Radom, 19.05.2015

Prof. dr hab. inż. Andrzej Lewiński
Wydział Transportu i Elektrotechniki,
Instytut Automatyki i Telematyki Transportu
Uniwersytet Technologiczno – Humanistyczny im. K. Pułaskiego w Radomiu

Recenzja rozprawy doktorskiej mgr inż. Mariusza Maciejewskiego pt. „Metoda budowy komputerowych systemów sterowania ruchem kolejowym" napisanej pod kierunkiem dr hab. Wiesława Zabłockiego, profesora nadzwyczajnego Politechniki Warszawskiej.

1. Podstawa opracowania, przedmiot recenzji

Podstawą recenzji jest pismo Dziekana Wydziału Transportu Politechniki Warszawskiej z dnia 2.04.2015.

Przedmiotem recenzji jest rozprawa doktorska mgr inż. Mariusza Maciejewskiego pt. „Metoda budowy komputerowych systemów sterowania ruchem kolejowym". Rozprawa zawiera 147 stron, 36 rysunków (w tym fotografii i obrazów monitora komputerowego), 21 tabel, wykaz literatury obejmuje 128 pozycji.

Rozprawa dotyczy koncepcji bezpiecznego oprogramowania komputerowego systemu sterowania ruchem kolejowym (systemu srk) na podstawie formalnej specyfikacji funkcjonalnej w języku automatów o skończonej liczbie stanów. Należy w tym miejscu podkreślić, że Autor dysertacji jest uznanym specjalistą w środowisku inżynierów zajmujących się ogólną tematyką srk w zakresie projektowania wdrażania i utrzymania komputerowych systemów srk. (systemy te są od wielu lat eksploatowane w kolejnictwie polskim).

2. Ocena wyboru tematu rozprawy

Temat rozprawy związany jest z metodą specyfikacji, projektowania i implementacji bezpiecznego systemu komputerowego na podstawie sformalizowanego opisu funkcjonalnego w postaci deterministycznych automatów o skończonej liczbie stanów.

Autor przedstawił zasadę projektowania bezpiecznego systemu sterowania ruchem kolejowym (srk) zgodnego z obowiązującymi w UE (i oczywiście w kolejnictwie polskim) wymaganiami i standardami (dotyczy to głównie grupy norm 50 12x). Obejmuje ona m. in. zasady konfiguracji sprzętu, utworzenia odpowiedniego oprogramowania oraz implementacji systemu komputerowego uwzględniającego wymagane procedury weryfikacji.

Autor przedstawia metodę konfiguracji sterowników komputerowych na bazie typowego, dostępnego na rynku sprzętu do sterowania komputerowego co prowadzi do ekonomicznego, ale bezpiecznego systemu srk.

Jeśli chodzi o bezpieczne oprogramowanie takich systemów, Autor zaproponował oryginalną transformację opisu systemu na poziomie automatu o skończonej liczbie stanów do implementacji tak opisanych obiektów w postaci modułów oprogramowania w czasie rzeczywistym.

Implementacja tak projektowanego systemu wymagała przy integracji sprzętu i oprogramowania odpowiednich metod weryfikacji i testowania, Autor poza zalecaną dla takich systemów metodą V zaproponował inne metody m. in. w celu poznania reakcji systemu na sytuacje awaryjne.

Zaproponowana w rozprawie przez Autora koncepcja wykorzystuje do specyfikacji systemu srk aparat formalny opracowany przez prof. W. Zabłockiego, taka specyfikacja gwarantuje jednoznaczność i poprawność matematyczną. Autor zaproponował własną, oryginalną realizację automatów abstrakcyjnych poprzez programowanie strukturalne i obiektowe.

Autor pokazuje też możliwości swojej metody na wybranym przykładach – wdrożonych systemach srk (WSKR i WTUZ), których był współautorem.

Autor słusznie stwierdza, że zastosowane w dysertacji oryginalne (ale oparte na ogólnie dostępnych technologiach informatycznych) metody projektowania, weryfikacji i wdrażania pozwalają na implementację „oryginalnego, bezpiecznego i ekonomicznie uzasadnionego" komputerowego systemu srk. Wiąże się to z zapewnieniem realizacji systemu zgodnej z obowiązującymi wymaganiami i standardami oraz parametrami nie ustępującymi podobnym realizacjom w UE.

Przedstawiona rozprawa jest z pogranicza dwu dziedzin:

- współczesnej informatyki obejmującej nowe metody specyfikacji, projektowania i modelowania systemów technicznych wykorzystujące technologie nowoczesnego sterowania komputerowego zapewniające poprawne (pod względem formalnym), bezpieczne (zgodnie z wymaganiami teorii sterowania ruchem kolejowym) oraz niezawodne technicznie systemy (komputerowe),

- nowoczesnej teorii sterowania ruchem kolejowym opartej na niezawodności systemów i obejmującej probabilistyczne oraz czasowe kryteria wystąpienia sytuacji krytycznej w złożonych systemach technicznych, głównie komputerowych.

Główny aspekt pracy dotyczy nowych metod i środków projektowania, analizy, modelowania komputerowych systemów srk. Autor poparł to własnymi przykładami projektowania i analizy systemów oraz zaproponował własny, oryginalne metody weryfikacji.

3. Ocena znaczenia i aktualności problematyki rozprawy

Aktualnie w państwach Unii Europejskiej obowiązują normy i zalecenia dotyczące projektowania , wdrażania i eksploatacji komputerowych (elektronicznych) systemów srk. Dla bezpiecznych komputerowych systemów sterowania w kolejnictwie są to standardy:

- Norma PN-EN 50126:2002 (U) Zastosowania kolejowe. Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa (RAMS),
- Norma PN-EN 50129:2007 Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem,

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

W rozproszonych, zdecentralizowanych systemach srk istotną rolę ze względu na bezpieczeństwo i poprawne funkcjonowanie systemu odgrywa transmisja, której niezawodność definiuje dla każdego poziomu SIL wartość THR, co przedstawia:

- Norma PN-EN 50159:2011 (U) Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Łączność bezpieczna w systemach transmisyjnych.

Dodatkowo bezpieczeństwo systemów srk powinny zapewnić procedury analizy bezpieczeństwa przedstawione jako następujące standardy:

- Norma PN-EN 60812:2009 Techniki analizy nieuszkadzalności systemów. Procedura analizy rodzajów i skutków uszkodzeń (FMEA),
- Norma PN-EN 61025:2007 Analiza drzewa niezdatności (FTA),
- Norma PN-EN 61078:2006 Techniki analizy niezawodności – Metoda schematów blokowych niezawodności oraz metody boolowskie,
- Norma PN-IEC 60300-3-9:1999 Analiza ryzyka w systemach technicznych.

Są to typowe standardy techniczne, w sposób statyczny uwzględniające charakterystyki niezawodnościowe - intensywności uszkodzeń elementów, urządzeń i podsystemów najczęściej nadmiarowych, oraz czas detekcji uszkodzeń pojedynczych i wielokrotnych.

Dodatkowo w systemach srk należy uwzględnić oddziaływania EMC i warunki środowiskowe, w tym klimatyczne.

Autor z oczywistych poziomów ograniczył się w rozprawie do trzech fundamentalnych norm 50 12x (wszystkie pozostałe normy zostały uwzględnione w opracowanych, wdrożonych i dopuszczonych do eksploatacji systemach srk w których doktorant był współautorem).

Przy analizie bezpieczeństwa sprzętu zastosowanego w systemie srk podstawowym, obligatoryjnym kryterium jest THR - tolerowany poziom ryzyka będący zredukowaną intensywnością systemu nadmiarowego uwzględniający czas detekcji usterki w systemie. Autor w poprawny sposób przeprowadził analizę tego wskaźnika w wdrożonych do eksploatacji systemach (załącznik C).

Niekwestionowanym, oryginalnym osiągnięciem Autora jest specyfikacja funkcjonalna systemu srk na poziomie abstrakcyjnym w postaci deterministycznych automatów o skończonej liczbie stanów (co gwarantuje matematyczną poprawność) oraz ich implementacja w postaci modułów programowania obiektowego przy zastosowaniu kwalifikowanych narzędzi zalecanych w normie PN-EN 50 128 (w tym systemów operacyjnych czasu rzeczywistego.

Autor zapewnia integrację bezpiecznego sprzętu i oprogramowania poprzez zalecany w normie PN-EN 50126 schemat V, przy zastosowaniu własnych procedur testowania i wykrywania reakcji systemu na usterki.

Praca Autora wychodzi na przeciw wymaganiom określonym we wspomnianych fundamentalnych normach dotyczących zasad projektowania, wdrażania i eksploatacji bezpiecznych systemów srk. Tematyka poruszona przez Autora w rozprawie praktycznie nie była podejmowana w Polsce. Znane mi publikacje (również w UE) nie podejmują tematyki

formalnej specyfikacji oprogramowania dla uwarunkowanych bezpieczeństwem systemów srk, chociaż metoda jest szczególnie zalecana we wspomnianej normie PN-EN 50 129.

4. Ocena strony edytorskiej rozprawy

Strona edytorska przedstawionej rozprawy jest poprawna. Układ tekstu jest przejrzysty a materiał ilustracyjny przygotowany poprawnie (rysunki, wykresy i tabele są wykonane niezwykle starannie i zamieszczone w sposób podkreślający zamierzenia Autora). Praca zawiera stosowne odniesienia do pozycji literatury, a także do zamieszczonego materiału ilustracyjnego.

Należy podkreślić bardzo dobrą stronę graficzną wszystkich zamieszczonych diagramów, grafów automatów oraz fotografii ilustrujących wdrożeniowy dorobek Autora. Pozwala to na łatwą analizę opisanych w ten sposób problemów.

Podczas czytania nie stwierdza się obecności błędów, wszystkie zastosowane skróty zostały wyjaśnione, terminy fachowe pochodzące z języka angielskiego zostały prawidłowo przetłumaczone. Wszystkie wzory zamieszczone w pracy są prawidłowo przedstawione i skomentowane, ich czytelność i poprawność matematyczna nie budzi zastrzeżeń. Pewne drobne błędy literowe nie mają żadnego wpływu na stronę merytoryczną pracy.

5. Ocena układu rozprawy

Rozprawa składa się z 7 rozdziałów, wykazu literatury oraz 6 załączników. Na wstępie Autor przedstawił:

- słownik pojęciowy, w którym zostały określone pojęcia z dziedziny srk, niezawodności i komputerowych systemów sterowania
- wykaz najważniejszych zmiennych, które zostały wykorzystane w opisie formalnym systemu srk
- wykaz najważniejszych funkcji występujących w przedstawianej metodzie.

Rozdział 1 jest wprowadzeniem w tematykę bezpiecznych systemów srk. Przedstawiona ewolucja systemów srk dotyczy przejścia z układów przekaźnikowych do realizacji bezpiecznych sterowników komputerowych.

W sformułowanym w tym rozdziale problemie Autor założył, że można za pomocą ogólnie dostępnych technologii informatycznych zbudować oryginalny i bezpieczny oraz ekonomicznie uzasadniony komputerowy system sterowania ruchem kolejowym. Została też postawiona teza, że można zbudować system sterowania ruchem kolejowym spełniający obowiązujące wymagania bezpieczeństwa na poziomie SIL4 przy wykorzystaniu standardowych komponentów automatyki. Następnie przedstawił tezę pomocniczą mówiącą, że realizowany bezpieczny system automatyki srk będzie oparty o ogólnie dostępne elementy automatyki przy zastosowaniu specjalizowanych, bezpiecznych elementów wykonawczych stanowiących integralne wyposażenie modułów wejścia – wyjścia systemu. Realizacja tezy głównej (oraz pomocniczej) stanowi cel pracy, którego osiągnięcie potwierdzi słuszność obu tez.

Postawiona teza chociaż wydaje się oczywista (przecież obecnie wszystkie realizowane na świecie systemy srk są oparte na bezpiecznych sterownikach komputerowych), to jednak metoda realizacji takich systemów zaproponowana przez autora jest oryginalna i nowatorska w warunkach kolejnictwa polskiego.

W Rozdziale 2 Autor charakteryzuje system srk na bazie ogólnej teorii systemów (podział na powiązane ze sobą warstwę logiczną i fizyczną stanowiące system informatyczny). Pod względem funkcjonalnym system srk jest zdekomponowany na funkcje nie niosące ryzyka, funkcje o podwyższonym ryzyku oraz funkcje specjalne (powodujące zagrożenie – wystąpienie sytuacji katastroficznej). Autor zgodnie z zaleceniami normy PN –EN 50 126 wprowadza model V – integrację sprzętu i oprogramowania na poziomie testowania systemu. Dla nowoprojektowanego systemu srk Autor zaproponował schemat postępowania , którego główne punkty są następujące:

- sformułowanie założeń i opis nieformalny systemu srk,
- przedstawienie systemu srk jako złożonego ze względu na bezpieczeństwo systemu informatycznego (przyjęcie wskaźnika MTBF jako podstawowego kryterium wyboru sprzętu),
- wybór systemu operacyjnego oraz zasada tworzenia bezpiecznego oprogramowania z wykorzystaniem innych poza normą PN – EN 50 128 zaleceń (np. standardu MISRA),
- testowanie i uruchamianie systemu,
- walidacja i opracowanie dowodu bezpieczeństwa systemu.

Przedstawiony sposób projektowania i implementacji systemu srk uwzględnia cykl życia systemu bezpiecznego, zalecany dla systemów automatyki kolejowej.

W rozdziale tym zostały poprawnie przedstawione podstawowe kryteria systemu bezpiecznego: Tolerowalny Poziom Ryzyka (THR) oraz dostępność/gotowość systemu (A). Podane w pracy wartości dostępności różnych systemów (podzielonych na klasy) świadczą o bardzo dobrej znajomości przez Autora tych zagadnień.

Autor przedstawił swoją metodę MM , ściśle nawiązującą do obowiązujących norm PN – EN 50 12x. (W pewnej części normy te nie są ściśle obligatoryjne, podane zalecenia pozwalają na pewną własną realizację podanych rekomendacji.)

Rozdział 3 to ogólny opis systemu srk, będący podstawą specyfikacji formalnej na poziomie deterministycznego, automatu abstrakcyjnego. Został tutaj wprowadzony sekwencyjny (cykliczny) sposób przetwarzania informacji z uwzględnieniem systemu uwarunkowanego bezpieczeństwem, jakim jest system srk. (Wiąże się to z wprowadzeniem stanów dopuszczalnych, kontrolowanych, w których może przebywać system srk – przypisanych do zdefiniowanych obiektów (stanowiących podstawowe struktury danych).

Osobnym, zasługującym na szczególną uwagę jest formalna specyfikacja systemu srk i związany z nią model matematyczny zbudowany na bazie teorii automatów o skończonej liczbie stanów (FSA). Autor oparł się tutaj na cenionej w środowisku srk pracach prof. W. Zabłockiego z Wydziału Transportu Politechniki Warszawskiej, co zapewniło precyzyjny i spójny pod względem formalnym zapis. Potraktowanie systemu srk jako złożenie dwóch podsystemów, statycznego będącego odwzorowaniem topografii obiektów i ich powiązań w tablicy przebiegów, oraz dynamicznego uwzględniającego realizację przebiegów przy uwzględnieniu zmiany stanów obiektów (odcinków izolowanych, położenia zwrotnic, odwzorowania sygnalizatorów itp.) jest intuicyjne i zrozumiałe dla specjalistów z dziedziny srk. Należy zwrócić uwagę na zapewnienie matematycznej poprawności zarówno struktur danych jak i algorytmów realizujących wszystkie funkcje systemu srk (kompletności danych, powiązań obiektów, zapisu przebiegów itp.). Kwestie te wyjaśnia zamieszczony przykład zapisu danych statycznych rzeczywistego obiektu oraz prawidłowej realizacji przebiegów w postaci struktur dynamicznych.

Oryginalna jest w tym przypadku propozycja takiej specyfikacji systemu na poziomie automatów abstrakcyjnych, wprawdzie Autor nie podaje sposobu udowodnienia formalnej poprawności takiego zapisu, ale przedstawiony w następnej części rozprawy sposób weryfikacji takiej specyfikacji zapewnia pełną poprawność (tzw. metody semi-formalne, *ang.* semi-formal methods).

W rozdziale 4 Autor przedstawił charakterystykę automatów wykonawczych realizujących funkcje systemu srk. Została przedstawiona zasada tworzenia kolejnego cyklu sterowania:

- automat sterowania i kontroli wyjść fizycznych,

- automat dekodowania stanu i kontroli wejść fizycznych,

- automat kontroli niezajętości toru.

W Rozdziale 5 Autor podaje zasady weryfikacji i walidacji projektowanego systemu srk poprzez odpowiednie procedury testowania. Dotyczy to sprawdzenie spełnienia założeń, testowanie oprogramowania, testów służących wykrywania błędów, testów służących wykrywania przyczyn błędów. Autor odniósł sie też do oszacowania niezawodności i jakości oprogramowania, ale metody takie nie gwarantują oprogramowania całkowicie wolnego od błędów – zapewnia to matematyczna teoria formalnej poprawności oparta na specyfikacji formalnej przeniesionej na poziom języka abstrakcyjnego i implementacji poprzez certyfikowane narzędzia (kompilator, system operacyjny). Przedstawione przez Autora różne procedury testowania prowadzą do weryfikacji i walidacji projektowanego systemu, zaś zamieszczony przykład sprawdzenia pod tym kątem systemu WTUZ (współautorstwa doktoranta), który jest dopuszczony do eksploatacji w metrze warszawskim potwierdza poprawność i utylitarność metody zaproponowanej przez doktoranta.

Rozdziały 6 i 7 to podsumowanie metody zaproponowanej przez Autora i wykazanie postawionej na początku tezy oraz realizacji założonego celu. Szkoda, że autor nie odniósł sie w tym miejscu do innych metod projektowania bezpiecznych systemów srk (realizowanych przez wiodące firmy automatyki kolejowej w UE), oraz do współczesnych publikacji pokazujących tendencje rozwojowe na świecie w dziedzinie oprogramowania rozproszonych systemów srk (ERTMS i ruchomy odstęp blokowy, otwarta transmisja bezprzewodowa, itp).

Należy też wspomnieć o 6 dodatkach, bardzo dobrze ilustrujących zagadnienia omawiane w rozprawie i potwierdzających wysoki profesjonalizm autora w dziedzinie.

6. Ocena realizacji postawionej tezy badawczej

Autor sformułował następujący problem badawczy: „można za pomocą ogólnie dostępnych technologii informatycznych zbudować oryginalny i bezpieczny oraz ekonomicznie uzasadniony komputerowy system sterowania ruchem kolejowym”

Przedstawił też tezę, z której wynika, że „stosując metodę MM można zbudować system sterowania ruchem kolejowym spełniający obowiązujące wymagania bezpieczeństwa na poziomie SIL4 przy wykorzystaniu standardowych komponentów automatyki”. Z tezą główną wiąże się teza pomocnicza: „można zrealizować bezpieczny system automatyki srk w oparciu o ogólnie dostępne elementy automatyki przy zastosowaniu specjalizowanych, bezpiecznych elementów wykonawczych stanowiących integralne wyposażenie modułów wejścia – wyjścia systemu”.

Autor sformułował cel rozprawy związany z wykazaniem poprawności tezy – „opracowanie metody projektowania i tworzenia sytemu komputerowego srk oraz wykazanie, że można opracować bezpieczny, tani i nowoczesny komputerowy system srk o poziomie bezpieczeństwa SI-4 z zastosowaniem metody COTS, czyli zbudowany z komponentów sprzętu komputerowego i automatyki dostępnych na rynku".

Na pierwszy rzut oka zarówno problem badawczy, teza jak i cel rozprawy wydają się oczywiste (przecież jest wiele współczesnych komputerowych systemów srk spełniających wymagania dla poziomu SIL-4 dopuszczonych do eksploatacji w kolejnictwie UE, zbudowanych z typowych komponentów spełniających wymagania norm EN 50 12x). Ale po wnikliwym przeczytaniu rozprawy i zaznajomieniem się z imponującym dorobkiem wdrożeniowym Autora należy stwierdzić:

- Bezsprzecznie dużym osiągnięciem Autora jest pokazanie specyfikacji systemu srk na poziomie automatów abstrakcyjnym (przy zastosowaniu precyzyjnego, sprawdzonego i poprawnego formalizmu zaproponowanego przez prof. Zabłockiego). Pozwala to wykluczyć juz na poziomie wstępnego opisu błędy i niejednoznaczności danych statycznych (odnoszących sie do obiektów srk), ale przede wszystkim błędy w dynamicznym opisie realizowanych funkcji komputerowego systemu srk.
- Niewątpliwym osiągnięciem Autora w proponowanej metodzie jest wprowadzenie profesjonalnych kryteriów wyboru sprzętu opartych na teorii niezawodności i uwzględnieniu parametrów czasowych (Tolerowanego Poziomu Ryzyka THR opartego na intensywności uszkodzeń poszczególnych modułów oraz czasie reakcji i detekcji uszkodzeń, oraz dostępności systemu A).
- Oryginalnym są autorskie metody testowani, weryfikacji i walidacji systemu.

Obowiązujące normy PN – EN 50 12x nie są w całości obligatoryjne, stąd też wiele rozwiązań systemów jest oryginalnym, chronionym, opracowaniem zespołów autorskich firm produkujących systemy automatyki kolejowej. Stąd też wynika oryginalność metody projektowania systemów srk przedstawionych w rozprawie.

W celu wykazania poprawności postawionej tezy Autor w dalszej części pracy przeanalizował zasady poprawnej specyfikacji systemu. W tym celu opracował modele na bazie teorii automatów dla wybranych przykładów, i co ważne pokazał zasady implementacji takich systemów (WSKR i WTUZ). Ostatecznie badania laboratoryjne i eksploatacyjne potwierdziły poprawność metody

Należy stwierdzić, że w ten właśnie sposób teza ta została udowodniona w pracy. Jest to praktycznie metoda precyzyjnego i poprawnego zdefiniowania systemu i jego specyfikacji oraz podanie zasad implementacji bezpiecznego, zgodnego z obowiązującymi wymaganiami systemu srk.

7. Ocena metodyczna i merytoryczna rozprawy

Tematyka recenzowanej rozprawy dotyczy bardzo ważnej dziedziny jaką jest projektowanie uwarunkowanych bezpieczeństwem komputerowych systemów srk.

Zaproponowana specyfikacja na bazie deterministycznych automatów abstrakcyjnych o skończonej liczbie stanów, zalecana w normie PN – EN 50 128, jest przedstawiona w sposób poprawny, a zamieszczone liczne przykłady dobrze ilustrują zamierzenia Autora. Dotyczy to również wszystkich innych istotnych aspektów bezpiecznego oprogramowania systemów srk

(np. wybór kompilatora, języka programowania, systemu operacyjnego, testowania modułów, itp.).

Przedstawiona metoda projektowania bezpiecznych komputerowych systemów srk jest zgodna z obowiązującymi regulacjami, bardzo dobrze wykorzystuje poza tym osiągnięcia ogólnej teorii systemów, teorii sterowania, teorii niezawodności, a przede wszystkim teorii sterowania ruchem kolejowym.

Zaproponowana w pracy terminologia dotycząca zarówno sterowania ruchem kolejowym jak komputerowych systemów sterowania czasu rzeczywistego jest poprawna i zgodna z obowiązującymi w tym zakresie wytycznymi.

Wszystkie modele zamieszczone w pracy są poprawne pod względem formalnym, dotyczy to również schematów i diagramów związanych z wprowadzonymi automatami i sposobem ich realizacji w systemie komputerowym.

Należy w tym miejscu podkreślić dużą umiejętność Autora w połączeniu skomplikowanego aparatu matematycznego z intuicyjnością opisu złożonych systemów technicznych (uwzględniających specyfikę systemów srk, wymagania i obowiązujące normy) oraz umiejętność analizy parametrów niezawodnościowych (probabilistycznych i czasowych) przy ocenie sprzętu.

8. Główne walory i cechy pozytywne rozprawy

Podstawową zaletą recenzowanej rozprawy jest podjęcie przez Autora bardzo ważnego tematu związanego z wprowadzaniem nowych technologii informacyjnych do tematyki srk, jako nadbudowę na istniejące rozwiązania komputerowych systemów sterujących. Autor w sposób naukowy podszedł zarówno do problemu formalnej specyfikacji oprogramowania i jego poprawnej implementacji, ale też do uwarunkowanej bezpieczeństwem konfiguracji sprzętu. Całość dopełnia metodyka weryfikacji i walidacji takich systemów poparta przez Autora dużym doświadczeniem i praktyką projektowania i wdrażania takich systemów w warunkach kolejnictwa polskiego.

Zastosowana w rozprawie metoda jest faktycznie, oryginalnym i nowatorskim podejściem nie tylko do problemu bezpiecznego, zgodnego z wymaganiami komputerowego systemu srk, ale też do analizy ich bezpieczeństwa i gotowości/dostępności.

Niekwestionowanym osiągnięciem Autora jest zastosowanie teorii automatów do specyfikacji funkcjonalnej systemu srk oraz do implementacji na bazie programowania obiektowego. Zaproponowany sposób i zaimplementowana metoda MM poparta przykładami wdrożonych (i z powodzeniem od wielu lat eksploatowanych systemów potwierdzają bardzo dobrą znajomość przez Autora zagadnień współczesnej inżynierii oprogramowania oraz komputerowego sterowania procesami.

Zarówno zaproponowana metoda projektowani a przede wszystkim implementacja tej metody stanowią oryginalny i niekwestionowany dorobek Autora.

9. Zagadnienia dyskusyjne i problemy do wyjaśnienia

W pracy Autor nie odniósł się do następujących kwestii:

- Kto w kraju i za granicą stosował opis teorii automatów do specyfikacji formalnej systemu srk, czy innych rozwiązań automatyki kolejowej (w bibliografii brak jest pozycji na ten temat).
- Czy zaproponowaną specyfikację można zastosować do innych rozwiązań sprzętowych, np modułów realizowanych w formie układów FPGA (są takie rozwiązania w kolejnictwie UE i polskim).

Do specyfikacji systemu autor ogranicza się do teorii automatów, co odpowiada sytuacji sprzed 20 lat, kiedy powstawały normy dotyczące bezpiecznych, komputerowych systemów srk. W przypadku bardziej złożonych (też rozproszonych) systemów automatyki kolejowej stosuje się inne modele oparte m. in. na Procesach Markowa (MP), których zastosowanie do analizy bezpieczeństwa m. in. w kolejnictwie znakomicie przedstawili J. Jaźwinski i K. Ważyńska – Fiok. (MP). Pozwala to na oszacowanie probabilistycznych i czasowych kryteriów bezpieczeństwa związanych z przebywaniem systemu w określonych stanach (zwłaszcza tych niebezpiecznych, czy katastroficznych). W obecnej chwili znakomita większość prac badawczych dotyczących ERTMS/ETCS/GSM-R stosuje takie podejście do analizy bezpieczeństwa i funkcjonalności. Dotyczy to również takich modeli w których stosuje się Kolorowane Sieci Petriego (CPN) czy Probabilistyczne Drzewa Niezdatności z Zależnościami czasowymi (PDNZC). Dotyczy to np. analizy bezpiecznej transmisji informacji w systemach zmiennego odstępu blokowego.

Innym zagadnieniem staje się wykorzystanie języka UML do specyfikacji procesów, w tym uwarunkowanym bezpieczeństwem (można tutaj sięgnąć chociażby do prac A. Kochana i M. Sumiły). W przypadku specyfikacji modeli zdefiniowanych w formie PM, CPN czy PDNZC można w prosty sposób poza kodem wynikowym otrzymać np. moduł wynikowy do symulacji Monte Carlo.

To są aktualne trendy w badaniach procesów (w tym występujących w systemach srk) i dobrze byłoby się do nich odnieść, chociażby we wstępie lub podsumowaniu.

W liczącej 128 pozycji bibliografii 56 pozycji stanowią normy, wytyczne, dokumentacje, słowniki i materiały szkoleniowe. Nie wszystkie takie dokumenty, np. normy dotyczące EMC znajdują uzasadnienie w pracy.

10. Podsumowanie

Podsumowując całość przedstawionych rozważań stwierdzam, że rozprawa doktorska mgr inż. Mariusza Maciejewskiego wnosi istotne elementy poznawcze do dziedziny komputerowych systemów srk, w zakresie konfiguracji bezpiecznego systemu, specyfikacji formalnej funkcji systemu, analizy bezpieczeństwa oraz weryfikacji i walidacji. przedstawioną przez Autora metodę projektowania i implementacji bezpiecznego systemu srk można uznać za oryginalną.

Do głównych osiągnięć Autora zaliczyłbym:

- bardzo dobrą znajomość ogólnych zagadnień związanych z projektowaniem bezpiecznych, komputerowych systemów srk,
- bardzo dobrą znajomość teorii automatów w zakresie modelowania funkcji systemu srk,
- bardzo dobrą znajomość teorii sterowania i technologii informatycznych w zakresie projektowania i implementacji systemów czasu rzeczywistego,

- interesujące, dobrze ilustrujące przykłady oparte na wieloletniej praktyce.

Należy też podkreślić poza tym utylitarny charakter rozprawy, prezentowana metoda może być rekomendowana jako uzupełnienie obowiązujących norm w zakresie projektowania i wdrażania komputerowych systemów srk.

Praca jest wartościowa i kwalifikuje się do opublikowania w formie monografii dotyczącej nowych metod projektowania i implementacji komputerowych systemów srk, ale też jako podręcznik przeznaczony dla inżynierów i specjalistów oraz studentów zajmujących się tą tematyką w kolejnictwie polskim. Pomimo pewnych uwag o charakterze polemicznym pragnę stwierdzić, że recenzowana rozprawa doktorska spełnia wszystkie wymogi stawiane rozprawom doktorskim w świetle obowiązującej Ustawy o stopniach i tytule naukowym oraz o stopniach i tytule w zakresie sztuki z dnia 14 marca 2003 r. (z późniejszymi zmianami).

Uważam ponadto, że recenzowana praca zasługuje na wyróżnienie.

Mając powyższe na uwadze wnoszę o dopuszczenie mgr inż. Mariusza Maciejewskiego do publicznej obrony recenzowanej rozprawy na Wydziale Transportu Politechniki Warszawskiej.

(Andrzej Lewiński)