system sterujący, blokada liniowa,
analiza bezpieczeństwa, FMEA, FTA

Tadeusz CICHOCKI*
Janusz GÓRSKI**

ANALIZA BEZPIECZEŃSTWA SYSTEMU SAMOCZYNNEJ BLOKADY LINIOWEJ

Wymagania bezpieczeństwa, sformułowane na bazie kryteriów zdefiniowanych w trzech normach CENELEC, dotyczących systemów sterowania ruchem kolejowym: EN 50126 (o cyklu życia systemu), EN 50128 (o oprogramowaniu), EN 50129 (o konstrukcji dowodu bezpieczeństwa dla systemu), były podstawą dla zrealizowanego w Adtranz Zwus w Katowicach komputerowego systemu sterującego Samoczynnej Blokady Liniowej (SBL). W artykule przedstawiono elementy analizy bezpieczeństwa wykonanej dla tego systemu. Podkreślono działania, jakie będą podjęte w pracach nad rozwojem metody analizy.

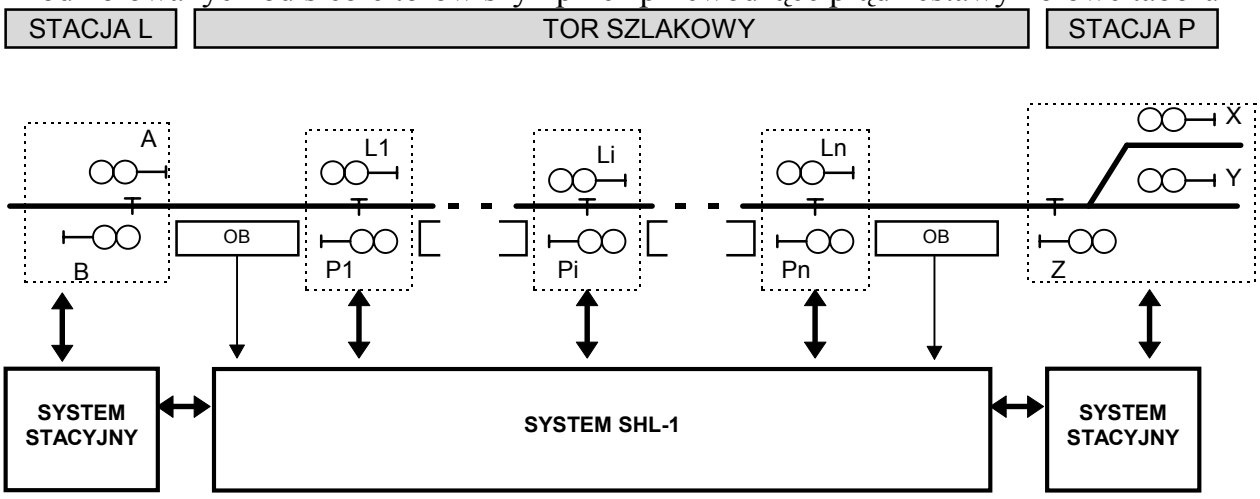
1. WSTĘP

Adtranz Zwus w Katowicach, firma grupy ABB Daimler-Benz Transportation, jest producentem systemów sterowania ruchem kolejowym przeznaczonych dla odbiorców krajowych i zagranicznych. Systemy te muszą charakteryzować się możliwie najwyższym poziomem bezpieczeństwa. Wymagania dotyczące procesu projektowego, metod, technik i narzędzi, architektury oraz wiarygodności systemu są sformułowane w trzech normach „kolejowych" CENELEC: EN 50126 (cykl życia systemu [9]), EN 50128 (oprogramowanie [10]), EN 50129 (konstrukcja dowodu bezpieczeństwa dla systemu [11]). Interpretacje tych norm są obecnie przyjmowane przez zarządy krajowe kolei w Europie, w tym przez PKP i Główny Inspektorat Kolejnictwa, instytucję nadzorującą operatorów transportu kolejowego w Polsce. Mając na uwadze wytyczne tych norm, w Adtranz Zwus zrealizowano komputerowy system sterujący Samoczynnej Blokady Liniowej (SBL). W artykule przedstawiono elementy analizy bezpieczeństwa systemu sterującego SBL. Miejsce systemu (nazwanego systemem SHL-1) w ramach systemu SBL pokazuje rysunek 1.

System SHL-1 bada zajętość odcinków toru (nazywanych *odstępami blokady*) oraz steruje sygnalizacją semaforową. Zezwolenie na przejazd pociągu może być udzielone tylko wówczas, gdy urządzenia kontroli zajętości odstępów wskazują, że odpowiedni odcinek toru jest wolny. Urządzeniem takim może być *obwód torowy* - obwód elektryczny, którego częścią są szyny. Szyny umożliwiają dwuprzewodowe doprowadzenie prądu elektrycznego (zwanego prądem sygnałowym) od nadajnika (źródła prądu) do odbiornika (zwykle przekaźnika torowego). Działanie obwodu torowego polega na zwieraniu lub nie zwieraniu

* Adtranz Zwus, ul. Modelarska 12, 40-142 Katowice, e-mail: tadeusz.cichocki@plsig.mail.abb.com
** Katedra Zastosowań Informatyki, Politechnika Gdańska, ul. Narutowicza 11/12, 80-952 Gdańsk, e-mail: jango@pg.gda.pl

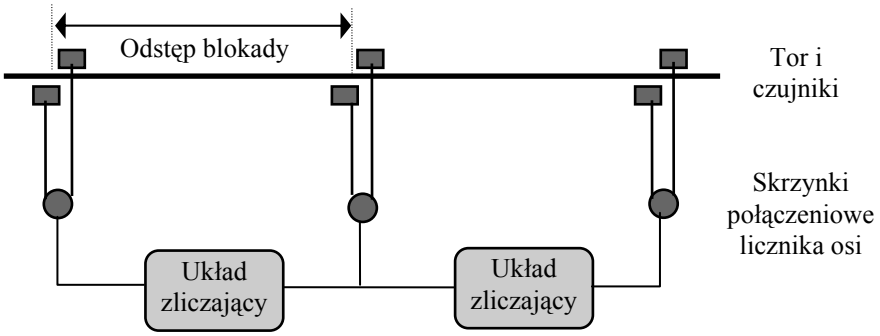
odizolowanych od siebie torów szyn przez przewodzące prąd zestawy kołowe taboru



Znaczenie symboli:
A, B - semafory stacyjne stacji kolejowej L (A - wjazdowy, B - wyjazdowy),
X, Y, Z - semafory stacyjne stacji kolejowej P (X i Y - wyjazdowe, Z - wjazdowe),
L1 - Ln - semafory odstępowe dla kierunku ruchu pociągów P→L (od stacji P do stacji L),
P1 - Pn - semafory odstępowe dla kierunku ruchu pociągów L→P (od stacji L do stacji P),
OB - odstęp blokady (odcinek toru pomiędzy semaforami).

Rysunek 1. System Samoczynnej Blokady Liniowej [3].

kolejowego. Kontrolę zajętości odcinka torowego można uzyskać także stosując liczniki osi (licznikowe obwody torowe [1]) lub inne rozwiązania. Kryterium niezajętości odstępu jest spełnione wtedy, gdy ta sama liczba osi zostanie zliczona na wejściu i na wyjściu danego odcinka toru (patrz rysunek 2).



Rysunek 2: Urządzenia kontrolujące zajętość odstępów blokady.

2. STEROWANIE RUCHEM KOLEJOWYM MIĘDZY STACJAMI

Celem każdego systemu kolejowego jest utrzymanie zadanego poziomu ruchu kolejowego (np. przelotowości szlaku kolejowego) oraz, co równie ważne, zapewnienie odpowiedniego poziomu bezpieczeństwa. W ciągu lat ewolucji systemów kolejowych zdefiniowano specyficzne zasady regulacji ruchu, *zasady sygnalizacji*, określające tzw.

bezpieczeństwo funkcjonalne. Każdy system sterowania ruchem kolejowym musi zachowywać się zgodnie z tymi zasadami, zarówno w przypadku właściwego funkcjonowania, jak i w przypadku uszkodzeń. Zadaniem Samoczynnej Blokady Liniowej (SBL) jest sterowanie ruchem pociągów na szlaku między stacjami poprzez wyświetlanie odpowiednich wskazań na semaforach osłaniających odcinki torowe o stałej długości (funkcjonowanie i ogólne wytyczne do budowy urządzeń sterowania ruchem kolejowym dla PKP są opisane w [1, 2]). Na każdy odstęp składa się izolowany odcinek toru oraz ustawiony przed nim semafor, którego wskazania uzależnione są od tego, czy osłaniany odstęp jest uznany za zajęty, czy wolny. Głównym celem bezpieczeństwa funkcjonalnego jest, aby w każdym odstępie mógł przebywać co najwyżej jeden pociąg.

Stany blokady są charakteryzowane przez następujący zestaw atrybutów:

- zestaw obrazów sygnałowych na semaforach i możliwości przejść między nimi,
- ustawienie kierunku ruchu na szlaku (ustawiony lub nie ustawiony, LP - z „lewej" na „prawą", PL - z „prawej" na „lewą", zastopowany, nie zastopowany),
- przebieg wyjazdowy ze stacji dla danego toru szlakowego (utwierdzony lub nie, realizowany lub nie),
- sprawność urządzeń blokady,
- zajętość odstępów blokowych.

Zmiana stanu blokady jest możliwa jedynie po wydaniu odpowiedniego polecenia przez dyżurnego ruchu (poprzez interfejs do urządzeń stacyjnych) znajdującego się na jednym z posterunków obsługi ograniczających dany szlak.

3. BEZPIECZEŃSTWO W KONTEKŚCIE BLOKADY LINIOWEJ

Realizacja bezpieczeństwa funkcjonalnego blokady odbywa się poprzez wyświetlanie wskazań sygnałów na semaforach. Zdefiniowano siedem wskazań na semaforach odstępowych (tzw. *obrazów sygnałowych*, będących kombinacją świateł zapalonych i zgaszonych), które są opisane jako S0, S1, S2, S3, S4, S5 i S.

Obraz sygnałowy	**Opis stanu świateł**	**Znaczenie obrazu sygnałowego dla mechanika jadącego pociągu przyjęte w PKP (por. [4])**
S0	brak światła (CIEMNY)	Stój - awaria semafora
S1	jedno światło czerwone ciągłe	Stój (przed semaforem)
S2	jedno światło zielone ciągłe	Jazda z największą dozwoloną prędkością
S3	jedno światło zielone migające	Jazda z największą dozwoloną prędkością, a przy następnym semaforze z prędkością nie przekraczającą 100 km/h
S4	jedno światło pomarańczowe migające	Jazda z największą dozwoloną prędkością, a przy następnym semaforze z prędkością nie przekraczającą 40 lub 60 km/godz
S5	jedno światło pomarańczowe ciągłe	Jazda z największą dozwoloną prędkością, a przy następnym semaforze - Stój
S	każda inna kombinacja (WĄTPLIWY)	Stój - awaria semafora

Dodatkowo muszą być spełnione zasady następstwa sygnałów dotyczące sąsiednich semaforów, zdefiniowane dla odpowiedniego rodzaju blokady: dwustawnej, trzystawnej lub czterostawnej. W myśl tych zasad, semafor odstępowy powinien wskazywać sygnał „Stój" tylko wtedy, gdy osłaniany odstęp jest zajęty.

- *W blokadzie dwustawnej*, światło zielone ciągłe oznacza, że co najmniej jeden odstęp blokowy za semaforem, patrząc w kierunku jazdy pociągu, nie jest zajęty.
- *W blokadzie trzystawnej*, światło zielone ciągłe oznacza, że co najmniej dwa odstępy blokowe za semaforem, nie są zajęte.
- *W blokadzie czterostawnej*, światło zielone ciągłe oznacza, że co najmniej trzy odstępy blokowe za semaforem nie są zajęte.

Przy zmianach sygnałów na semaforach odstępowych, jedynym dozwolonym stanem przejściowym jest stan z ciemnym semaforem.

W *normalnym* trybie pracy obraz sygnałowy każdego semafora odstępowego zależy od:

- stanu blokady dla każdego kierunku ruchu,
- wskazania na semaforze następnym w danym kierunku ruchu,
- zajętości odstępu blokowego osłanianego przez dany semafor,
- tego, czy jest to ostatni semafor odstępowy, czy nie.

Bezpieczeństwo funkcjonalne wynika z właściwej realizacji zasad zarządzania stanem blokady liniowej (ustalanie kierunków ruchu, ustalanie obrazów sygnałowych na semaforach). Implementacja bezpieczeństwa funkcjonalnego wymaga zastosowania różnorodnych urządzeń współpracujących ze sobą w ramach ustalonej *architektury systemu*. W sposób naturalny powstaje więc pytanie co się stanie gdy jedno lub więcej z tych urządzeń zawiedzie (i w konsekwencji naruszy zasady gwarantujące bezpieczeństwo funkcjonalne). Prowadzi to do pojęcia *bezpieczeństwa strukturalnego,* związanego z tworzeniem gwarancji, że usterki składników architektury systemu nie zagrożą bezpieczeństwu funkcjonalnemu. W kolejnictwie bezpieczeństwo strukturalne jest osiągane poprzez stosowanie mechanizmów *tolerowania usterek*, ograniczanie od góry czasu *ujawniania usterek* oraz zastosowanie *stanu bezpiecznego*, który jest automatycznie osiągany przez system, w przypadku ujawnienia usterki jego elementu. Awarie, które powinny być tolerowane przez SBL, to:

- wszelkie awarie semaforów (nawet wszystkich żarówek we wszystkich semaforach),
- wszelkie awarie czujników niezajętości odstępów blokowych (nawet, gdy sygnalizowana jest zajętość wszystkich odstępów),
- wszelkie awarie systemów alarmowych (nawet, gdy wszystkie alarmy są aktywne),
- pojedyncze błędy transmisji w komunikacji pomiędzy posterunkami.

Jeżeli na określonym semaforze zgaśnie żarówka światła czerwonego mimo, że odstęp chroniony tym semaforem jest zajęty przez pociąg, to sygnał „Stój" jest automatycznie przeniesiony na poprzedni semafor. Następuje automatyczne wydłużenie odstępu blokowego, gdyż musi być zachowana podstawowa zasada ochrony pociągu sygnałem „Stój". Jeśli na semaforze podającym sygnał przepali się żarówka pomarańczowa, to na tym semaforze podany będzie sygnał „Stój", zaś na semaforach poprzednich odpowiednie sygnały. Niemożność wyświetlenia sygnału właściwego (dla danej sytuacji) prowadzi do

próby wyświetlenia sygnału bardziej restrykcyjnego.

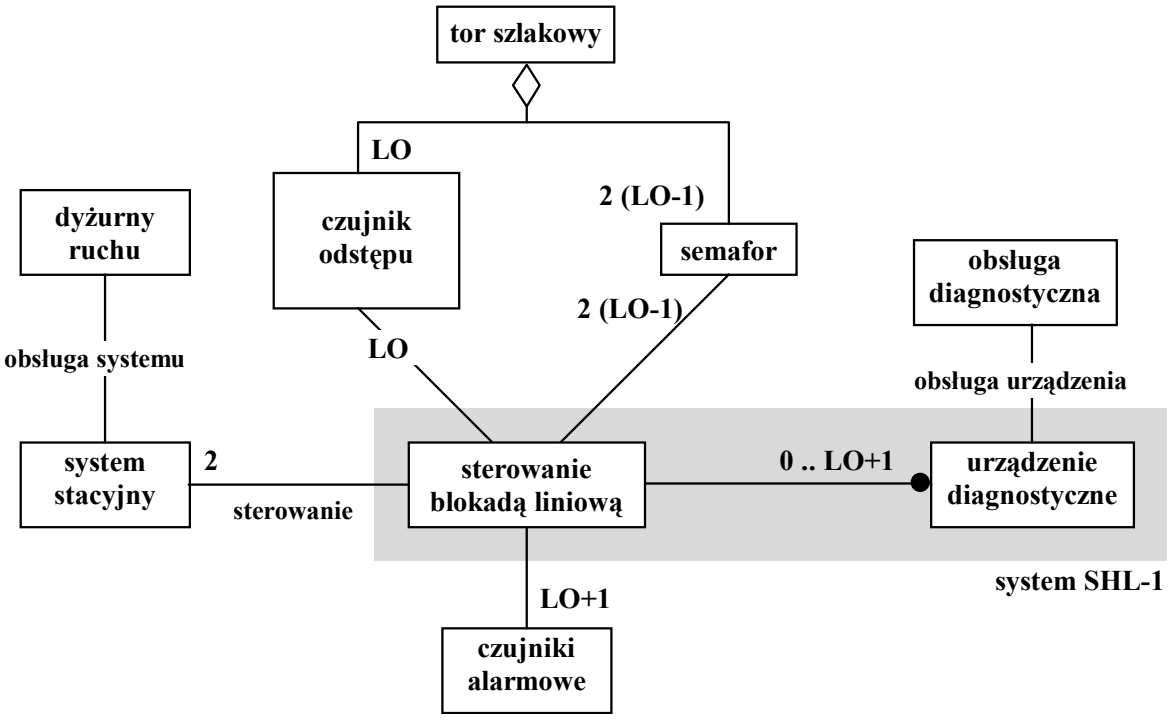
W „kolejowych” normach CENELEC mechanizmy bezpieczeństwa funkcjonalnego i strukturalnego są uzupełniane przez rygorystycznie zdefiniowany proces rozwojowy systemu, mający ograniczyć możliwość wprowadzenia do systemu usterek systematycznych (unikanie usterek).

4. ARCHITEKTURA SYSTEMU STERUJĄCEGO SHL-1

System SHL-1 jest komputerowym systemem sterowania systemem SBL. System SHL-1 współpracuje z torem szlakowym oraz z systemami stacyjnymi poprzez interfejsy, które:

- sterują semaforami odstępowymi,
- odczytują sygnały o stanie danego odcinka blokowego,
- przekazują informacje o stanie blokady do dwóch sąsiednich punktów sterowania i, poprzez stacyjne punkty sterowania, do urządzeń stacyjnych,
- współpracują z systemami do kontroli prowadzenia pociągów (opcjonalnie),
- współpracują z systemami samoczynnej sygnalizacji przejazdowej (opcjonalnie).

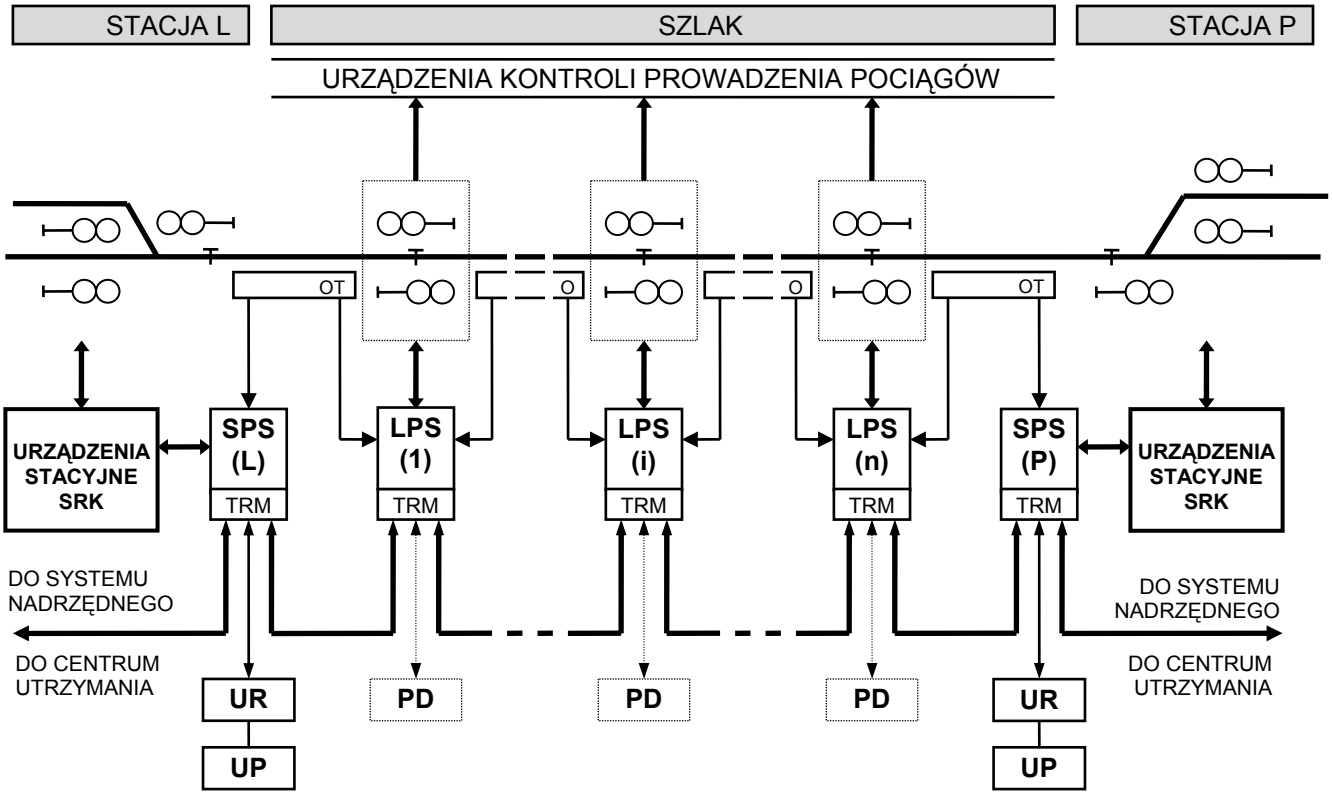
Model systemu SHL-1 i jego środowiska wyrażony w notacji obiektowej [8] przedstawia rysunek 3.



Rysunek 3. Model obiektowy systemu SHL-1 w jego środowisku.
LO - liczba odcinków blokowych na torze szlakowym objętym systemem SHL-1.

Na rysunku 4 przedstawiono architekturę systemu SHL-1. Oprogramowanie sterujące jest rozproszone między punkty sterowania: liniowe (LPS) i stacyjne (SPS). Każdy punkt sterowania jest realizowany w strukturze zróżnicowanych modułów programowo-

sprzętowych. Oprogramowanie komunikacyjne pomiędzy punktami sterowania łączy te moduły w jedną strukturę całej blokady.



Znaczenie symboli:

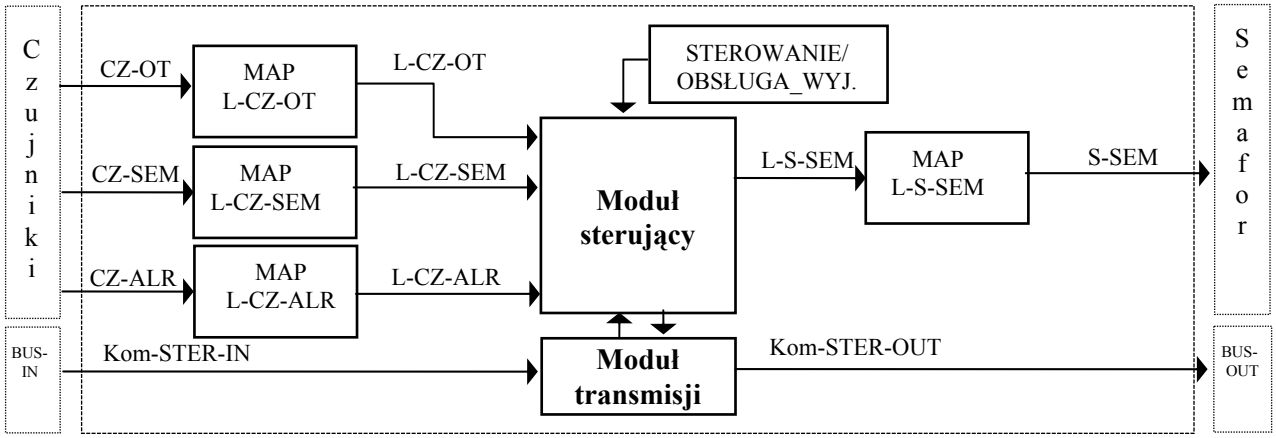
OT	- odcinek torowy
SPS	- stacyjny punkt sterowania
LPS	- liniowy punkt sterowania
UR	- urządzenie rejestrujące („czarna skrzynka”)
UP	- urządzenie prezentacji (komputer PC)
PD	- panel diagnostyczny
TRM	- łącza transmisyjne

Rysunek 4. Architektura systemu SHL-1 [3].
Na rysunku nie uwzględniono systemów alarmowych.

Powiązanie ze stacją jest realizowane poprzez interfejs do urządzeń stacyjnych będący częścią *stacyjnego punktu sterowania* (SPS). Realizacja sprzętowa interfejsu, zależnie od typu urządzeń stacyjnych, bazuje na technice przekaźnikowej lub elektronicznej. SPS obsługuje polecenia obsługi dotyczące ustawiania kierunku ruchu. Urządzenia stacyjne przekazują do SHL-1 informacje o stanie semafora wjazdowego oraz informacje o zadanym stanie danego toru szlakowego. SHL-1 przekazuje do urządzeń stacyjnych informacje o stanach blokady opisywanych poprzez ustawiony kierunek ruchu na szlaku lub stany pośrednie oraz informacje (w tym sygnałowe) o stanie pierwszego semafora blokady, a jeśli blokada ma tylko jeden odstęp (następny semafor za semaforem wyjazdowym stacji jest semaforem wjazdowym następnej stacji), także informację o wskazaniach następnego semafora.

5. OPROGRAMOWANIE LOKALNEGO PUNKTU STERUJĄCEGO (LPS)

Architekturę oprogramowania lokalnego punktu sterującego przedstawiono na rysunku 5.



Znaczenie symboli:

CZ-OT	- grupa czujników zajętości odstępów blokowych,
CZ-SEM	- grupa czujników żarówek semaforów,
CZ-ARM	- grupa czujników alarmowych (zasilanie, drzwi obudowy, przeciwpożarowe),
S-SEM	- sygnał sterowania semaforem,
Kom-STER-IN/OUT	- port komunikacyjny między sąsiednimi punktami sterowania.

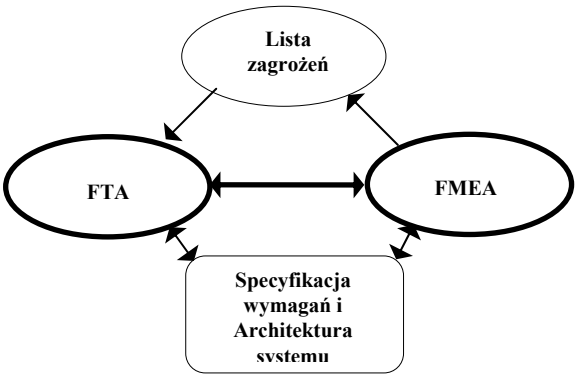
Rysunek 5. Architektura oprogramowania LPS.

W blokadzie z licznikami osi na końcach kontrolowanego odstępu umieszczone są czujniki zajętości odstępów blokady, które reagują na każdą przejeżdżającą nad nimi oś taboru. Do LPS jest przekazywana informacja o liczbie osi w odstępie, o kierunku zliczania, o poprawności działania elementów układu (lub sygnał „usterka"). Równowaga (stan zerowy) w układzie liczącym oznacza spełnienie kryterium niezajętości odstępu i powoduje wyświetlenie na semaforze sygnału zezwalającego na jazdę pociągu w danym odstępie (sygnał „droga wolna"). Naruszenie tej równowagi świadczy o zajętości odstępu i powoduje włączenie sygnału „stój" na semaforze go osłaniającym. Usterka w urządzeniu lub wyłączenie z działania jakiejkolwiek jego części zawsze likwidują stan niezajętości odstępu. Informacja o stanach (logicznych i fizycznych) LPS przesyłana jest cyklicznie do sąsiednich punktów sterowania. Zadania realizowane przez LPS są realizowane zgodnie ze zdefiniowanym cyklem pracy o długości T. W ramach pojedynczego okresu T muszą zostać zrealizowane wszystkie te zadania, których wynik ma wpływ na wskazania semaforów odstępowych.

6. ANALIZA BEZPIECZEŃSTWA SYSTEMU SHL-1

Analizę bezpieczeństwa systemu przeprowadzono zgodnie ze schematem przedstawionym na rysunku 6. Punktem wyjścia analiz była z jednej strony lista zagrożeń względem systemu, a z drugiej strony specyfikacja wymagań względem systemu oraz

specyfikacja jego architektury. Podstawowe techniki, które zastosowano do analiz to analiza drzew błędów (*Fault Tree Analysis - FTA*) [13] oraz FMEA (*Failure Mode and Effect Analysis*) [7, 5]. Wykorzystano tu komplementarny charakter tych technik, które dają podstawy do wzajemnej weryfikacji dostarczanych przez nie wyników. W dalszej części tego rozdziału omówiono dokładniej zakres przeprowadzonych analiz.



Rysunek 6. Struktura analizy bezpieczeństwa systemu SHL-1.

6.1. ANALIZA ZAGROŻEŃ

Poniżej przedstawiono klasyfikację zagrożeń w systemie samoczynnej blokady liniowej:

- brak wskazania sygnału „Stój", gdy osłaniany odcinek jest zajęty (w wyniku uszkodzenia żarówki światła czerwonego lub powstania przerwy w jej obwodzie),
- rozerwanie pociągu (rozpięcie wagonów),
- rozkręcenie szyn,
- uszkodzenie przewodów połączeniowych obwodów lub semafora,
- wyczerpanie baterii zasilającej obwód lub semafor,
- zakłócenia w obwodzie torowym (błędne naliczanie osi).

Stany awaryjne, które muszą być prezentowane personelowi obsługi oraz personelowi utrzymania na posterunkach zapowiadawczych obejmują:

- wykrycie usterki w obwodzie żarówki semafora odstępowego,
- otwarcie kontenera,
- pożar w kontenerze.

6.2. SPECYFIKACJA WYMAGAŃ WZGLĘDEM SYSTEMU

Warunkiem bardziej szczegółowych analiz było dokonanie precyzyjnej spacyfikacji wymagań względem systemu. Prace w zakresie inżynierii wymagań wymagały uściśleń w interpretacji przepisów PKP (WTB E-10 i E-1 [1, 4]) i doprowadziły do wytworzenia dokumentu Specyfikacji Wymagań Systemowych odpowiadającego przyjętemu wcześniej standardowi. Ustalono tryby pracy systemu, jego granice logiczne i fizyczne. Ustalono definicje stosowanych terminów, jednoznacznych dla realizatorów analizy, zgodnych z

pozostałą dokumentacją i działaniami projektowymi. Wyspecyfikowano funkcje systemu związane ze sterowaniem blokadą i realizacją bezpieczeństwa funkcjonalnego. Wyróżniono *stan bezpieczny* systemu jako stan po reakcji na usterkę, polegający na:

- uniemożliwieniu ustawienia przebiegu wyjazdowego na stacji,
- brak realizacji poleceń ruchowych dla blokady,
- osłanianie obszaru wystąpienia usterki przez wskazania odpowiednich semaforów odstępowych.

Zdefiniowano także stan bezpieczny elementu systemu, jako taki jego stan, który inicjuje przejście systemu blokady do jego stanu bezpiecznego.

6.3. ANALIZA FMEA

Analiza FMEA bazuje na systematycznym podejściu do *identyfikacji* oraz oceny *propagacji* i *efektów* pojedynczych usterek elementów systemu. Wyprowadzana informacja obejmuje *typy, scenariusze i wzorce uszkodzeń* oraz dostępne i planowane akcje ujawniania, kontroli i odtwarzania po błędach.

Lista elementów struktury SHL-1 oraz ich usterek wyróżnionych w analizie FMEA wyglądała następująco:

Lp.	**Element**	**Lista usterek elementu**	**Uzasadnienie listy**
1	SPS	a. Brak lub błędna komunikacja do urządzeń stacyjnych. b. Brak lub błędna komunikacja do UR. c. Brak lub nieprawidłowy jeden z dwóch sygnałów sterujących do OT. d. Brak lub błędny sygnał sterujący do urządzeń stacyjnych. e. Brak lub błąd komunikatu do LPS. f. Błąd informacji do drugiego UR.	Negacja funkcji określającej misję tego elementu: *łączenie „blokady liniowej" z „urządzeniami stacyjnymi"*.
2	LPS	a. Brak lub nieprawidłowy jeden z dwóch sygnałów kontrolnych do OT/L lub do OT/P. b. Brak lub nieprawidłowy komunikat do LPS/ L lub do LPS/ P. c. Brak sterowania semaforem LP lub PL. d. Sterowanie semaforem bardziej restrykcyjne niż wynika to z sytuacji ruchowej.	Negacja funkcji określajacej misję tego elementu: *sterowanie semaforami na podstawie informacji z „blokady liniowej"*.
3	Łącze / moduł transmisyjny pomiędzy XPS-XPS (obejmuje procedury sprawdzania poprawności fizycznej i logicznej przesyłanych komunikatów)	a. Powtórzenie komunikatu w danym cyklu. b. Usunięcie / brak komunikatu. c. Wstawienie komunikatu. d. Zamiana kolejności przesyłanych komunikatów. e. Uszkodzenie komunikatu. f. Opóźnienie komunikatu. g. Komunikat błędny, uchodzący za autentyczny. h. Fizyczne uszkodzenie łącza transmisyjnego.	(Misja: *fizyczna realizacja kanału logicznego*.) Lista błędów komunikatów na podstawie normy EN 50159.

4	Semafor (element środowiska)	a. Nie świeci się żądana żarówka. b. Świeci się niepożądana żarówka. c. Nastąpiło zwarcie w obwodzie żarówki. d. Nastąpiła przerwa w obwodzie żarówki.	---
5	Obwód torowy (element środowiska)	a. Zwarcie w obwodzie (A lub M) odczytującym stan zestyku przekaźnika torowego. b. Przerwa w obwodzie (A lub M) odczytującym stan zestyku przekaźnika torowego.	---
6	Urządzenie rejestrujące (UR, „czarna skrzynka”)	a. Nie zapisuje i potwierdza. b. Źle zapisuje i potwierdza. c. Nie potwierdza.	(Misja: rejestracja i potwierdzanie rejestracji.)
7	Urządzenia stacyjne (element środowiska)	a. Brak informacji o stanie semafora wjazdowego. b. Brak poleceń. c. Brak informacji o utwierdzeniu przebiegu. d. Błędna informacja w jednym z kanałów (A lub M).	---
8	Zasilanie zewnętrzne 220 V (element środowiska)	a. Brak zasilania. b. Niewłaściwe parametry zasilania.	---

Awarie wyróżnionych elementów zostały zdefiniowane jako zaprzeczenie usług (funkcji) tych elementów świadczonych na rzecz innych elementów. Przyjęto następującą ogólną definicję usługi dostarczanej przez dany element: *właściwa operacja (dane, sygnały) we właściwym czasie*.

Rozważano następujące źródła błędów blokady z licznikami osi:

- usterki liczników,
- pomyłki przy zliczaniu jako osi różnych zwisających części taboru, takich jak klocki hamulcowe lub łączniki wagonów,
- nie wykrywanie pęknięć szyn,
- nie wykrycie zajętości odstępu przez wykolejony wagon z sąsiedniego toru,
- zakłócenia pochodzące od obcych prądów, pól magnetycznych i elektrycznych,
- brak stabilności pracy licznika w różnych warunkach atmosferycznych,
- wibracje i udary mechaniczne, przepięcia, zakłócenia elektromagnetyczne.

Przyjęto, że oprogramowanie sterujące musi reagować na następujące niepożądane zdarzenia zewnętrzne (generowane przez czujniki):

- usterka żarówki semafora lub kluczy przełączających,
- usterka obwodu torowego (czujnika zajętości toru),
- sygnał alarmowy,
- awaria innego punktu sterowania,
- brak/błąd polecenia sterującego.

Identyfikacja *ścieżek błędów* generowanych przez potencjalne usterki wyróżnionych

elementów służyła do weryfikacji mechanizmów odpowiedzi systemu na te zdarzenia: definicji podziału i zakresu odpowiedzialności współpracujących elementów. Sprawdzano, w szczególności, czy reakcja bezpieczeństwa (polegająca na przechodzeniu systemu do wyróżnionego stanu bezpiecznego) jest przez system podejmowana automatycznie w odpowiedzi na każdą usterkę elementów systemu. Wybrany poziom ujawniania usterek i wypracowywania decyzji o reakcji bezpieczeństwa sprawdzono pod względem kompletności. Rozumowanie to obok analizy misji wyróżnionych elementów tego poziomu struktury wsparte zostało analizą lokalną FMEA dla punktów sterowania oraz globalną analizą FTA (w drugim wniosku z tej analizy).

W przypadkach, w których reakcja bezpieczeństwa nie była podejmowana, dokonywano identyfikacji i oceny zagrożeń związanych z postulowanymi usterkami. Identyfikowane były możliwe zachowania niepożądane w celu podjęcia odpowiednich decyzji projektowych. Dokumentacja ostatniego cyklu analizy służyła do uzasadnienia kompletności analiz i poprawności architektury (zaproponowano rozwiązania wszystkich problemów) oraz stanowiła podstawę dla definicji przypadków testowych.

W analizie wybrano elementy odpowiadające poziomowi struktury systemu, na którym podejmowane są reakcje na zagrożenia bezpieczeństwa systemu (bezpieczeństwo strukturalne). Do tej listy dołączono istotne moduły współpracujące z systemem (udostępniające dane lub sterowane przez system) jako elementy środowiska.

Przyjęto, że awarie połączeń nie wymienione jawnie w analizie, ograniczone są do braku (zaniku) danego połączenia i przypisane są odpowiedniemu elementowi przynoszącemu daną usługę.

Za podstawę oceny krytyczności awarii przyjęto stopień degradacji funkcji dotkniętej daną awarią:

- możliwy zakres strat wynikający ze skutków awarii,
- czas trwania zakłócenia/utraty/degradacji funkcji systemu,
- dostępność środków alternatywnych umożliwiających (bezpieczną) kontynuację ruchu przy ograniczonej funkcjonalności systemu.

W uzupełnieniu rozważano ocenę i możliwości diagnostyczne operatora systemu.
Wyniki analiz zostały przedstawione w ramach następującej struktury danych.

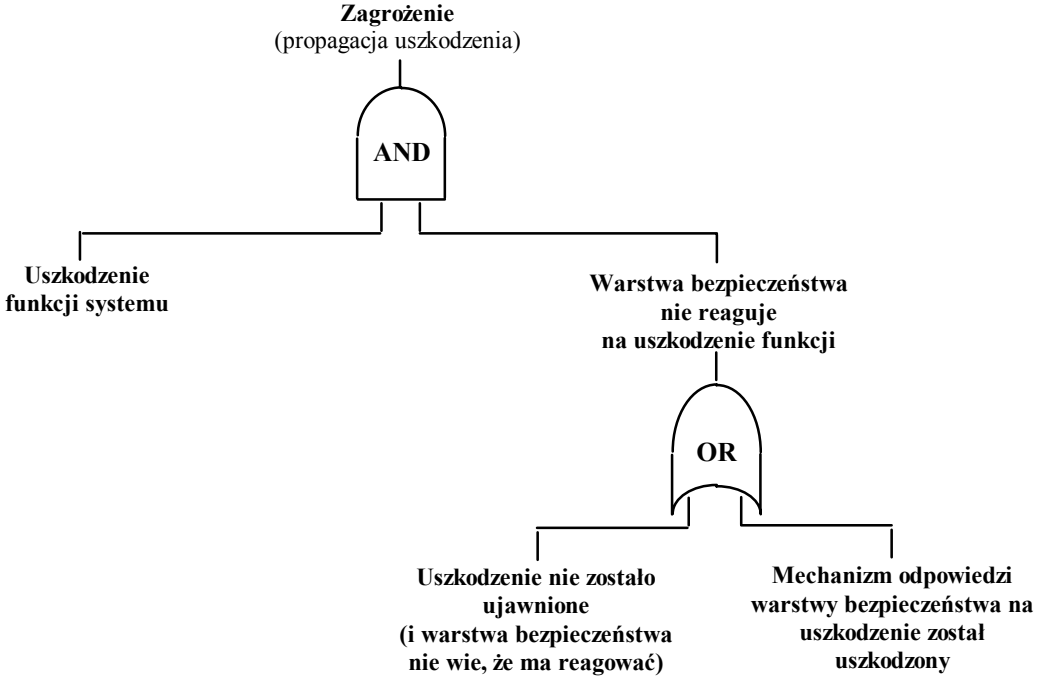
Rodzaj usterki / błędu	Efekt usterki / błędu (lokalny, wtórny i końcowy) *elementy bezpośrednio dotknięte usterką / błędem*	Przyczyna usterki / błędu	Ocena ryzyka dla tej usterki / błędu	Zalecane działania korekcyjne / prewencyjne	Ujawnie-nie usterki / błędu	Przejście do stanu bezpiecznego

W analizie FMEA (po raz pierwszy w Adtranz Zwus w takim stopniu) dokonano:

- (ważnego dla tej analizy) uporządkowania informacji wejściowej,
- uściślenia pojęć używanych w analizie,
- przygotowania raportu z uwzględnieniem postawionych celów, oraz
- pokazano członkom zespołu (element szkoleniowy: część zespołu wykazała się aktywnym udziałem w pracach) potrzebę i możliwości kroku poprawy.

6.4. ANALIZA FTA

Kombinacje usterek prowadzące do zagrożeń i odpowiedzi projektowe na te usterki były rozważone w ramach analizy drzew błędów FTA. Główną ideę drzewa błędów dla systemu SHL-1 zobrazowano na rysunku poniżej.



Rysunek 7. Struktura drzewa błędów dla systemu SHL-1.

Lista usterek, które mogą prowadzić do zagrożeń zawiera się w zestawie usterek postulowanych w analizie FMEA. Na bazie drzew błędów uzasadniono, że dowolna usterka systemu będącego w stanie bezpiecznym nie wyprowadza go z tego stanu, oraz, że wyprowadzenie systemu ze stanu bezpiecznego wymaga zewnętrznej ingerencji serwisowej. Uzasadnienia te zostały poparte odpowiednim programem badań w środowisku laboratoryjnym i użytkowania.

Nie analizowano niezawodności podsystemu transmisji na poziomie generowania ramek, poprzestając na implementacji systemu kodowania informacji, analogicznej do systemu Ebilock 850 (produkcji Adtranz Sweden) wielokrotnie sprawdzonego i certyfikowanego. Odniesiono się natomiast do możliwych błędów na poziomie zarządzania ramkami między punktami sterowania (według klasyfikacji z EN 50156 [12]): ramka powtórzona, zgubiona, przypadkowa (nadmiarowa), w niewłaściwym porządku, z uszkodzonymi danymi, spóźniona, oraz zmodyfikowana ale uchodząca za autentyczną.

7. UZYSKANE EFEKTY

Analiza bezpieczeństwa zastosowana do systemu SHL-1, realizowana w środowisku zarządzania jakością zgodnym z ISO 9001 i zarządzania bezpieczeństwem według EN 50126, pozwoliła na stwierdzenie, że spełnione zostały wymagania norm „kolejowych”

CENELEC. W wyznaczonym czasie dokonano weryfikacji architektury systemu w odniesieniu do zidentyfikowanych zagrożeń oraz usterek elementów. Działania te były także przykładem interpretacji wymienionych norm w kontekście konkretnego projektu, stając się przewodnikiem i punktem wyjścia dla innych projektów w Adtranz Zwus. Otwarte pozostało pytanie o efektywność procesu analizy (szczególnie w sytuacji nacisków dotyczących terminów zakończenia prac).

Akceptacja ze strony instytucji oceniającej wyniki analiz (była to jedna z pierwszych w Polsce analiz dokonanych w oparciu o normy CENELEC) została związana z postulatem rozważenia dodatkowej usterki niższego poziomu. Niezależnie zaprojektowane testy funkcjonalne i bezpieczeństwa ujawniły usterkę i zachowanie nie uwzględnione w analizie. W odpowiedzi dokonano natychmiast weryfikacji specyfikacji systemu oraz odpowiednich jej modyfikacji. Pozytywne wyniki testów środowiskowych i wyjaśnienia zespołu projektowego uzupełniły przygotowany pakiet bezpieczeństwa: system SHL-1 uzyskał certyfikat bezpieczeństwa.

Dominującym sposobem postępowania w analizach dotyczących SHL-1 była „burza mózgów" zespołu projektowego dotycząca wyróżnienia elementów architektury systemu oraz ich powiązań. Analizy te nie znajdowały jednak właściwego wsparcia w kompletnej i precyzyjnej dokumentacji systemu. Wiedza o systemie była wiedzą któregoś z członków zespołu biorącego udział w pracach projektowych i programistycznych.

Pośrednim efektem przeprowadzonych analiz był wzrost świadomości projektantów systemu i lepsze zrozumienie przez nich celów i wymogów związanych z osiąganiem właściwego poziomu bezpieczeństwa projektowanego systemu.

Zdobyte doświadczenia wskazują [7], że należy wzmacniać bazę dla analizy FMEA poprzez:

- poprawę jakości źródeł danych do procesu analizy, a w szczególności poprawę jakości powstających specyfikacji i związanych z nimi modeli,
- integrację procesu FMEA z innymi (wykonywanymi równolegle) działaniami w ramach procesu projektowo-wytwórczego,
- poprawę efektywności procesu zapewniania jakości tworzonego oprogramowania.

LITERATURA

[1] „*Wytyczne techniczne budowy urządzeń sterowania ruchem kolejowym w przedsiębiorstwie Polskie Koleje Państwowe*" (WTB-E10), PKP Dyrekcja Generalna, Warszawa 1996.

[2] J. NEMEC, A. WOPIŃSKI, *Elektryczne urządzenia zabezpieczenia ruchu kolejowego. Urządzenia liniowe*, Wydawnictwa Komunikacji i Łączności, Warszawa 1974.

[3] Specyfikacja wymagań systemu SHL-1, Projekt ADZ-SHL-1 (ITTI/Adtranz Zwus), 1997.

[4] „*Przepisy sygnalizacji na Polskich Kolejach Państwowych*" (E1), PKP Dyrekcja Generalna.

[5] IEC 812 (1985): Procedure for failure mode and effects analysis (FMEA), TC56 (polskie tłumaczenie: PN-IEC 812: 1994).

[6] NANCY G. LEVESON, Safeware: System Safety and Computers, Addison-Wesley Publishing Co., 1995, ISBN 0-201-11972-2.

[7] T. CICHOCKI, J. GÓRSKI, Analiza bezpieczeństwa przemysłowych zastosowań informatyki z wykorzystaniem metody FMEA, III Konferencja Naukowo-Techniczna „Diagnostyka Procesów Przemysłowych", Jurata k/Gdańska, 7-10 września 1998.

[8] J. RAMBAUGH, M. BLAHA, W. PREMERLANI, F. EDDY, W. LORENSEN: *Object-Oriented Modelling and*

Design, Prentice-Hall Int., 1991.
[9] EN 50126: Railway applications - The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS), CENELEC, Final Draft version, June 1997.
[10] EN 50128: Railway applications - Software for railway control and protection systems, CENELEC, Final Draft version, June 1997.
[11] ENV 50129: Railway applications - Safety Related Electronic Systems for Signalling, CENELEC, ver. 1.0, January 1997.
[12] prEN 50159-1: Railway applications - Communication, signalling and processing systems. Part 1: *Safety-related communication in closed transmission systems*, CENELEC, Final Draft, June 1998.
[13] IEC 1025, Fault Tree Analysis (FTA), 1990
(*polskie tłumaczenie*: PN-IEC 1025, Analiza drzewa niezdatności (FTA), grudzień 1994).

A SAFETY ANALYSIS OF A LINE BLOCK SYSTEM

Adtranz Zwus in Katowice, an ABB Daimler-Benz Transportation group company, is a railway control systems developer. The requirements for the systems include safety requirements implied by the currently developed three „railway" CENELEC norms: EN 50126 (for system life cycle), EN 50128 (for software), EN 50129 (for safety proof construction). Interpretations of these norms are now under development taken by the national railway authorities in Europe, including PKP and GIK in Poland. With the requirements in mind, Adtranz Zwus developed a Computerised Line Block system. The article presents the main steps of the safety analysis performed for the system. Conclusions underline the steps in the development of the analysis which are going to be taken.