Samoczynna sygnalizacja przejazdowa, urządzenia komputerowe, sterowanie, sterowanie ruchem kolejowym, bezpieczeństwo

DYDUCH Janusz[1]
KORNASZEWSKI Mieczysław[2]
PNIEWSKI Roman[3]

METODY ZAPEWNIANIA BEZPIECZEŃSTWA SAMOCZYNNYCH SYGNALIZACJI PRZEJAZDOWYCH

Współczesne systemy sterowania ruchem kolejowym są realizowane w postaci urządzeń komputerowych. Ze względu na specyfikę urządzeń srk, muszą one spełniać ostre wymagania dotyczące bezpieczeństwa i niezawodności. W artykule poruszono zagadnienia związane z bezpieczeństwem komputerowych systemów sterowania ruchem kolejowym na przykładzie systemów samoczynnej sygnalizacji przejazdowej.

METHODS OF ENSURING SAFETY OF AUTOMATIC OF THE LEVEL CROSSINGS

Existing systems of railway traffic control are implemented in computer equipment form. Due to the specificity of railway traffic control devices, they must meet stringent of safety and reliability requirements. The article presents issues related to safety of computer systems of railway traffic control what is shown on the example of automatic of systems of the level crossing.

1. WSTĘP

Urządzenia sterowania ruchem kolejowym (srk) służą do zapewnienia bezpieczeństwa przemieszczania pojazdów po sieci kolejowej i wymaganej sprawności w sposób uzasadniony technicznie i ekonomicznie. Niezależnie od technologii, w jakiej są wykonane (mechaniczne, elektromechaniczne, przekaźnikowe, hybrydowe, komputerowe) zawsze mają to samo przeznaczenie. Wymagania bezpieczeństwa na kolei, obwarowane konkretnymi przepisami, mogą być spełnione na drodze sprzętowej lub też w przypadku urządzeń komputerowych na drodze programowej. W systemach komputerowych zwiększenie bezpieczeństwa osiąga się w najprościej przez redundancję urządzeń i oprogramowania, ale również i innymi sposobami.

[1] Politechnika Radomska, Wydział Transportu i Elektrotechniki; 26-600 Radom; ul. Malczewskiego 29. *Tel: + 48 48 361-77-27, Fax: + 48 48 361-77-42, E-mail: j.dyduch@pr.radom.pl*
[2] Politechnika Radomska, Wydział Transportu i Elektrotechniki; 26-600 Radom; ul. Malczewskiego 29. Tel: + 48 48 361-77-28, Fax: + 48 48 361-77-42, E-mail: m.kornaszewski@pr.radom.pl
[3] Politechnika Radomska, Wydział Transportu i Elektrotechniki; 26-600 Radom; ul. Malczewskiego 29. Tel: + 48 48 361-77-28, Fax: + 48 48 361-77-42, E-mail: r.pniewski@pr.radom.pl

Szczególnie newralgicznymi miejscami na kolei są przejazdy kolejowe, czyli skrzyżowania w jednym poziomie drogi kolejowej z kołową, na których mogą wystąpić znaczne szkody materialne oraz często ofiary w ludziach. Jest to szczególnie istotnie z uwagi na wielkości charakteryzujące ruch pojazdów szynowych, takie jak: prędkość, ciężar, droga hamowania mają one pierwszeństwo przejazdu na przejeździe kolejowym przed pojazdami poruszającymi się po drogach kołowych.

Polskie ustawodawstwo dotyczące zabezpieczenia jednopoziomowych skrzyżowań linii kolejowych z drogami kołowymi opiera się na Rozporządzeniu Ministra Transportu i Gospodarki Morskiej w sprawie warunków technicznych, jakim powinny odpowiadać skrzyżowania linii kolejowych z drogami publicznymi i ich usytuowanie z dnia 26.02.1996r., które dopuszcza takie skrzyżowania na liniach kolejowych o max. prędkości pociągów do 160km/h i wyróżnia 6 kategorii skrzyżowań:

- kategoria A – przejazd użytku publicznego z rogatkami lub bez rogatek, na którym ruch na drodze kierowany jest sygnałami nadawanymi przez pracowników kolejowych, na liniach o max. prędkości do 160km/h,
- kategoria B – przejazd użytku publicznego z samoczynną sygnalizacją świetlną i z półrogatkami, na liniach o max. prędkości do 160km/h,
- kategoria C – przejazd użytku publicznego z samoczynną sygnalizacją świetlną lub uruchamiany przez pracowników kolei, na liniach o max. prędkości do 140km/h,
- kategoria D – przejazd użytku publicznego bez rogatek i półrogatek i bez samoczynnej sygnalizacji świetlnej, na liniach o max. prędkości do 120km/h,
- kategoria E – przejścia użytku publicznego,
- kategoria F – przejazdy i przejścia użytku niepublicznego.

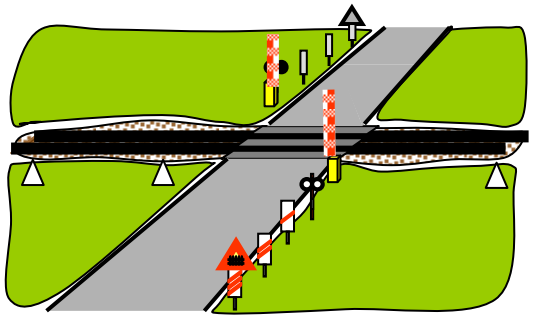
2. SAMOCZYNNA SYGNALIZACJA PRZEJAZDOWA

2.1 Idea funkcjonowania

Urządzenia samoczynnej sygnalizacji przejazdowej (ssp) służą do zabezpieczenia ruchu na skrzyżowaniach w jednym poziomie dróg kołowych z liniami kolejowymi. Urządzenia te uruchamiane są przez zbliżający się do przejazdu pociąg za pomocą czujników torowych (ewentualnie elektrycznych obwodów nakładanych). Na przejeździe zainstalowane są urządzenia ostrzegawcze, w skład których wchodzą: sygnalizatory drogowe świetlne (2÷4 szt.) uzupełnione sygnałem dźwiękowym oraz jedna lub dwie pary półrogatek. Uruchomienie sygnalizacji następuje na minimum 30 sekund przed wjechaniem czoła pociągu na przejazd, a wyłączenie po około 5 sekundach od momentu zjechania ostatniej osi z przejazdu kolejowego. W skład mikroprocesorowych samoczynnych sygnalizacji przejazdowych wchodzą następujące urządzenia:

- oddziaływania (wykrywające zbliżający się do przejazdu pociąg, np. czujniki torowe),
- sterująco-kontrolne (szafy aparatowo-zasilające ze sterownikami PLC),
- ostrzegawcze (sygnalizatory drogowe, dzwony, napędy rogatek, tarcze ostrzegawcze przejazdowe),
- pomocnicze dla celów wizualizacji działania urządzeń ssp,
- diagnostyczne (urządzenia zdalnej kontroli, przenośne panele diagnostyczne, a w wyjątkowych przypadkach moduły diagnostyczne).

W latach 90 XX wieku do powszechnego stosowania na kolejach polskich przyjęto trzy nowoczesne systemy samoczynnej sygnalizacji przejazdowej skonstruowane w oparciu o sterowniki mikroprocesorowe, z zastosowaniem rozbudowanych mechanizmów autokontroli, rejestracji zdarzeń i diagnostyki technicznej, umożliwiającej zdalne uzyskiwanie informacji o zdarzeniach oraz rodzajach usterek. Są to systemy wyprodukowane przez firmy: Bombardier ZWUS Katowice, Scheidt & Bachmann i Siemens, czy też nieco później Zakłady Automatyki KOMBUD S.A. z systemem RASP- 4.



Rys.1. Przykład rozmieszczenia urządzeń zabezpieczających w samoczynnej sygnalizacji przejazdowej (przejazd kolejowy kategorii B)

3. ROZWIĄZANIA SPRZĘTOWE I PROGRAMOWE ZABEZPIECZANIA SAMOCZYNNYCH SYGNALIZACJI PRZEJAZDOWYCH

Podstawową cechą bezpiecznych realizacji komputerowych systemów sterowania przyjętą w kolejnictwie jest zasada *„fail-safe”*, która mówi, że pojedyncze uszkodzenie (sprzętu, oprogramowania) lub zakłócenie nie może spowodować sytuacji niebezpiecznej, przy założeniu, że prawdopodobieństwo wystąpienia uszkodzenia podwójnego (wielokrotnego) jest pomijalnie małe. W celu zapewnienia bezpieczeństwa komputerowych systemów wymagane jest spełnienie przez systemy wymagań zawartych w normach: EN 50128 i EN 50129, EN 50159-1 lub EN 50159-2 (dla otwartych systemów transmisji). Wprowadzenie dowolnego systemu wymaga przeprowadzenia dowodu bezpieczeństwa. Zgodnie z normą dokumentacja dowodu bezpieczeństwa powinna zawierać:

- definicja systemu,
- raport zarządzania jakością (rozdz. 5.2 normy EN 50129),
- raport zarządzania bezpieczeństwem (rozdz. 5.3 normy EN 50129),
- raport bezpieczeństwa technicznego,
- powiązane dowody bezpieczeństwa,
- wniosek

Wszystkie wymagane działania w czasie projektowania, wdrażania i eksploatacji elektronicznych systemów SRK zebrano tabelach E1 ÷ E10 (załącznik E do normy EN 50129).

Bezpieczne działanie systemu wymaga prawidłowej reakcji na uszkodzenia. Do kategorii I usterek (zagrażających bezpośrednio bezpieczeństwu ruchu) zalicza się:

1. usterkę czujników włączających dla każdego toru i kierunku jazdy;
2. brak ciągłości kabla w obwodach czujników torowych;

3. obniżenie napięcia baterii akumulatorów poniżej ustalonego progu;
4. awarie uniemożliwiające poprawną pracę systemu wykryte przez układy samokontroli.
   - stwierdzenie braku komunikacji z układami przez którykolwiek ze sterowników,
   - brak komunikacji pomiędzy PLC a kontrolerem magistrali,
   - brak obecności jednego sterownika wykryty przez drugi sterownik,
   - brak zgodności między sterownikami w zdiagnozowanych stanach awarii kategorii I lub II;
5. brak ciągłości włókien żarówek w sygnalizatorach drogowych;
6. brak ciągłości drągów rogatkowych;
7. awarię napędów - nieprawidłowe położenie drągów rogatkowych w stanie ostrzegania.

W przypadku wykrycia usterki kategorii I powinno nastąpić ograniczenie prędkości pociągów w strefie przejazdu (załączenie pomarańczowych świateł na sygnalizatorach TOP). Ponadto w przypadku uszkodzenia czujników wjazdowych, sterownika lub utraty transmisji system przechodzi natychmiast w stan ostrzegania.

3.1. Rozwiązania sprzętowe

Elementy (sterowniki), które bezpośrednio wpływają na bezpieczeństwo zrealizowano jako układy dwukanałowe, pracujące na zasadzie „2 z 2". Oznacza to, że do prawidłowego funkcjonowania jest niezbędna prawidłowa i zgodna praca obu kanałów sterowników. W celu zwiększenia poziomu bezpieczeństwa systemu zastosowano asymetrię rozkazów wysyłanych ze sterowników decyzyjnych do urządzeń wykonawczych

- dla zamknięcia rogatek i załączenia sygnalizatora wystarcza komenda wysłana przez jeden ze sterowników decyzyjnych, otwarcie przejazdu wymaga potwierdzenia komendy przez obydwa sterowniki.
- zapalenie białych świateł a tarczach ostrzegawczych TOP przez sterowniki wymaga przesłania niezależnych komend od obu sterowników.

3.2. Rozwiązania programowe

Zgodnie z tabelami A2 i A18 normy CENELEC przy oprogramowaniu bezpiecznych systemów sterowania stosuje się odpowiednie środki.

Wymagania, określające współpracę sterowników i urządzeń zdalnych powinny być opracowane przez projektanta w postaci diagramów czasowych, określających następstwo sygnałów i komunikatów. W diagramach tych pisuje się ściśle określone ramy czasowe opisujące wymagane czasy reakcji poszczególnych urządzeń, oraz następstwo (w postaci opisu odpowiadającego składni FSM) poszczególnych: sygnałów, stanów i komunikatów.

W programie sterowników decyzyjnych stosuje się następujące środki (zgodnie z wytycznymi normy):

- programowanie defensywne,
- sprawdzanie zakresów zmiennych,
- sprawdzanie wartości indeksów dla tablic,
- sprawdzanie wartości i „wiarygodności" sygnałów wejściowych (odbierane dane nie mogą być sprzeczne),

– redundancja informacji - dane o stanie poszczególnych elementów przechowywane są w różnych zmiennych i informacja z tych zmiennych nie może być sprzeczna (chroni to program przed przekłamaniami dla poszczególnych zmiennych).

Oprogramowanie sterownika powinno uwzględniać wytyczne, zawarte w tabeli A.18 normy, tzn.:

– blok decyzyjny programu realizowany w oparciu o automat stanów (poszczególne sytuacje odwzorowane są w postaci odrębnych stanów),
– poszczególne zadania dotyczące komunikacji, analizy odebranych sygnałów i komunikatów oraz podejmowanie decyzji i wysyłanie rozkazów, realizowane w postaci osobnych funkcji i procedur. Procedury te wybierane są przez automat stanów lub wywoływane sekwencyjnie w przypadku konieczności zachowania odpowiednie kolejności sekwencji.

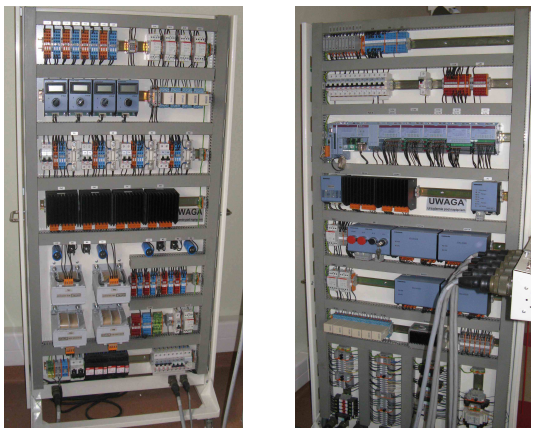
4. PORÓWNANIE WYBRANYCH MIKROPROCESOROWYCH SAMOCZYNNYCH SYGNALIZACJI PRZEJAZDOWYCH

4.1. Budowa sygnalizacji przejazdowej SPA-5

Urządzenia sterowania i zasilania umieszczono w szafie kontenerowej ERR-10, przy czym urządzenia poszczególnych kanałów (A, B) zainstalowano na odrębnych stojakach.

Na stojakach dla poszczególnych kanałów zmontowano:

– moduł jednostki centralnej (7CP476.60-1) serii 2003 firmy Bernecker & Rainer,
– moduły wejść/wyjść (7DI439.7, 7DM465.7, 7DM435.7, 7DI435.7),
– moduły przetwornic typu EDL-52,
– moduł sterowania ręcznego MP typu EMH-2,
– moduł generatora dźwięku typu EDG-4,
– moduły interfejsów czujników pociągu typu EOD-10,
– moduły stabilizatorów typu EMF-60, EMF-61,
– interfejs przekaźnikowy EDJ-43.



Rys. 2. Widok stojaków zasilania i sterowania sygnalizacji przejazdowej SPA-5

4.2. Budowa sygnalizacji przejazdowej RASP-4f

Wyposażenie kontenera głównego stanowią:
- układ zasilania,
- baterie akumulatorów,
- sterownik PLC(I) serii 90-30,
- sterownik PLC(II) serii 90-30,
- bloki wejścia/wyjścia GENIUS,
- terminal operatorski TIU 110,
- modem do komunikacji z RASP-UZK.

Rys. 3. Fragment stojaka z aparaturą sterującą sygnalizacji przejazdowej RASP-4f

Aparatura sterująco-kontrolna zlokalizowana jest w kontenerze głównym RASP-KG. Odbiera ona i analizuje sygnały pochodzące od urządzeń oddziaływania pociągu (czujników torowych) oraz steruje następującymi urządzeniami zewnętrznymi:
- sygnalizatorami drogowymi,
- napędami rogatkowymi,
- tarczami ostrzegawczymi przejazdowymi.

5. WNIOSKI

W praktycznych rozwiązaniach komputerowych systemów srk zwiększenie bezpieczeństwa osiąga się najczęściej przez nadmiar strukturalny. W najprostszy sposób realizuje się ją przez dwukanałową budowę układów, polegającą na zastosowaniu dwóch równolegle pracujących kanałów funkcjonalnych i komparacji ich pracy oraz dwa niezależne programy napisane przez różne zespoły programistów.

Zastosowanie samoczynnej sygnalizacji przejazdowej wykonanej w technice komputerowej, jak np. wyrobów produkcji Bombardier ZWUS Katowice, Scheidt & Bachmann, Siemens czy Z.A. KOMBUD Radom powoduje znaczne

oszczędności eksploatacyjne (tj. skrócenie czasu przejazdu, zmniejszenie kosztów zużycia energii), a jednocześnie zapewni odpowiedni poziom bezpieczeństwa komunikacyjnego.

Praca urządzeń samoczynnej sygnalizacji przejazdowej jest kontrolowana za pomocą urządzeń zdalnej kontroli (uzk), wykonanych w postaci specjalnego powtarzacza lub komputera diagnostycznego. Urządzenia te pozwalają na kontrolę ciągłości włókien żarówkowych, położenia i ciągłości drągów rogatek, połączenia z czujnikami, sprawności układów sterujących, itp.

Kontrola działania komputerowych urządzeń ssp polega m.in. na sprawdzaniu on-line oprogramowania sygnalizacji. Funkcje sterujące sygnalizacji przejazdowej realizowane są przez dwa różne programy, których wyniki są porównywane. Dodatkowo kontrolowany jest czas wykonania obu programów, komunikacja między sterownikami sygnalizacji, itp.

6. BIBLIOGRAFIA

[1] Dokumentacja Techniczno-Ruchowa: *Samoczynna sygnalizacja przejazdowa typu SPA-5*, Bombardier Transportation (ZWUS) Polska, Katowice 2002.
[2] Dokumentacja Techniczno-Ruchowa: *Samoczynna sygnalizacja przejazdowa RASP-4F*, Z.A. KOMBUD S.A. - KOMSTER S.A., Radom-Warszawa 2002.
[3] Dyduch J., Kornaszewski M.: *Analiza bezpieczeństwa systemów automatyki przejazdowej*, XI Konferencja „Drogi kolejowe 01", Wrocław-Żmigród 2001.
[4] Dyduch J., Kornaszewski M.: *Systemy sterowania ruchem kolejowym*, Wydawnictwo Politechniki Radomskiej, Radom 2007.
[5] Dyduch J.: *Innowacyjne systemy sterowania ruchem kolejowym.* Wydawnictwo Politechniki Radomskiej, Radom 2010.
[6] Kornaszewski M., Łukasik Z.: *Safe implementation of automatic microprocessor systems of level crossing on the example of the SPA-4 system*, PROBLEMY TRANSPORTU Tom 2 Zeszyt 2, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
[7] Kornaszewski M.: *Safe computer solutions applied in new generation railway traffic control systems*. Computer Systems Aided Science And Engineering Work in Transport, Mechanics and Electrical Engineering. Kasimir Pulaski Technical University of Radom, Faculty of Transport, Monograph No 122, Radom 2008.
[8] Lewiński A.: *Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego*, Wydawnictwo Politechniki Radomskiej, Radom 2001.
[9] Normy CENELEC: *EN50128, EN0129, EN50159-1, EN50159-2.*
[10] http://www.kombud.com.pl/