości (obrazu sygnałowego), przekaźników sygnałowych, automatycznego zwalniania przebiegu, doraźnego zwalniania przebiegu.

W systemach przekaźnikowych obowiązująca zasada *fail-safe* jako nadrzędne wymaganie bezpieczeństwa sprowadzała się do wykrycia usterki krytycznej i bezpiecznej reakcji systemu na wykrytą usterkę. W praktyce zdefiniowano zarówno zasady bezpiecznego projektowania, jak i sklasyfikowano usterki w zależności od ich wpływu na bezpieczeństwo działania systemów:

- usterki niekrytyczne (bezpieczne), które powodują ograniczenie funkcjonalności systemu, powodując zakłócenia w ruchu pociągów, ale bez możliwości spowodowania kolizji;
- usterki krytyczne (niebezpieczne), które wprowadzają bezpośrednie zagrożenie bezpieczeństwa i mogą prowadzić do powstania sytuacji niebezpiecznej – kolizji.

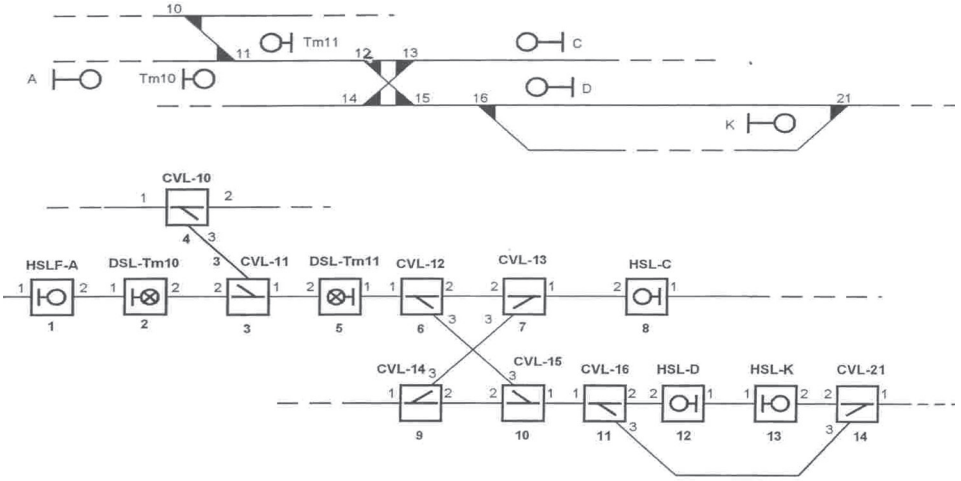
W praktyce realizacja zasady *fail-safe* opiera się, jak to było powiedziane wcześniej, na stosowaniu odpowiednich elementów – przekaźników klasy I (N), gdzie wykorzystuje się ich właściwości asymetryczności uszkodzeń polegającą na przyjęciu założenia iż jako prawdopodobnie przyjmujemy zdarzenie niewzbudzenia się przekaźnika (przy zamknięciu obwodu wzbudzenia) na skutek np. przerwy w obwodzie cewki przekaźnika, oraz jako nieprawdopodobne ze względów konstrukcyjnych wystąpienie przypadku pozostania przekaźnika w stanie wzbudzonym po zaniku zasilania uzwojenia cewki tego przekaźnika. A w przypadku przekaźników klasy II (C), jako prawdopodobne przyjmuje się wystąpienie obu opisanych zjawisk (uszkodzeń, np. pozostanie w stanie wzbudzonym na skutek sklejenia styków).

W praktyce na stacjach eksploatowanych przez PKP PLK S.A. spotkać można wiele systemów przekaźnikowych srk zarówno wykonanych w technice przebiegowej (urządzenia typu E, PB), jak



Lp	Przebieg	Opis przebiegu	Przebiegi pociągowe	Przebiegi manewrowe	Zwrotnice i wykolejnice	Odcinki izolowane	
						Torowe	Zwrotnicowe
1	A^2_3	Zest. Bielawy na tor 3	– + +	+ + +	+ – +	A,3	1,2,$\frac{3}{11}$
2	A^1_1	Zest. Bielawy na tor 1	+ – +	+ + +	+ + $\frac{3}{11}$ $\frac{10}{11}$	A,1	1,2
3	A^2_2	Zest. Bielawy na tor 2	+ + –	+ + +	– $\frac{3}{11}$ $\frac{10}{11}$	A,2	1

Rys. 2. Przykładowy układ torowy stacji wraz z tablicą zależności



Rys. 3. Przykładowy sposób powiązania modułów systemu JZH 111

i zblokowanej (IZH 111, SUP-3, OSA-H, …), które coraz częściej dostosowywane są do współpracy z komputerowymi pulpitami nastawczymi oraz podlegają centralizacji sterowania w ramach budowy lokalnych centr sterowania. Świadczy to o tym, że urządzenia te spełniają zakładane funkcje ruchowe, ponadto jak wykazały to doświadczenia ponad 50 lat eksploatowania urządzeń przekaźnikowych na sieci PKP, charakteryzują się one dużą trwałością i niezawodnością oraz gwarantują wymagany poziom bezpieczeństwa technicznego (pod warunkiem zachowania zasad ich utrzymania i eksploatacji, co staje się ze względu na upływ czasu coraz trudniejsze), zapewnienie właściwych elementów niezbędnych do ich bezpiecznej eksploatacji (tj. przekaźniki, których produkcja jest kosztowna ze względu na konieczność utrzymywania drogiej technologii oraz spadające zapotrzebowanie na rynku).

W przypadku systemów E okazało się, że ze względu na sposób projektowania obwodów (indywidualnie dla każdego obiektu), pomimo braku ograniczeń formalnych co do wielkości stacji (liczba zwrotnic, przebiegów, sygnałów) w praktyce okazało się, że system ten najlepiej sprawdza się w przypadku stacji małej i średniej wielkości, ponieważ dla dużych stacji kłopotliwe jest odpowiednie zaprojektowanie obwodów tak, aby możliwe było osiągnięcie optymalnych wskaźników eksploatacyjno – ruchowych dla stacji (głównie w przypadku definiowania wykluczeń przebiegów sprzecznych).

Bezpieczeństwo systemów komputerowych

Komputerowe systemy srk również opierały się o zasadę *fail-safe*. Ponieważ uszkodzenie komputerów (0→1, 1→0) były jednakowo prawdopodobne, bezpieczne konfiguracje opierały się na redundancji (układy 2z2, 2z3).

W związku z wejściem Polski do struktur unijnych obowiązujące stały się normy oznaczone odpowiednio: PN-EN 50126 [7], PN-EN 50128 [8] oraz PN-EN 50129 [9].

W normie PN-EN 50126 określono niezawodność, gotowość, dostępność i bezpieczeństwo (RAMS – ang. *Reliability, Availability, Maintainability and Safety*), jako proces oparty o cykl życia systemu (ang. *system life-cycle*). W procesie tym zdefiniowano poszczególne etapy systemu i procedury związane z zatwierdzaniem przed przejściem do następnego etapu. (specyfikacja wymagań, projekt., implementacja, itp.). Norma PN-EN 50128 określa procedury i wymagania techniczne do projektowania oprogramowania bezpiecznego systemu elektronicznego sterowania i zabezpieczenia na kolei [8, 9]. Należy stwierdzić, że norma ta nie jest w pełni obligatoryjna. Norma PN-EN 50129 definiuje wymagania dotyczące projektowania, testowania, odbioru i zatwierdzania elektronicznych systemów, podsystemów i urządzeń sygnalizacji związanych z bezpieczeństwem w zastosowaniach kolejowych.

Koncepcja bezpiecznych systemów komputerowych stosowanych w kolejnictwie zakłada bardzo małą intensywność usterek, co przy całkowitej niezależności kanałów przetwarzania (2 lub 3) gwarantuje znikome prawdopodobieństwo wystąpienia usterki podwójnej lub wielokrotnej – decydującej o uszkodzeniu katastroficznym (krytycznym). Podstawą analizy jest akceptowalny, dopuszczalny poziom ryzyka. W tabeli 2 przedstawiono europejskie wymagania dotyczące intensywności usterek zawarte w normie EN 50193.

Zgodnie z normą [9] bezpieczeństwo systemu zależy nie tylko od intensywności uszkodzeń, ale od czasu detekcji uszkodzeń pojedynczych i podwójnych (wielokrotnych). W tym celu wprowadzono współczynnik tolerowalnego poziomu uszkodzeń (*THR - Tolerable Hazard Rate*). Współczynnik ten można obliczyć z zależności:

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

gdzie:

λ_i – intensywność uszkodzeń dla kanału *i*,

$t_{d_i}^{-1}$ – czas reakcji systemu na błąd od czasu powstania dla kanału *i*.

Uwzględniając takie parametry jak: czas reakcji systemu na błąd od czasu wykrycia, czas reakcji systemu na błąd od czasu powstania, czas cyklicznego testowania elementu systemu, średnie czasy T_{MBF} składowych systemu, można wyznaczyć współczynnik *THR*. Dopuszczalne wartości współczynnika *THR* dla poziomów bezpieczeństwa SIL przedstawiono w tabeli 1 [9].

Tabela 1

Dopuszczalne wartości *THR* [10]

THR [na godzinę na funkcję]	SIL (*Safety Integrity Level*)
$10^{-9} \le THR < 10^{-8}$	4
$10^{-8} \le THR < 10^{-7}$	3
$10^{-7} \le THR < 10^{-6}$	2
$10^{-6} \le THR < 10^{-5}$	1

Z bezpieczeństwem systemów srk zakwalifikowanych do poziomu SIL-4 wiąże się również czas diagnostyki usterek pojedynczych:

$$T_{sf} = \frac{k}{1000\,\lambda} \qquad (2)$$

oraz usterek podwójnych:

$$T_{sf} = \frac{2}{\lambda} \qquad (3)$$

gdzie:

k – współczynnik nadmiarowości równy 1 dla systemów „2z2" i 0,5 dla systemów „2z3",

λ – suma średnich intensywności uszkodzeń elementów, których jednoczesne uszkodzenie może prowadzić do zagrożenia.

Dla systemów z cyklicznym testowaniem czas t_d jest równy:

$$t_d = \frac{T}{2} + NT \qquad (4)$$

gdzie:

T – czas cyklu testowania,

NT – czas reakcji (ang. *negation time*).

Gdyby architektura systemu była oparta tylko na jednym kanale przetwarzania informacji, to na podstawie wzoru (1) wartość *THR* byłaby równa λ, czyli średniej, wypadkowej intensywności usterek w systemie. Dlatego też z tego powodu stosuje się systemy nadmiarowe (ang. *redundant systems*), gdzie poprzez bezpośrednie porównanie informacji w równoległych kanałach przetwarzania (najczęściej 2 lub 3) wartość *THR* spełnia wymagania podane w tabeli 1.

Współczesne komputerowe systemy sterowania i ich bezpieczeństwo

Systemy nadrzędne

System nadrzędny jest zbiorem odpowiednio skonfigurowanych i oprogramowanych urządzeń wspomagających pracę dyspozytora i realizujących funkcje niezbędne do właściwej kontroli dyspozytorskiej, przy jednoczesnym spełnieniu wszystkich wymagań formalnych i technicznych stawianych tego typu systemom. Oprócz funkcji śledzenia i kierowania ruchem, system ten także wykrywa konflikty, a w razie potrzeby dokonuje korekcji ruchu.

Dobrym przykładem współczesnego systemu nadrzędnego jest ILTOR-2 (produkcji firmy KONTRON [17]). Jest to system nadrzędny, bezpośrednio pracujący z systemami nastawnic elektronicznych różnych producentów dopuszczonymi do eksploatacji na sieci PKP PLK S.A., tj SIMIS – W, MOR-3, WT UZ, WT UZm, oraz z dowolnym typem urządzeń elektrycznych przekaźnikowych po zastosowaniu odpowiedniego interfejsu powiązania. System ILTOR-2 jest wielofunkcyjnym systemem komputerowym stworzonym do kompleksowego sterowania i nadzorowania ruchem kolejowym na odcinkach obejmujących wiele posterunków ruchu. ILTOR-2 działa w czasie rzeczywistym. W celu zwiększenia niezawodności zastosowano konfigurację sprzętową i oprogramowanie pozwalające na zapewnienie dostępności systemu w przypadku uszkodzenia niektórych komputerów. ILTOR-2 jest komputerowym systemem rozproszonym o budowie modułowej. Większość modułów systemu ILTOR-2 może pracować samodzielnie. W system ILTOR-2 wchodzą następujące podsystemy: ILTOR–ZS (zdalne i miejscowe sterowanie ruchem kolejowym), ILTOR–KR (kierowanie ruchem), ILTOR–DIAG (system diagnostyczny). Na rysunku 4 przedstawiono strukturę warstwową systemu ILTOR – 2. składającą się z trzech warstw: Centrum Kierowania Ruchem (CKR), Lokalne Centrum Sterowania (LCS), Obiekty Sterowane (OS).

W warunkach kolei polskich eksploatowanych jest wiele systemów nadrzędnych klasy ksr (kierowanie i sterowanie ruchem) różnych dostawców. Wymienić tu należy między innymi system EBI Screen 3.0, EBI Screen 300, WSKR (produkcji Bombardier ZWUS z Katowic), czy MOR-2zs, MOR-2Icsr (produkcji Z.A. KOMBUD z Radomia).

Systemy scentralizowane

Systemy scentralizowane stanowią *n*-kanałową (przeważnie 2 lub 3) strukturę wielomodułową o odpowiednio dobranej konfiguracji, realizującą w czasie rzeczywistym funkcję nastawiania przebiegów zgodnie z obowiązującymi wymaganiami bezpieczeństwa. Bezpieczeństwo takich systemów zapewnia odpowiednio dobrana technologia, w tym odpowiednia struktura oprogramowania, realizująca zasadę *fail-safe*. Ze względów bezpieczeństwa stosuje się konfigurację sprzętową umożliwiającą porównywanie wyników, najczęściej „2z2". Odpowiedni poziom bezpieczeństwa można uzyskać przez zastosowanie jednego komputera głównego i tzw. gorącej rezerwy, wprowadzając odpowiednie oprogramowanie (przetwarzanie dwóch różnych programów napisanych przez różne zespoły) [9]. Systemy scentralizowane należą do grupy urządzeń stacyjnych. Na rysunku 5 przedstawiono system SIMIS [6, 7]

Systemy liniowe

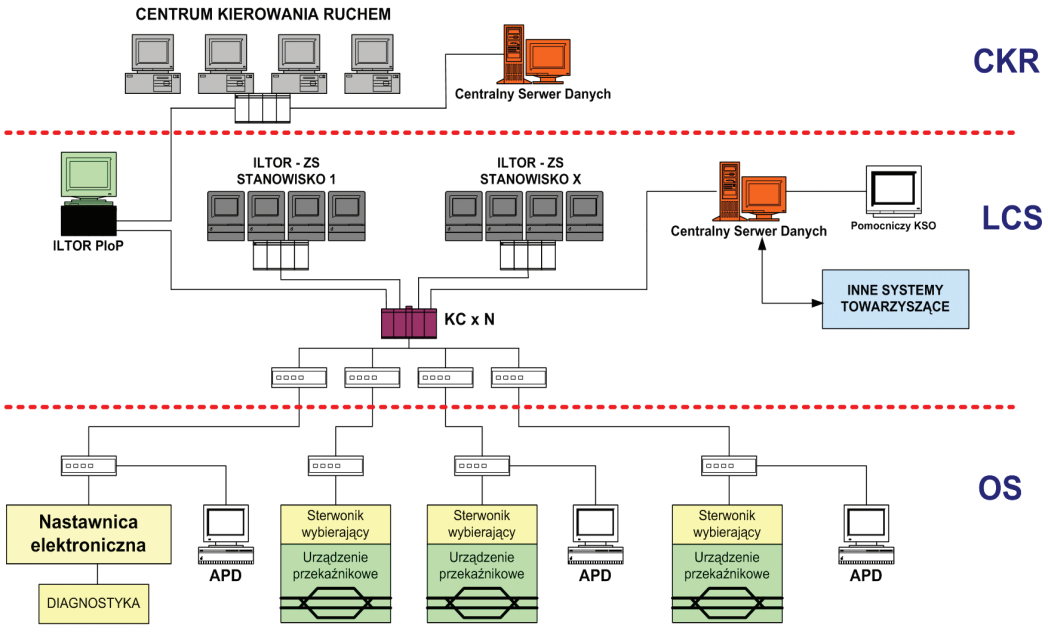
Systemy pracujące na szlakach kolejowych, których zadaniem jest regulacja ruchu pociągów między posterunkami nazywa się systemami liniowymi [1].

Przykładem takiego systemu jest samoczynna sygnalizacja przejazdowa typu RASP-4F służąca do zabezpieczenia przejazdów kategorii „B" i „C" oraz dodatkowo przejazdów kategorii „A". Sygnalizacja przejazdowa typu RASP-4F może być stosowana na liniach kolejowych, na których maksymalna prędkość pociągów nie przekracza 160 km/h. Do wykrywania zajętości toru zastosowano nowoczesny układ liczników osi pociągu, oparty na indukcyjnych czujnikach koła typu RSR-180 (firma Frauscher). W skład systemu wchodzą między innymi: kontener główny (RASP-KG), szafy aparatowe (RASP-SA1, RASP-SA2) oraz urządzenie zdalnej kontroli (RASP-UZK).

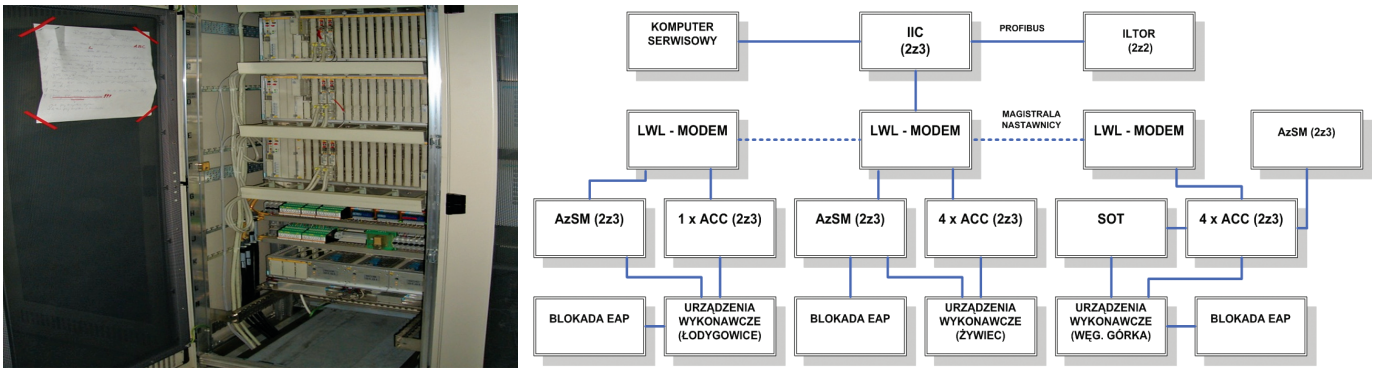
Samoczynna sygnalizacja przejazdowa RASP-4F jest typem urządzenia, w którym zastosowano rozwiązanie „2z2". W celu spełnienia wymagań bezpieczeństwa systemu RASP-4 zastosowano redundancję: urządzeń kontrolno-sterujących wraz z funkcją samotestowania, urządzeń wykonawczych wraz z funkcją samotestowania i urządzeń zasilających. System RASP-4F może współpracować z różnymi stacyjnymi urządzeniami srk [21]. Schemat współpracy układów sterowania samoczynnej sygnalizacji przejazdowej RASP-4 przedstawiono na rysunku 6.

Inne systemy srk

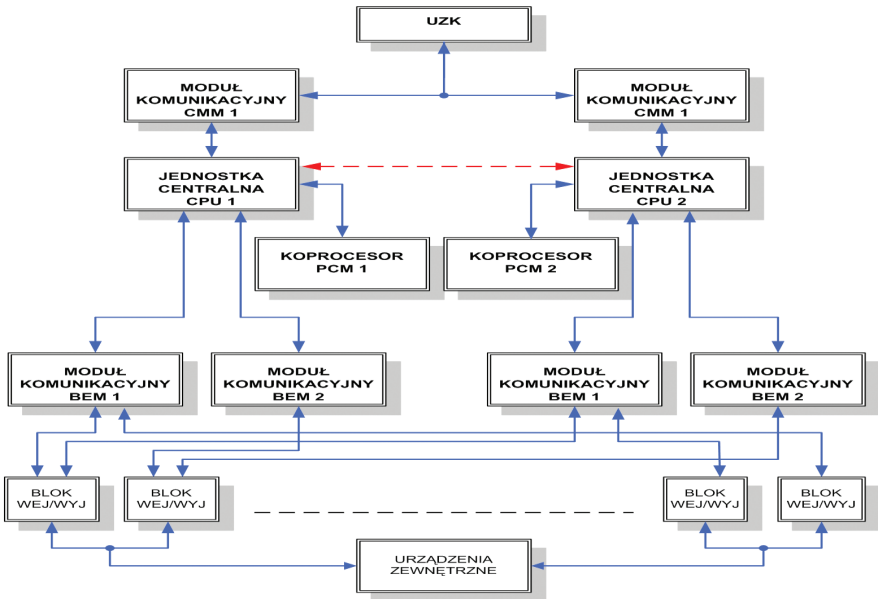
- **Systemy zdalnego sterowania**. Systemy te zaliczone do poziomu bezpieczeństwa SIL2 umożliwiają sterowanie z jednego punktu wszystkimi urządzeniami na stacjach objętych zdalnym



Rys. 4. Struktura warstwowa systemu ILTOR-2



Rys. 5. System SIMIS, konfiguracja 2z3



Rys. 6. Schemat współpracy układów sterowania samoczynnej sygnalizacji przejazdowej RASP-4

sterowaniem. Realizowane jest to przy użyciu specjalnych urządzeń zainstalowanych na stacjach i urządzeń w centrum sterowania. Urządzenia te zapewniają pełne zobrazowanie sytuacji ruchowej na obszarze objętym zdalnym sterowaniem oraz możliwości sterowania z centrum urządzeniami znajdującymi się na tym obszarze, realizowane są przeważnie w konfiguracji nadmiarowej, dwukanałowej.

Przykładem systemu zdalnego sterowania jest system sterownia zainstalowany w warszawskim metrze. W skład centrum wchodzą trzy podstawowe stanowiska dyspozytorskie, które kontrolują ruch pociągów oraz zarządzają innymi urządzeniami (energetycznymi, sanitarnymi, czy mechanicznymi). Centrum dyspozytorskie zbiera informacje z nadzorowanych urządzeń oraz dokonuje ich analizy. Z centrum sterowania zainstalowanego na stacji Politechnika następuje zdalne sterowanie na całej linii metra. Podczas przejazdu pociągu, nadaje on swój numer bezprzewodowo do odbiorników zainstalowanych na stropie tunelu w określonych miejscach, który jest przekazywany do centrum sterowania. Jako medium transmisji informacji wykorzystuje się sygnał podczerwieni [1]. Prowadzenie pociągów oraz bezpieczeństwo pasażerów podlega dyspozytorowi ruchu. Dyspozytor ten ma do dyspozycji między innymi: komputerowy system monitorowania ruchu pociągów, system TV przemysłowej, system łączności przewodowej i bezprzewodowej.

■ **Systemy ATP/ATC**. Systemy te zaliczane do poziomu SIL2 monitorują i kontrulują przemieszczanie się pociągu na szlaku. Jednym z urządzeń wspomagających bezpieczne prowadzenie pociągu jest system SOP-2, będący systemem ATP (ang. *Automatic Train Protection,* polska nazwa AOP – automatyczne ograniczanie prędkości). System ten został zainstalowany w metrze warszawskim dla zapewnienia bezpiecznego prowadzenia pociągów. W systemie tym wysoki poziom bezpieczeństwa uzyskano przez dwukanałowe, niezależne przetwarzanie informacji z bezpieczną komparacją i kontrolą sygnałów w obu kanałach (komparator *fail-safe*). Podstawowym zadaniem systemu jest automatyczne ograniczanie prędkości pociągu. Urządzenia nadawcze w sposób ciągły transmitują do pojazdu informacje o sytuacji ruchowej i wynikającej z niej prędkości dopuszczalnej. Przy przekroczeniu prędkości dopuszczalnej, układ napędowo-hamujący pojazdu powoduje automatyczne ograniczenie prędkości do takiej, która zapewnia dalszą bezpieczną jazdę lub zatrzymanie pojazdu przed przeszkodą, sygnalizowaną przez urządzenia srp. Transmisja z toru do pojazdu odbywa się za pośrednictwem obwodów przewodowych ułożonych między szynami. System może współpracować z dowolnymi urządzeniami srk.

■ **Kolejowe systemy informacyjne**. Warto w tym miejscu także wspomnieć o komputerowych systemach zobrazowania, ułatwiających w znacznym stopniu podgląd sytuacji ruchowej na monitorach. Przykładem takiego systemu jest MOR-1, odpowiedzialny

za monitorowe odwzorowanie obszaru sterowanego, zaliczany do poziomu SIL2. System ten może współpracować z dowolnymi przekaźnikowymi i komputerowymi urządzeniami zależnościowymi. Transmisja jest realizowana poprzez siec Ethernet. Stanowisko obsługi stanowi typowa konfiguracja – komputer klasy IPC, monitor, mysz i klawiatura. Sterownik stacyjny stanowi jeden komputer. Sterownik poleceń składa się z dwóch sterowników pracujących w konfiguracji „2z2".

Komputerowym systemem należącym do poziomu bezpieczeństwa SIL0 jest System Centralnej Rezerwacji Miejsc i Sprzedaży Biletów Krajowych i Zagranicznych – KURS 90. System składa się z komputera centralnego firmy TANDEM oraz kilkuset terminali kasowych pracujących w sieci X.25 (KOLPAK).

Bezpieczeństwo komputerowych systemów srk

Zgodnie z wymaganiami wymienionych norm dla systemów komputerowych obligatoryjne jest oszacowanie wartości współczynnika *THR*, który powinien mieścić się w wymaganym zakresie (tab. 1). W przypadku systemów aktualnie wdrażanych lub eksploatowanych od kilku lat mamy dwie możliwości takiej analizy.

Szacowanie *THR* na podstawie danych producenta

W systemie RASP 4F 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. W skład pojedynczego sterownika wchodzą (rys. 7):

- kaseta bazowa IC695CHS012,
- zasilacz prądu stałego IC695PSD140,
- jednostka centralna typu IC695CPU310,
- interfejs komunikacyjny IC695ETM001,
- moduł wejść dyskretnych IC694MDL660,
- moduł wyjść dyskretnych IC694MDL754.

Do zastosowanego sprzętu podano następujące wartości MTBF (średni czas między wystąpieniem uszkodzeń) na podstawie danych producenta/dystrybutora sprzętu (firma Astor Kraków):

a) kaseta bazowa IC695CHS012 – 761 000 [h],
b) zasilacz prądu stałego IC695PSD140 – 1 092 000 [h],
c) jednostka centralna IC695CPU310 – 638 000 [h],
d) interfejs komunikacyjny IC695ETM001 – 992 000 [h],
e) moduł wejść dyskretnych IC694MDL660 – 6 393 000 [h],
f) moduł wyjść dyskretnych IC694MDL754 – 553 000 [h].

Konfiguracja sterowników zawiera różną liczbę modułów, co przy założeniu najgorszego przypadku (szeregowa struktura niezawodnościowa) prowadzi do wypadkowej wartości MTBF dla poszczególnych zestawów:

- zestaw z 2 modułami e) i 1 modułem f) – 144 374.4267 [h],
- zestaw z 3 modułami e) i 1 modułem f) – 141 185.9945 [h],
- zestaw z 4 modułami e) i 1 modułem f) – 138 135.3490 [h],
- zestaw z 6 modułami e) i 2 modułami f) – 106 832.6186 [h].

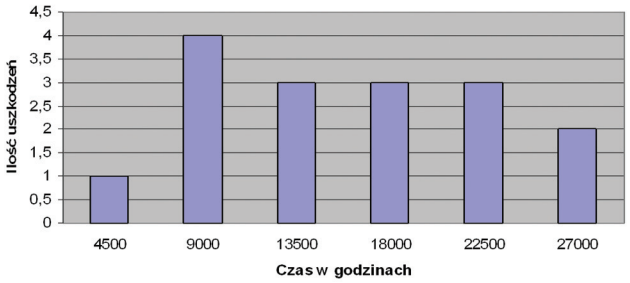
Zapewniono dostatecznie krótki czas wykrywania pojedynczego uszkodzenia i przejście do stanu bezpiecznego (czas ten, t_{sf}, jest znacznie krótszy niż oczekiwany średni czas między uszkodzeniami obu komputerów). Zgodnie z normą PN-EN 50129 czas wykrywania pojedynczego uszkodzenia spełniający warunek $t_{sf} \leq k/(1000 \cdot a)$, gdzie $k = 1{,}0$ dla systemów „2z2", a – 1/MTBF. Do obliczeń współczynnika *THR* przyjęto następujące wartości czasu:

- cyklicznego testowania wejść/wyjść (T) 250 ms,
- reakcji na błąd (NT) 1 s,

co daje wartość czasu reakcji na błąd (SDT) równą 0,0003125 [h] i w efekcie wartość *THR* równą 2,19e–13, zgodnie z normą PN-EN 50129 dla poziomu SIL4. Obliczony czas wykrycia bledów pojedynczych (TSF) spełnia kryterium wynikające z granicznej wartości odniesionej do oszacowanej wartości MTBF dla systemu „2z2" podane w normie PN-EN 50129.

Szacowanie *THR* na podstawie danych eksploatacyjnych

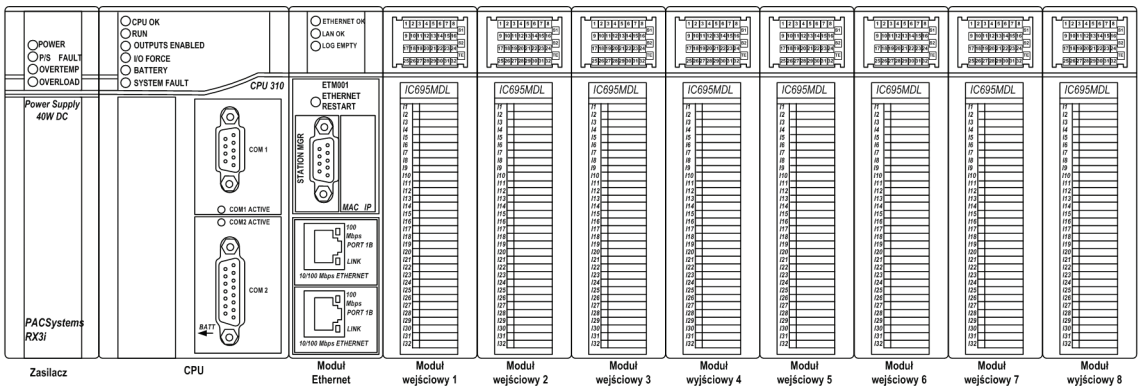
Systemy RASP-4 są eksploatowane od wielu lat. Na podstawie danych eksploatacyjnych możliwe było oszacowanie wartości intensywności uszkodzeń. Na rysunku 8 przedstawiono wykaz uszkodzeń dla badanych systemów w założonym przedziale czasu 27 000 h (każdy przedział po 4500 h). Razem zarejestrowano 16 usterek.



Rys. 8. Wykaz uszkodzeń w przedziale czasu

Oszacowana globalna wartość współczynnika uszkodzeń λ wyniosła:

$$\lambda = 7{,}40741 \cdot 10^{-5}\ h^{-1} \qquad (5)$$



Rys.7. Kaseta samoczynnej sygnalizacji przejazdowej RASP-4F

Do obliczenia współczynnika *THR* użyto danych z prognozowania. Korzystając z zależności (4), do obliczeń przyjęto następujące wartości:

- czas cyklicznego testowania wejść/wyjść $T = 500$ ms
- czas reakcji na błąd wejścia $NTwe = 1$ s
- czas reakcji na błąd wyjścia $NTwy = 1$ s

Ponieważ czasy dla kanału A i B są jednakowe:

$$t_{dA} = t_{dB} = \frac{500\text{ ms}}{2} + 1\text{ s} = 1{,}25\text{ s} \qquad (6)$$

stąd obliczony wskaźnik *THR* wyniósł $5{,}56 \cdot 10^{-12}$.

Systemy przyszłościowe i ich bezpieczeństwo

Nowe technologie informacyjne, wynikające z regulacji Unii Europejskiej, wymuszają na producentach systemów srk stosowanie innowacyjnych rozwiązań. Doskonałym przykładem może być transmisja bezprzewodowa wykorzystująca standardy publiczne, w tym Internet. Zasady stosowania transmisji otwartej w systemach srk reguluje norma PN-EN 50159 [I0].

Bezprzewodowa transmisja radiowa w systemach srk

W koncepcji systemu bezpiecznej transmisji, zaproponowanej przez firmę KOMBUD S.A. [15] (rys. 9), zastosowano kanał radiowy (otwarty system transmisji) do przekazywania informacji. 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).

System transmisji otwartej oparty jest na radiolinii zapewniający kontrolę autoryzacji dostępu. Do celów łączności wybrano radiomodemy Satellar firmy Satel. Transmisja odbywa się w kanale 433.725 MHz (odstęp sąsiedniokanałowy 25 kHz) z prędkością w kanale radiowym do 19 200 bit/s. Zastosowany sprzęt transmisyjny charakteryzuje się wysoką niezawodnością – MTBF około 525 600 h, co poświadcza odpowiedni certyfikat.

W koncepcji systemu ESTER (Ekonomiczny System zdalnego STERowania i kierowania ruchem kolejowym) przyjęto telegramy zgodne z typem transmisji B0 podanym w normie PN-EN 50 159 [10], 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 (ang. *Cyclic Redundancy Check*), które zabezpieczają przed przypadkowymi błędami, umożliwiając wykrycie pojedynczych lub seryjnych błędów.

Bezpieczeństwo systemów srk z transmisją radiową

Na rysunku 10 przedstawiono realizację bezpiecznej transmisji bezprzewodowej w sygnalizacji przejazdowej SZP, będącej podsystem wspomnianego projektu ESTER. Jest to podsystem 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 (lokalna sieć kontenerowa).

W przypadku analizy systemu o nieznanych charakterystykach niezawodnościowych elementów, możliwe jest wstępne oszacowanie wskaźników poprzez obliczenie wypadkowych intensywności uszkodzeń systemu na podstawie liczby i struktury niezawodnościowej zastosowanych elementów dyskretnych oraz scalonych o różnej skali integracji. Ogólna postać dla szacowania niezawodności eksploatacyjnej dyskretnych elementów półprzewodnikowych wynosi:

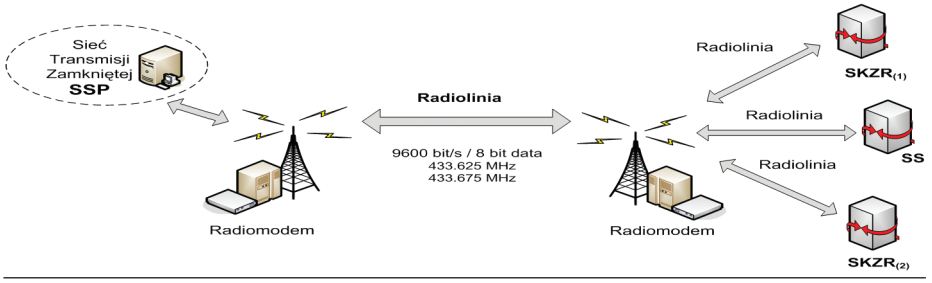
$$\lambda_p = \lambda_b(\pi_T \cdot \pi_A \cdot \pi_R \cdot \pi_S \cdot \pi_C \cdot \pi_Q \cdot \pi_E) \qquad (7)$$

gdzie:

- $\lambda_b = \lambda_0 \cdot \pi_{ST}$ – bazowa intensywność uszkodzeń, zależna od parametru λ_0 oraz obciążenia temperaturowego i elektrycznego π_{ST},
- λ_p – intensywność uszkodzeń podczas eksploatacji,
- π_E – współczynnik uwzględniający oddziaływanie czynników środowiskowych innych niż temperatura,
- π_A – współczynnik uwzględniający rodzaj aplikacji,
- π_S – współczynnik uwzględniający obciążenia napięciowe,
- π_T – współczynnik temperaturowy,
- π_R – współczynnik uwzględniający maksymalne dopuszczalne parametry elementu,
- π_Q – współczynnik jakościowy,
- π_C – współczynnik uwzględniający wpływ obecności kilku złącz w jednej obudowie lub konstrukję.

Na rysunku 11 przedstawiono uproszczony schemat systemu uwzględniającego transmisję bezprzewodową w nowo projektowanym systemie SSP. Na podstawie otrzymanej dokumentacji technicznej dokonano wstępnego studium analizy bezpieczeństwa w celu wyznaczenia wskaźnika intensywności uszkodzeń λ oraz wyznaczenia współczynnika *THR*. Wyniki z szacowania podano w tabeli 2:

Wynik z tabeli 2 (przy czasie t_d rzędu 1,25 s) daje wartość $THR = 1{,}1\ 10^{-10}\ h^{-1}$.



Rys. 9. Struktura systemu sterowania ruchem kolejowym z transmisją radiową

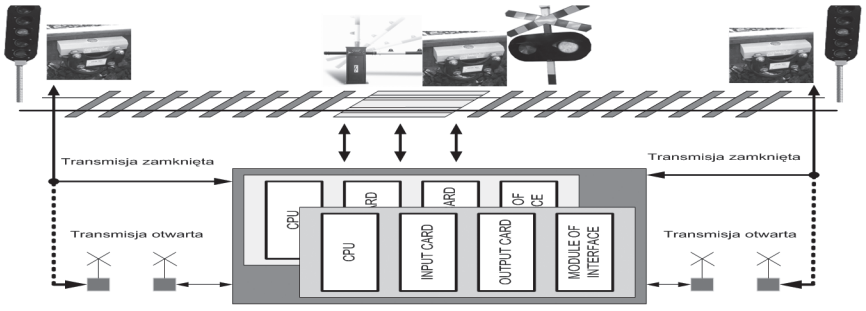
Podsumowanie

Systemy srk zawsze były projektowane jako systemy bezpieczne. Przedstawione rozwiązania systemów JZH i E oparte były na koncepcji bezpiecznego przekaźnika,

Tabela 2

Wartości intensywności usterek

Element	Wartość współczynnika λ
Sterownik czujników i tarcz	8,8E-05
Sterownik radiowy 1	4,09558E-05
Sterownik radiowy 2	1,50242E-05
Układ decyzyjny	2,54E-04
Razem	**3,98E-04**

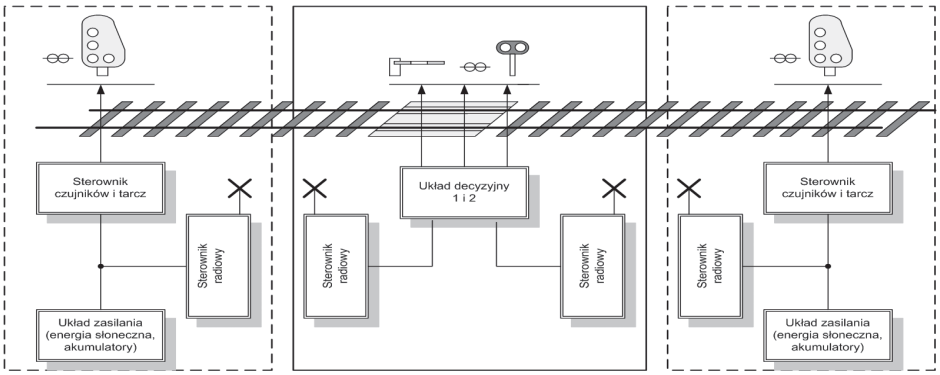


Rys. 10. System sterowania ruchem kolejowym z transmisją radiową otwartą (radiową)

którego najbardziej prawdopodobne uszkodzenie nie miało wpływu na bezpieczne wysterowanie urządzeń zewnętrznych. Omówione powszechnie stosowane systemy komputerowe oparte były na nadmiarowości i stosunkowo krótkim czasie wykrywania usterek. Wynikowym parametrem był *THR* (Tolerowalny Poziom Ryzyka), którego wartości były zdefiniowane w obowiązujących normach (PN EN 50 159).

Kolejnym krokiem było wprowadzenie otwartych standardów transmisji opartych na publicznych sieciach, głównie bezprzewodowych. Badania potwierdzają, że zastosowanie typowych standardów komunikacji opartych na bezprzewodowym dostępie do Internetu przy zastosowaniu odpowiednich procedur, a zwłaszcza metod kryptograficznych, pozwala zapewnić ten sam poziom bezpieczeństwa co w przypadku dotychczas stosowanych transmisji kablowych w rozproszonych systemach komputerowych. Generalnie począwszy od systemów przekaźnikowych po przyszłe realizacje oparte na transmisji otwartej stosowana jest ta sama zasada *fail-safe*: każde pojedyncze uszkodzenie nie może prowadzić do sytuacji niebezpiecznej. W systemach komputerowych wyznaczany jest dodatkowo czas detekcji usterki. W systemach opartych na sieciach publicznych dodatkowo analizuje się minimalizację czasu opóźnień (spowodowanych np. zanikiem lub przekłamaniem transmisji i związaną z tym koniecznością powtórzeń itp.) co pozwoliło zapewnić identyczny poziom funkcjonalności co w systemach realizowanych dotychczas, tych komputerowych, jak i przekaźnikowych.

❑



Rys. 11. Uproszczony schemat nowego systemu

Literatura

[1] Dąbrowa-Bajon M.: *Podstawy sterowania ruchem kolejowym*. Wydawnictwo Politechniki Warszawskiej 2002.

[2] Dyduch J., Kornaszewski M.: *Systemy sterowania ruchem kolejowym*. Wydawnictwo Politechniki Radomskiej, Radom 2003.

[3] Lewiński A.: *Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego*. Wydawnictwa Politechniki Radomskiej, seria monografie Nr 49, Radom, 2001.

[4] Lewiński A.: *Nowoczesne systemy telematyki kolejowej*. Radom, 2012.

[5] Lewiński A., Toruń A., Perzyński T.: *Tendencje rozwojowe systemów srk w ciągu ostatnich lat*. Problemy Kolejnictwa, zeszyt 153/2011.

[6] Miksza E.: *Zblokowany system sterowania ruchem kolejowym na stacjach typu IZH 111*. WKŁ, Warszawa 1979.

[7] Grant MNil *Wpływ nowych technologii informacyjnych na poprawę funkcjonalności i bezpieczeństwa ruchu pociągów*" nr 4T12C00529. Politechnika Radomska 2006.

[8] 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.*

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

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

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

[12] *Album schematów – zbiór przykładowych rozwiązań – geograficzny system stacyjnych przekaźnikowych urządzeń srk typu CBP83*. 1985 r.

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

[14] Siemens - materiały firmy Siemens

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

[16] Kontron – materiały Kontron East Europe sp. z o.o

Autor dziękuje dr. inż. Tomaszowi Perzyńskiemu z UTH w Radomiu i mgr. inż. Andrzejowi Toruniowi z IK za pomoc przy opracowaniu tego artykułu.

Andrzej Lewiński
a.lewinski@uthrad.radom.pl