Radom, 20..06. 2022

Prof. dr hab. inż. Andrzej Lewiński
Wydział Transportu i Elektrotechniki,
Instytut Automatyki i Telematyki Transportu
Uniwersytet Technologiczno – Humanistyczny im. K. Pułaskiego w Radomiu
e-mail: a.lewinski@uthrad.pl

Recenzja rozprawy doktorskiej mgr inż. Dariusza Szmela pt.
„Metoda analizy bezpieczeństwa komputerowych systemów sterowania ruchem kolejowym"

Promotor: prof dr hab. inż. Jacek Skorupski
Warszawa 2022
Dziedzina: Nauki Inżynieryjno - Techniczne,
Dyscyplina: Inżynieria Lądowa i Transport

1. Podstawa opracowania, przedmiot recenzji

Podstawą recenzji jest pismo Id; WTBD.521.DR.103.2022 z dnia 19.05.2022 Przewodniczącego Rady Dyscypliny Inżynieria Lądowa i Transport Politechniki Warszawskiej, Dr hab. inż. Konrada Lewczuka, Profesora Uczelni z prośbą o wykonanie recenzji rozprawy doktorskiej mgr inż. Dariusza Szmela pt. „Metoda analizy bezpieczeństwa systemów sterowania ruchem kolejowym". Rozprawa zawiera 198 stron, w tym 7 załączników (39 stron).

Rozprawa doktorska przedstawia propozycję zastosowania racjonalnej i efektywnej metodyki analizy i oceny bezpieczeństwa w komputerowych systemach sterowania ruchem kolejowym. Metoda oparta na modelowaniu procesów związanych (w tym bezpieczeństwa) poprzez zastosowanie kolorowanych sieci Petriego – narzędzia matematycznego umożliwiającego analizę uwzględniającą różne zdarzenia, w tym warunki środowiskowe i czynnik ludzki. W niniejszej pracy autor przedstawił propozycję racjonalnej i efektywnej metodyki analizy i oceny bezpieczeństwa opartej o model systemu srk z wykorzystaniem formalnych metod analitycznych.

2. Teza i cel pracy

W rozdziale pierwszym utor określił następującą tezę pracy: **„Zastosowanie opracowanej metody identyfikacji źródeł zagrożeń, utworzonych klas uszkodzeń oraz analizy opartej na modelu struktury systemu srk, procesów ruchowych i jego otoczenia z zastosowaniem znakowanych, kolorowanych, hierarchicznych i czasowych sieci Petriego zapewnia w sposób racjonalny przeprowadzenie analizy bezpieczeństwa komputerowych systemów srk uwzględniając złożony charakter czynników wpływających na jego prawidłowe działanie".** Została też zdefiniowana teza pomocnicza" Zaproponowana metoda zapewnia

formalną weryfikację poprawności modelu umożliwia też cenę ilościową celów bezpieczeństwa komputerowych zgodnie z obowiązującymi w UE standardami.

Opracowanie modelu i jego analiza uwzględnia głównie zadaszenia na przejazdach kolejowych różnych kategorii. Zastosowanie w tym celu metod formalnych opartych o matematyczne zależności zapewnia przeprowadzenie formalnego dowodu poprawności zastosowanych rozwiązań. Sieci Petriego są w normach CENELEC (50128)zalecane do analizy bezpieczeństwa

Dla potrzeb opracowania modelu systemu w postaci sieci Petriego do opisu funkcjonalności oraz wymiany informacji z otoczeniem rozpatrywanego systemu autor wykorzystał program Capella i język SysML, oraz system wymiany informacji (SWI) dyżurnego ruchu i dróżnika przejazdowego.

Autor określił cel rozprawy- **„Przedstawienie propozycji zastosowania racjonalnej i efektywnej metodyki analizy bezpieczeństwa w komputerowych systemach sterowania ruchem kolejowym"**. Opracowany model, może zostać zastosowany do opisu struktury systemu srk oraz procesów ruchowych posłuży również do modelowania otoczenia i interakcji poszczególnych komponentów oraz identyfikacji źródeł zagrożeń z uwzględnieniem zależności czasowych, Model został wykorzystany też do analizy transmisji oraz czynności obsługowych zgodnie z wymaganiami najwyższego poziomu bezpieczeństwa SIL4.

Autor pracował algorytm realizacji (opracowanie modelu, jego analizę i weryfikację) w celu wykazania poprawności tezy i celu rozprawy

3. Ocena zawartości rozprawy.

W rozdziale drugim, autor przedstawił Zagadnienia bezpieczeństwa sterowania ruchem kolejowym, czyli aktualny tan regulacji UE i CENELEC w zakresie bezpieczeństwa systemów, podsystemów i urządzeń sterowania ruchem kolejowym. Należy podkreślić oryginalne podejście do problematyki w transporcie kolejowym (kultura bezpieczeństwa) – jako sposób na eliminację zagrożeń i potencjalnych wypadków związanych z działaniami rutynowymi organizacji i służącymi do przeciwdziałania im poprzez spełnienie odpowiednich wymagań. oraz jak największa automatyzacja pracy w celu eliminacji człowieka i błędów ludzkich w trakcie procesu sterowania.

Autor opisał proces identyfikacji zagrożeń na początkowym etapie realizacji systemu., bardzo dobrze scharakteryzował obowiązujące (obligatoryjne lub rekomendowane) metody identyfikacji zagrożeń, analizy i oceny ryzyka takie jak HAZOP, FTA czy FMEA. Szczególną uwagę Autor poświęcił procesom Markowa pozwalającym m. in. określić prawdopodobieństwo wystąpienia stanu krytycznego związanego z utratą kontroli nad systemem.. takie modelowanie systemu jest zalecane w normach CENELEC, pomimo złożonego aparatu matematycznego.

Autor powołał się ł też inne zalecane metody (m. in. PHA - Preliminary Hazard Analysis, RRA - Rapid Ranking Analysis),.stosowane w innych systemach uwarunkowanych bezpieczeństwem.

Rozdział ten stanowi wprowadzenie w zagadnienia bezpieczeństwa systemów sterowania ruchem kolejowym, wymienione metody są rekomendowane do analizy bezpieczeństwa, nie tylko w kolejnictwie.

Rozdział 3, będący podstawą recenzowanej rozprawy doktorskiej przedstawia nową hybrydową metodę analizy bezpieczeństwa - to ocena bezpieczeństwa całego systemu. W tym

celu autor opracował model systemu srk wraz interfejsami oraz dynamiką działania w oparciu o znakowane, czasowe, kolorowe i hierarchiczne sieci Petriego oraz algorytm analizy.

Model w postaci sieci Petriego uwzględnia czasowe parametry brzegowe do przejść między stanami., a także wprowadzenie funkcji generujących liczby losowe w celu odwzorowania parametrów niezawodnościowych. Umożliwia to modelowanie oraz symulację (weryfikację) z uwzględnieniem współpracy człowieka – operatora z systemem srk. Przedstawiona metoda pozwala definiować sieci różniące się pewnymi właściwościami, ale istnieje jednak zbiór cech, które są dla tego rodzaju sieci wspólne.

Autor przedstawił bardzo dobrze sieci Petriego – sposób modelowania i analizę we wszystkich formach, w tym sieci kolorowanych zastosowanych w metodzie. W przykładach pokazane zostały scenariusze uwzględniające postępowanie człowieka z systemem. W modelu uwiedziony został aspekt prawdopodobieństwa błędnie wygenerowania funkcji opisującej zdarzenia losowe. Przedstawiono opis formalny modelu będącego adaptacją sieci Petriego dla potrzeb analiz i oceny bezpieczeństwa komputerowych systemów srk. Wykonano identyfikację zagrożeń i analizę bezpieczeństwa modelu komputerowego systemu sterowania ruchem kolejowym reprezentującą rzeczywistą architekturę istniejącego systemu. kolejowym. Ze względu na sposób przeprowadzonych operacji oraz wielomodułowość komponentów współpracujących przyjęto podział sieci na: instalacje, scenariusze, funkcje oraz bezpieczeństwo. Autor wykorzystał hierarchiczność sieci, można ją podzielić na podsieci, które będą połączone specjalnymi konstrukcjami tj. fuzje miejsc i tranzycje podstawienia.

Przedstawiona metoda, i związany z nią opis matematyczny oparty został o obszerne prace z tematyki siec iPetriego i teorii niezawodności i bezpieczeństwa. Wkład Autora w niniejszej rozprawie dotyczył matematycznego opisu struktury sieci wykorzystany do analizowanych problemów. Autor zdefiniował i opracował model zawierający scenariusze operacyjne niezbędne do wykonania analizy bezpieczeństwa opracowano w środowisku ARCADIA z wykorzystaniem narzędzie Capella (bardzo dobry przykład implementacja kroków metody związanych z opracowaniem modelu sieci Petriego i symulacją).

Należy podkreślić bardzo dobrą znajomość norm obowiązujących w UE, dotyczy to m.in., kryterium TFFR (ang. Tolearable Functional Failure Rate).

Rozdział ten potwierdza bardzo dobrą znajomość przez autora aparatu matematycznego – sformalizowanej specyfikacji procesów współbieżnych w postaci sieci Petriego, a zwłaszcza analizę zdarzeń z uwzględnieniem ich charakteru losowego.

W rozdziale 4 przeprowadzono eksperymenty z wykorzystaniem środowiska symulacyjnego w CPN Tools. Przeprowadzone symulacje potwierdzają prawidłowe działanie modelu w przypadku wybranego scenariusza., też wykazano poprawność działania modelu. (Model przechodził do odpowiednich stanów zgodnie z oczekiwaniami.). W ramach realizowanych zadań opracowano również modele środowiska operacyjnego w narzędziu Cappela za pomocą języka SysML. Zdefiniowano szczegółowe poziomy krytyczności uszkodzeń, które mogą mieć zastosowanie do analizy HAZOP, FMEA lub FMECA

W rozdziale 5 autor przedstawił weryfikację przedstawionego modelu, potwierdzają to wyniki badań związanych z zastosowaniem metody do analizy bezpieczeństwa systemu. Przy tworzeniu modelu głównego przyjęto możliwie jak najbardziej realne odzwierciedlenie rzeczywistej części systemu kolejowego wraz z działającym w tym środowisku systemem sterowania ruchem kolejowym. Autor zakłada, że stwierdzić, że możliwe jest uogólnienie modelu i poszczególnych sieci na grupy typowych i powtarzających się układów stacyjnych i ruchowych. Hierarchiczne sieci Petriego będą miały tutaj zastosowanie poprzez łączenie niehierarchicznych sieci (podsieci) w jeden duży model. Przedstawiono też analizę wyników

badań, wykazano przewagę zastosowania hybrydowej metody analizy bezpieczeństwa opartej o identyfikację zagrożeń metodą HAZOP oraz analizę modelu w postaci sieci Petriego. Metoda pozwala na identyfikację zagrożeń, których nie można w sposób racjonalny i pewny identyfikować innymi metodami, w szczególności w przypadku błędów powstałych w wyniku różnych zależności czasowych i sekwencji działania poszczególnych komponentów. Omówiono też wyniki spostrzeżeń i wnioski z przeprowadzonych eksperymentów.

W tym rozdziale autor dyskusję wyników badań, przeprowadził też ponowną ocenę przyjętych kryteriów do zaproponowanej metody analizy bezpieczeństwa opartej o sieci Petriego. Na podstawie przyjętych kryteriów najkorzystniejszą metodą z punktu widzenia racjonalnościi wiarygodności zastosowania jest metoda oparta o sieci Petriego. Wiąże się to zastosowaniem kolorowanych znakowanych czasowych i hierarchicznych sieci Petriego, co gwarantuje to bardziej szczegółowe wyniki w zakresie analizy bezpieczeństwa. Autor uważa że: koncepcja hierarchiczności sieci umożliwia modelowanie bardzo złożonych systemów, a możliwości symulacyjne oraz zastosowanie znakowania jest kolejną przewagą nad innymi metodami. Zastosowanie kolorowania rozszerza zbiór typów danych, które można zdefiniować w modelu, co jest odpowiednikiem definiowania typów danych w językach oprogramowania. Wykorzystanie znaczników czasowych oraz przedziałów czasowych znacznie zwiększa możliwości analizowania złożonych systemów, a możliwość wykorzystania funkcje generujących liczby losowe może zweryfikować pracę poszczególnych komponentów systemów oraz dobrać odpowiednich wartości współczynników niezawodności lub prawdopodobieństwa. Wynik przeprowadzonej weryfikacji wykonanej przez Autora wskazuje na brak stanów mogących doprowadzić do określonych zagrożeń.

Na podstawie przeprowadzonych badań można stwierdzić, że zastosowana metoda umożliwia przeprowadzenie racjonalnej analizy zagrożeń w analizie bezpieczeństwa.

W podsumowaniu (rozdział 6) autor potwierdził poprawność postawionej tezy oraz zrealizowanie celu pracy Ważnym elementem tej dyskusji są przede wszystkim istotne korzyści z zastosowania sieci Petriego. Metoda ta nie jest nowym rozwiązaniem w modelowaniu systemów technicznych również w obszarze sterowania ruchem kolejowym. Jednak przedstawiona w rozprawie hybrydowa metoda bezpieczeństwa zapewnia bardzo sprawne i bardzo szczegółowe odwzorowanie funkcjonowania modelowanego obiektu srk. Dotychczasowe prace nie przedstawiały pełnych możliwości użycia kolorowanych, hierarchicznych, czasowych, znakowanych sieci Petriego w aplikacjach związanych z transportem kolejowym. Autor przedstawił dwa kluczowe wnioski wynikające z przeprowadzonej analizy i badań symulacyjnych:

- Zastosowanie metody analizy bezpieczeństwa opartej o sieci Petriego umożliwia szczegółową identyfikację źródeł zagrożeń, w sposób racjonalny i kompleksowy. W szczególności istotne są tu takie właściwości sieci jak: możliwość zastosowania przedziałowych sieci czasowych, hierarchiczności sieci oraz kolorowych znaczników. Ponadto możliwości analityczne sieci Petriego oprócz typowych korzyści z projektowania opartego o model dynamiczny oraz symulacje umożliwiają analizę szczegółowych właściwości modelu charakteryzujących warunki poprawności działania systemów srk.

- Zastosowanie przedstawionej metody umożliwia określenie przewidywanego działania modelu i systemu srk w eksploatacji wpisując w model sieć bezpieczeństwa charakteryzującą już wcześniej zidentyfikowane zagrożenia oraz relacje i przejścia z innych stanów systemu. deterministyczne przejścia pomiędzy poszczególnymi stanami systemu, jednak możliwe jest również wprowadzenie funkcji losowych lub opartych o dany rozkład prawdopodobieństwa. wykorzystywanie danych rzeczywistych pozyskiwanych z obiektów będących w użyciu i

wprowadzania ich do modelu na przykład jako miejsca lub parametry graniczne dla przejść między tranzycjami.

Wartość utylitarna pracy to pokazanie sformalizowanej metody analizy bezpieczeństwa, zgodnej z wymaganiami obowiązujących standardów CENELEC, ale uwzględniający czynnik ludzki w scenariuszach operacyjnych . Jest to ważne z punktu projektowania współczesnych systemów srk. Autor przedstawił kierunki dalszych badań, które będą prowadzone w kierunku oceny ilościowych wymogów systemu bezpieczeństwa w odniesieniu do wyznaczonych przez zarządcę infrastruktury celów bezpieczeństwa.

Do pracy został dołączony wykaz literatury (liczący 124 pozycje (doktorant jest autorem lub współautorem 4 publikacji) oraz 7 załączników pokazujących metodologię zastosowaną w pracy.

4. Ocena strony edytorskiej rozprawy

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

W pracy nie stwierdziłem błędów redakcyjnych, wszystkie zastosowane skróty zostały wyjaśnione, terminy fachowe pochodzące z języka angielskiego zostały prawidłowo przetłumaczone, wzory zamieszczone w pracy są prawidłowo przedstawione i skomentowane, a ich czytelność i poprawność matematyczna nie budzi zastrzeżeń.

5. Poprawność i oryginalność postawionej tezy i stopniu w jakim została wykazana

Teza i cel pracy postawione przez doktoranta są poprawnie sformułowane i oryginalne (w analizie bezpieczeństwa systemów zarządzania i sterowania ruchem kolejowym nie są znane publikacje, w tym rozprawy naukowe stosujące taki aparat matematyczny).

Autor sformułował problem badawczy związany z opracowaniem metodologii analizy bezpieczeństwa w oparciu o sieci Petriego – sformalizowanego aparatu modelowania zdarzeń. Może to nie wynika z bezpośrednio z pracy, ale ten aparat matematyczny umożliwia modelowanie procesów współbieżnych, w tym równoległych, pozwala wykryć kolizje, kolejki i inne sytuacje krytyczne. Takie są sytuacje występujące w systemach sterowania ruchem kolejowym i Autor to potwierdził na wybranych przykładach.

Na tej podstawie została sformułowana teza i postawiony cel rozprawy. W ten sposób powstał system analizy bezpieczeństwa, który może być z powodzeniem wykorzystywany przy projektowaniu systemów zarządzania i sterowania ruchem kolejowym. Aspekty utylitarne wykorzystania systemu są przyszłościowe takie metody analizy (formalne lub semi-formalne) są rekomendowane w przyszłościowych systemach transportu kolejowego (zwłaszcza w kolejach dużych prędkości, gdzie czynnik ludzki jest mocno redukowany).

Bardzo ważnym aspektem pracy jest zastosowanie procesów stochastycznych jako czynnika losowego mającego wpływ na zdarzenia w transporcie kolejowym. Takie podejście zasługuje na uznanie, analiza poganistyczna jest zgodna z analizą bezpieczeństwa w transporcie kolejowym.

Teza główna została wykazana, podobnie jak został zrealizowany cel rozprawy. Zarówno problem badawczy, teza jak i cel rozprawy zostały właściwie określone. Bezsprzecznie dużym

osiągnięciem autora jest pokazanie nowych możliwości analitycznych (wspomaganych komputerowo) wykazania bezpieczeństwa nowoprojektowanych systemów srk.

6. Ocena metodyczna i merytoryczna rozprawy, ocena znaczenia i aktualności problematyki rozprawy

Tematyka recenzowanej rozprawy dotyczy bardzo ważnej dziedziny jaką jest projektowanie bezpiecznych systemów sterowania ruchem kolejowym. Wprawdzie obowiązują normy UE (CENELEC), ale spełnienie tych norm nie gwarantuje uwzględnienie poprawnych i bezpiecznych reakcji człowieka – operatora systemów i podsystemów srk. Autor zaproponował do analizy bezpieczeństwa metodę sformalizowaną opartą na sieciach Petriego. Takie matematyczne podejście gwarantuje wykrycie błędu na etapie projektu, ale też ilościowe wyznaczenia probabilistycznych i czasowych kryteriów bezpieczeństwa. Z weryfikowanego modelu systemu (urządzenia srk – człowiek/operator) można w prosty sposób przejść do modelu Markowa uwzględniającego zdarzenia losowe. Wyniki autora uzyskane w badaniach symulacyjnych potwierdzają tę metodologię.

Przedstawiona w rozprawie metodologii wspomagana komputerowym wspomaganiem (symulacje) jest aktualna, nawiązuje bezpośrednio do analizy bezpieczeństwa w innych dziedzinach uwarunkowanych bezpieczeństwem, takich jak transport lotniczy, kosmonautyka czy energetyka jądrowa.

Metoda analizy bezpieczeństwa przedstawiona w pracy jest oryginalna, wiele kroków przedstawionego algorytmu analizy ma charakter autorski wynikający z bardzo dobrej znajomości specyfiki systemów srk. Zaproponowana metoda oparta na sformalizowanej analizie bezpieczeństwa systemów srk z uwzględnieniem czynnika ludzkiego i losowego charakteru zdarzeń spełnia wymagania obowiązujące aktualnie normy (m. in. PN-EN 50 12x).

7. Główne walory i cechy pozytywne rozprawy

Podstawową zaletą recenzowanej rozprawy jest podjęcie przez Autora bardzo ważnego tematu związanego z wprowadzaniem metod matematycznych do analizy bezpieczeństwa systemów srk. Analiza bezpieczeństwa systemów strefowania ruchem kolejowym z uwzględnieniem interakcji z operatorem oraz losowego charakteru zdarzeń za pomocą sieci Petriego jest niekwestionowanym osiągnięciem autora. Zastosowany przez autora aparat matematyczny do analizy sytuacji krytycznych w funkcjonowaniu systemu jest unikatowy w kolejnictwie polskim, można to traktować jako formalne potwierdzenie analizy obligatoryjnie wynikającej z norm CENELEC.

Przedstawiona metodologia jest nowatorska, autor bardzo dobrze przedstawił kolejne kroki algorytmu, od zdefiniowania modelu procesu sterowania w formie sieci Petriego, poprzez analizę konfliktów i zagrożeń do symulacji w konkretnym środowisku. Należy bardzo dobrze ocenić przykłady, a szczególnie ich wizualizuje i odpowiednie komentarze.

Praca stanowi to istotny, niekwestionowany wkład doktoranta do nowoczesnych technologii w zarządzaniu i sterowaniu ruchem kolejowym. Zastosowana w rozprawie metoda jest faktycznie, oryginalnym i nowatorskim podejściem do problemu analizy bezpieczeństwa systemów sterowania ruchem kolejowym uwzględniającym czynnik ludzki i zdarzenia losowe zaproponowany aparat matematyczny faktycznie formalizujący analityczną analizę bezpieczeństwa jest pozytywnym aspektem rozprawy.

Zaproponowana metoda analizy bezpieczeństwa, a przede wszystkim algorytm opracowania modelu, ale wspomaganie komputerowe (symulacje) stanowią oryginalny i niekwestionowany dorobek Autora.

8. Zagadnienia dyskusyjne i problemy do wyjaśnienia, wskazanie głównych wad rozprawy, jej słabych stron oraz krytycznych uwag szczegółowych

Recenzent nie zgłasza problemów do wyjaśnienia, Ale autor nie podał ograniczeń stosowanej metodologii. Wprawdzie przy założeniu hierarchizacji sieci, należy zadać pytanie, czy sposób leczenia podsystemów uwzględnia ich autonomiczność (współbieżność). W związku z tym czy eksperymenty symulacyjne pozwalają na wykrycie konfliktów wynikających z niezależnych systemów sterowania. Wprawdzie większość systemów sterowania (hierarchicznych) nie dopuszcza współrzędności, ale przedstawiona metodologia pozwala na takie rozwiązanie.

9. Podsumowanie, w tym sformułowanie i uzasadnienie wniosku o dopuszczenie rozprawy doktorskiej do publicznej obrony, uzasadnienia wyróżnienia

Podsumowując całość przedstawionych rozważań stwierdzam, że rozprawa doktorska mgr inż. Dariusza Szmela wnosi istotne elementy do dyscypliny Inżynieria Lądowa i Transport w zakresie - bezpieczne systemy sterowania ruchem w transporcie kolejowym.

Przedstawioną przez autora metodę analizę bezpieczeństwa systemu sterowania ruchem kolejowym w oparciu o sformalizowany aparat matematyczny w postaci sieci Petriego jest oryginała, unikatową w skali kraju i wnosi istotne czynniki do projektowania takich systemów.

Praca jest wartościowa i kwalifikuje się do opublikowania w formie monografii dotyczącej nowych metod analizy bezpieczeństwa.

Dodatkowo rozprawa kwalifikuje się do wyróżnienia, w pracy zaprezentowano nowatorski aparat matematyczny (sieci Petriego) zastosowany do analizy bezpieczeństwa do tej pory nie stosowany przy analizie systemów srk, pokazano też na przykładach zalety przedstawionej metodologii w trudnych relacjach człowiek – system srk w wykrywaniu zagrożeń przy projektowaniu takich systemów przy uwzględnieniu losowego charakteru zdarzeń,

Stwierdzam, że recenzowana rozprawa doktorska spełnia wszystkie wymogi stawiane rozprawom doktorskim w świetle obowiązującej Ustawy z dnia 20 lipca 2018r. Prawo o szkolnictwie wyższym i nauce, w związku z tym wnioskuję o: **dopuszczenie rozprawy doktorskiej do publicznej obrony recenzowanej rozprawy przed Komisją Dyscypliny Inżynieria Lądowa i Transport na Politechnice Warszawskiej.**

(Andrzej Lewiński)