

Katarzyna TRZASKA

PROGRAMOWANIE BEZPIECZNYCH SYSTEMÓW STEROWANIA RUCHEM KOLEJOWYM W ASPEKCIE PRZEPISÓW NORMALIZACYJNYCH UNII EUROPEJSKIEJ

Streszczenie. W referacie przedstawiono problemy budowy bezpiecznego oprogramowania systemów sterowania ruchem kolejowych w aspekcie obecnego członkostwa Polski w strukturach Unii Europejskiej.

PROGRAMMING OF THE RAILWAY SAFETY CONTROL SYSTEMS IN THE ASPECTS OF EU REGULATIONS

Summary. This paper presents a problem of build the safety software of railway control system in the aspects of EU regulations.

1. WSTĘP

W artykule poruszone zostały problemy projektowania bezpiecznych systemów sterowania ruchem kolejowym w związku z integracją Polski ze strukturami Unii Europejskiej.

Podstawowymi regulacjami prawnymi, dotyczącymi systemów sterowania ruchem kolejowym, obowiązującymi do niedawna na obszarze Polski, były zalecenia opracowane w 1997 roku przez Zakład Sterowania Ruchem i Zasilania Centrum Naukowo – Technicznego Kolejnictwa (CNTK) w Warszawie „Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym”. Dodatkowo obowiązywała polska norma ZN-91/MTiGM-CBP-12 „Bezpieczeństwo systemów sterowania ruchem kolejowym”, opracowana w 1991 roku. Obecnie, po wstąpieniu Polski do struktur Unii Europejskiej na obszarze naszego kraju jako obowiązujące zostały przyjęte normy opracowane przez UIC i CENELEC.

2. REGULACJE PRAWNE OBOWIĄZUJĄCE W UNII EUROPEJSKIEJ

Podstawowymi zaleceniami normatywnymi, dotyczącymi zarówno sprzętu, oprogramowania, jak i standardów transmisji danych, opracowanymi w ramach prac CENELEC, są:

- Norma europejska PN-EN 50128: 2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Programy dla kolejowych systemów sterowania i zabezpieczenia (Railway Applications: Software for Railway Control and Protection Systems). Standard ten dotyczy projektowania bezpiecznego oprogramowania dla systemów kolejowych. Zawiera wykaz praktyk i metod, które powinny być stosowane w celu otrzymania niezawodnego i bezpiecznego produktu software'owego [3].
- Norma europejska PN-EN 50126: 2002 (U) Zastosowania kolejowe. Specyfikacja dostępności, niezawodności, podatności utrzymaniowej i bezpieczeństwa (Railway Applications: The specification and demonstration of reliability, availability, maintainability and safety (RAMS)), dotycząca ogólnych zasad powstawania systemów bezpiecznych wraz z ich podstawowymi parametrami, jakimi są: niezawodność, bezpieczeństwo, dostępność [2].
- Norma europejska PN-EN 50129: 2003 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem (Railway Applications: Safety Related Electronic Railway Control and Protection Systems), dotycząca konfigurowania komputerowego sprzętu sterującego dla systemów zależnościowych [1].
- Norma europejska PN-EN 50159-1: 2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 1: Łączność systemów bezpieczeństwa w układach otwartych (Railway Applications: Communication, signalling and processing systems. Part 1: Safety-related communication in opened transmission systems).
- Norma europejska PN-EN 50159-2: 2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 2: Łączność systemów bezpieczeństwa w układach zamkniętych (Railway Applications: Communication, signalling and processing systems. Part 2: Safety-related communication in closed transmission systems).

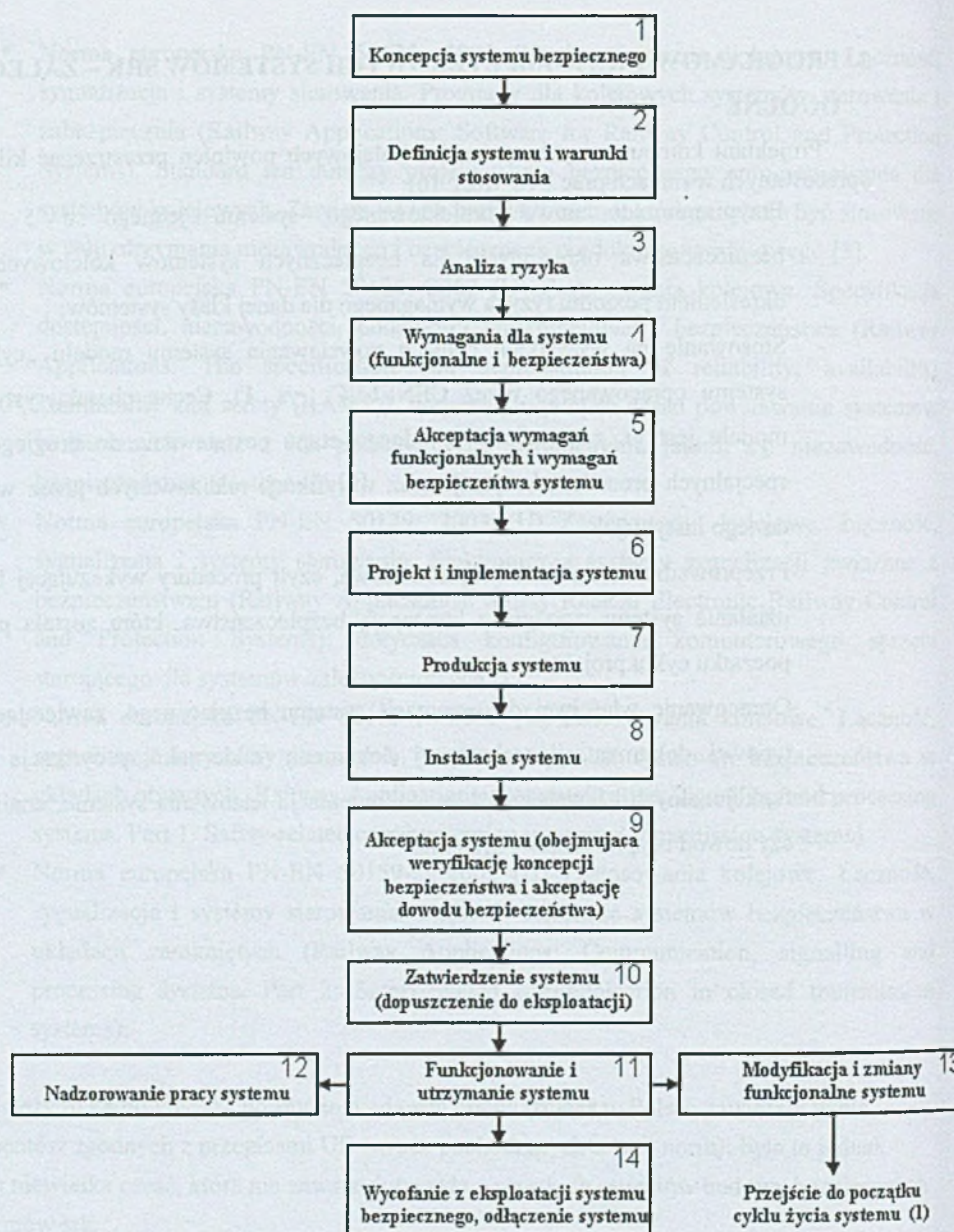
Należy tu nadmienić, że normy do niedawna obowiązujące w Polsce zawierały wiele elementów zgodnych z przepisami UE (wręcz pochodzących z tych norm); była to jednak tylko niewielka część, która nie zawsze dotyczyła wszystkich aspektów budowy bezpiecznych systemów srk.

Spośród innych standardów mających zastosowanie w programowaniu bezpiecznych systemów srk wymienić należy wytyczne Departamentu Obrony USA (tzw Military Handbooks). Normy te, chociaż nie są standardami obowiązującymi na obszarze Europy, są jednak często wykorzystywane w różnego rodzaju pracach związanych z systemami srk, głównie ze względu na szerokie omawianie wielu kwestii, które często w normach europejskich są traktowane marginalnie.

3. PROGRAMOWANIE KOMPUTEROWYCH SYSTEMÓW SRK – ZALECENIA OGÓLNE

Projektant komputerowych systemów kolejowych powinien przestrzegać kilku zaleceń opracowanych w ramach prac UIC-IRSE [6]:

- Przypisanie do nowo projektowanego systemu jednego z 5 poziomów bezpieczeństwa określonych dla bezpiecznych systemów kolejowych, wraz z określeniem poziomu ryzyka wymaganego dla danej klasy systemów;
- Stosowanie na wszystkich etapach powstawania systemu modelu „cyklu życia” systemu opracowanego przez CENELEC (rys. 1). Cechą charakterystyczną tego modelu jest to, że przejście z jednego etapu powstawania do drugiego wymaga specjalnych procedur akceptacji oraz weryfikacji realizowanych przez wyznaczone do tego instytucje;
- Przeprowadzenie dowodu bezpieczeństwa, czyli procedury wykazującej bezpieczne działanie systemu zgodnie z koncepcją bezpieczeństwa, która została przyjęta na początku cyklu projektowania;
- Opracowanie właściwej dokumentacji systemu bezpiecznego, zawierającej oprócz typowej dokumentacji technicznej dokumenty takie jak: specyfikacja wymagań funkcjonalnych i bezpieczeństwa, dokumentacja testowania systemu, analiza ryzyka czy dowód bezpieczeństwa systemu.



Rys. 1. "Cykl życia" systemu bezpiecznego [6]

Fig. 1. "Life cycle" of the safety system [6]

4. METODY ZALECANE PRZY PROJEKTOWANIU BEZPIECZNEGO OPROGRAMOWANIA

W zaleceniach dla systemów bezpiecznych sprzęt i oprogramowanie traktowane są jako niezależne części, które podlegają integracji dopiero na poziomie systemu. Metody zalecane przez UIC-IRSE dla części projektu związanej z oprogramowaniem przedstawione zostały w tabl. 1. Jak widać, stosowanie wielu metod zalecanych przy programowaniu nie jest jeszcze aktualnie obligatoryjne, jednak ich stosowanie pozwala na lepszą analizę oprogramowania.

Tablica 2 przedstawia specjalne metody zalecane (przez UIC i CENELEC) przy tworzeniu oprogramowania dla dwóch najwyższych poziomów bezpieczeństwa [3].

Tablica 1

Metody zalecane przez UIC-IRSE

Metody i procedury dla oprogramowania	Obligatoryjne	Szczególnie zalecane	Zalecane
1. Analiza skutków programu	x		
2. Statyczna analiza oprogramowania		x	
3. Dynamiczna analiza oprogramowania		x	
4. Analiza kodu programu		x	
5. Formalna specyfikacja programu		x	
6. Kompilator z gwarancją poprawności		x	
7. Języki algorytmiczne ('high level languages')		x	
8. Testowanie programu na docelowym sprzęcie	x		
9. Niezależność projektu od analizy	x		
10. Pełne testowanie każdej gałęzi programu	x		
11. Testowanie funkcjonalne modułów ('white box')		x	
12. Testowanie funkcjonalne	x		
13. Statyczna zgodność ze specyfikacją	x		
14. Dynamiczna zgodność ze specyfikacją		x	
15. Programowanie defensywne			x
16. Programowanie strukturalne	x		
17. Badania eksploatacyjne programu na prototypie		x	
18. Certyfikat jakości ISO 9001	x		
19. Określone zasady dokumentacji	x		

Tablica 2

Metody stosowane przy programowaniu systemów bezpiecznych (według CENELEC)

Etap/metoda	Specyfikacja wymagań dla oprogramowania	Specyfikacja architektury oprogramowania	Projekt oprogramowania	Weryfikacja oprogramowania	Integracja oprogramowania i sprzętu	Certyfikacja oprogramowania	Akceptacja/zatwierdzenie oprogramowania
Metody formalne	X		X				
Metody półformalne	X		X				
Programowanie strukturalne	X		X				
Programowanie defensywne		X					
Programowanie różnicowane		X					
Dane kodowane z detekcją błędów		X					
Kompilator z certyfikatem			X				
Testowanie typu „czarna skrzynka”				X	X	X	
Testowanie funkcjonalne				X	X	X	
Analiza statystyczna				X	X	X	
Analiza Drzewa Błędów (FTA)							X
Analiza Skutków Błędów (FMEA)							X
Analiza statyczna							X
Analiza dynamiczna							X

LITERATURA

1. PN-EN 50129: 2003 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Elektroniczne systemy sygnalizacji związane z bezpieczeństwem.
2. PN-EN 50126: 2002 (U) Zastosowania kolejowe. Specyfikacja dostępności, niezawodności, podatności utrzymaniowej i bezpieczeństwa.
3. PN-EN 50128: 2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Programy dla kolejowych systemów sterowania i zabezpieczenia.
4. PN-EN 50159-1: 2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 1: Łączność systemów bezpieczeństwa w układach otwartych.
5. PN-EN 50159-2: 2002 (U) Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Część 2: Łączność systemów bezpieczeństwa w układach zamkniętych.

6. Lewiński A.: Problemy oprogramowania bezpiecznych systemów komputerowych w zastosowaniach transportu kolejowego, Politechnika Radomska im. K. Pułaskiego, Monografia nr 49, Radom 2001.
7. Opracowanie CNTK, Zakład Sterowania Ruchem Kolejowym: Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym, Warszawa, luty 1998.

Recenzent: Doc. dr inż. Zbigniew Ginalski

Abstract

This paper presents a problem of build the safety software of railway control system. The hardware reliability analysis is based on well known methods in the reliability theory that mainly include the connection structure between subsystems, and devices or elements of the system. Analyzing the software there is a need to apply other methods of the probability estimation of the program correct execution. Creating acceptable programs depends of applying special procedures and programming methods (i.e. systematic, structural, defensive, or specified programming). According to UIC and CENELEC at each stage of the safe system software designing (beginning from specifications up to approving the conception) there is a necessity to apply sufficient analyses and methods of the software creation. Those elements are very important especially due to the EU expansion. The CENELEC standards and statements have been there already in use.

Praca wykonana w ramach: BW-443/RT4/2004.