MIĘDZYNARODOWA KONFERENCJA NAUKOWO-TECHNICZNA
TRANSPORT SZYNOWY-NAUKA-PRZEMYSŁ'99

ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
TRANSPORT z.36, nr kol.1429

Jerzy MIKULSKI
Marek SOBAŃSKI*)

BEZPIECZEŃSTWO SYSTEMÓW STEROWANIA RUCHEM KOLEJOWYM W ŚWIETLE WYMAGAŃ NORM CENELEC

Streszczenie. Artykuł prezentuje zagadnienia określania bezpieczeństwa systemów sterowania ruchem kolejowym w ujęciu europejskich norm CENELEC. Szczególną uwagę zwrócono na różnice w metodologii dowodzenia bezpieczeństwa w oparciu o badanie skutków poszczególnych uszkodzeń oraz w oparciu o analizę ryzyka.

SAFETY OF THE RAILWAY TRAFFIC CONTROL SYSTEMS ACCORDING TO CENELEC – STANDARDS

Summary. The article presents the problems of the safety estimation of the railway traffic control systems according to CENELEC – standards. Particular attention has been paid to the difference in the methodology of the proving the safety based on the failure effects analysis and the risk analysis.

1. WSTĘP

Wprowadzenie techniki cyfrowej w dziedzinie sterowania ruchem kolejowym (srk) spowodowało, że konieczne stało się opracowanie nowych kryteriów oceny urządzeń, ze szczególnym uwzględnieniem bezpieczeństwa ruchu. Stosowane dotychczas metody analizy systemów przekaźnikowych są bowiem nieprzydatne w odniesieniu do systemów komputerowych. Nowa idea osiągania i dokumentowania bezpieczeństwa systemów srk przedstawiona została w normach Europejskiego Komitetu Normalizacji Elektrotechnicznej (CENELEC). Normy te rozszerzają w znaczący sposób zakres zagadnień, jakie muszą być uwzględnione w procesie projektowania, realizacji i użytkowania urządzeń srk.

*) Instytut Transportu Politechniki Śląskiej – Zespół Automatyki w Transporcie; ul. Krasińskiego 8, 40-019 Katowice, tel. (032) 2552179, e-mail: zaitk@polsl.katowice.pl

2. BEZPIECZEŃSTWO

2.1. Ujęcie klasyczne (urządzenia przekaźnikowe)

W urządzeniach przekaźnikowych pojęcie bezpieczeństwa rozumiane jest jako pewna własność polegająca na tym, że każda usterka lub nieprawidłowość w obiekcie (lub jednym z jego podzespołów) powinna prowadzić do zatrzymania jego działania, czyli wykluczyć powstanie zagrożenia dla życia lub zdrowia ludzi - urządzenie powinno znaleźć się w stanie bezpiecznym. Opuszczenie stanu bezpiecznego przez urządzenie możliwe jest tylko na skutek świadomego działania człowieka. Urządzenia spełniające te warunki określane są jako „fail-safe" Dowodzenie bezpieczeństwa polega na wykazaniu bezpiecznych reakcji urządzenia lub systemu na różne rodzaje usterek. Analizy bezpieczeństwa polegają więc na badaniu reakcji danego układu na pewne typowe rodzaje usterek (np. niewzbudzenie przekaźnika, zespawanie lub brak kontaktu zestyków, zwarcia i przerwy w kablach). Są to tzw. analizy „dół-góra" („bottom-up"), u podstaw których leży pojedyncza usterka.

2.2. Ujęcie CENELEC

Zagadnienia bezpieczeństwa elektronicznych systemów srk zostały ujęte w wielu normach Europejskiego Komitetu Normalizacji Elektrotechnicznej CENELEC. Najważniejsze z nich to:

- EN 50126 Railway applications – The specification and demonstration of Reliability, Availability, Maintability and Safety (RAMS)
- EN 50128 Railway applications – Software for railway control and protection systems
- EN 50129 Railway applications – Safety related electronics systems for signalling
- EN 50159-1 Railway applications – Signalling and communications – Safety-related communication in closed transmission systems
- EN 50159-2 Railway applications – Signalling and communications – Safety-related communication in open transmission systems

Podstawową normą spośród wymienionych jest norma EN 50126, określająca główne cele i warunki, jakie musi spełniać urządzenie (lub system), aby można było uznać je za bezpieczne. Pozostałe wymienione normy (jak również inne, nie wspomniane tutaj) precyzują wymagania normy EN 50126.

Głównym celem, jaki muszą spełniać współczesne systemy, jest ich jakość usług, na którą składają się między innymi własności wykorzystywanych środków technicznych, oznaczane

jako RAMS (Reliability, Availability, Maintability, Safety). Zapewnienie odpowiedniej jakości wyrobu możliwe jest tylko poprzez odpowiednią organizację procesu rozwoju produktu (planowanie, projekt, wytwarzanie, kontrola jakości, utrzymanie). W tym zakresie normy CENELEC narzucają twórcom urządzeń srk konieczność spełnienia wymogów norm jakościowych serii ISO 9000.

W świetle norm CENELEC bezpieczeństwo (Safety) jest więc tylko jedną z własności, jakie powinny posiadać systemy i urządzenia srk. Jest ono jednak definiowane w nieco inny sposób niż w ujęciu klasycznym: system bezpieczny to system wolny od nieakceptowanego poziomu ryzyka. Ryzyko jest jednym z podstawowych pojęć teorii bezpieczeństwa i rozumiane jest jako iloczyn prawdopodobieństwa wystąpienia zdarzenia powodującego zagrożenie i rozmiaru skutków tego zdarzenia. Takie podejście do problemu oszacowania bezpieczeństwa systemu wynika z podstawowej cechy różniącej układy przekaźnikowe od półprzewodnikowych: podczas gdy nawet dla bardzo rozbudowanych układów stykowych możliwe jest określenie rodzajów usterek i ich skutków, to reakcje układów półprzewodnikowych (scalonych) na usterki są nieprzewidywalne. Tak więc klasyczne podejście do zagadnień bezpieczeństwa urządzeń srk ogranicza się do analizy jakościowej, podczas gdy odwołanie się do pojęcia ryzyka (czyli pośrednio do prawdopodobieństwa wystąpienia poszczególnych zdarzeń) uwzględnia konieczność ilościowego opisu poziomu bezpieczeństwa (np. poprzez podanie intensywności zagrożeń). Wiąże się to z koniecznością szczegółowej identyfikacji zdarzeń prowadzących do powstawania zagrożeń w systemie, w tym zdefiniowania parametrów liczbowych określających możliwość ich wystąpienia (prawdopodobieństwo, częstość, średni czas między zdarzeniami). Jak więc można zauważyć, nowe ujęcie problemu zapewnienia bezpieczeństwa łączy się ściśle z problemem zapewnienia niezawodności (Reliability) całego systemu i poszczególnych jego elementów składowych, zapewnienia jego dostępności (Availability) i podatności na konserwację (Maintability).

Ilościowe potraktowanie bezpieczeństwa nie oznacza równoczesnej rezygnacji z podejścia jakościowego. Zasada „fail-safe" pozostaje nadal aktualna, tzn. dla każdego urządzenia lub systemu muszą zostać zdefiniowane stany (reakcje) bezpieczne. Różnica polega na szerszym rozumieniu pojęcia bezpieczeństwa: jak już wspomniano, w urządzeniach elektronicznych zawierających układy scalone trudno przewidzieć zachowanie się urządzenia w momencie wystąpienia usterki. Znacznie większy jest również stopień złożoności układów elektronicznych. Analizy ilościowe mają na celu przede wszystkim dokonanie oceny

możliwości niespełnienia założeń „fail-safe", czyli braku reakcji bezpiecznej w chwili wystąpienia usterki.

Ilościowy opis bezpieczeństwa systemu opiera się głównie na analizach „góra-dół" („top-down"), np. z wykorzystaniem drzewa niezdatności (FTA-Fault Trec Analysis), podczas gdy analizy jakościowe opierają się najczęściej na metodzie rodzajów i skutków usterek (FMEA – Fault Mode And Effect Analysis). Przepisy wymagają, aby analizy bezpieczeństwa wykonywane były na bieżąco i uwzględniały kolejne zmiany wprowadzane w trakcie rozwoju systemu (urządzenia). Umożliwia to wczesne wykrywanie błędów i potencjalnych usterek mogących prowadzić do powstawania zagrożeń w systemie oraz ich eliminację, ograniczenie możliwości ich wystąpienia lub ograniczenie skutków (redukcję ryzyka). Algorytm planowania i realizacji bezpieczeństwa w systemie przedstawiony został na rys. 1.

3. DOWÓD BEZPIECZEŃSTWA

Struktura i spis dokumentów składających się na Dowód Bezpieczeństwa zawarte zostały w normach EN 50128 i EN 50129. W odróżnieniu od poprzednich form dokumentacji nie jest on wyłącznie prezentacją technicznych środków mających na celu zapewnienie realizacji funkcji „fail-safe". W świetle wymagań CENELEC Dowód Bezpieczeństwa jest udokumentowaną formą prezentacji spełnienia przez system nałożonych wymagań bezpieczeństwa, jednak nie tylko poprzez zastosowanie różnych środków technicznych, ale również poprzez odpowiednią organizację całego procesu tworzenia i eksploatacji urządzenia.

Dowód Bezpieczeństwa wg norm CENELEC powinien składać się z sześciu części:

Część 1: Definicja systemu

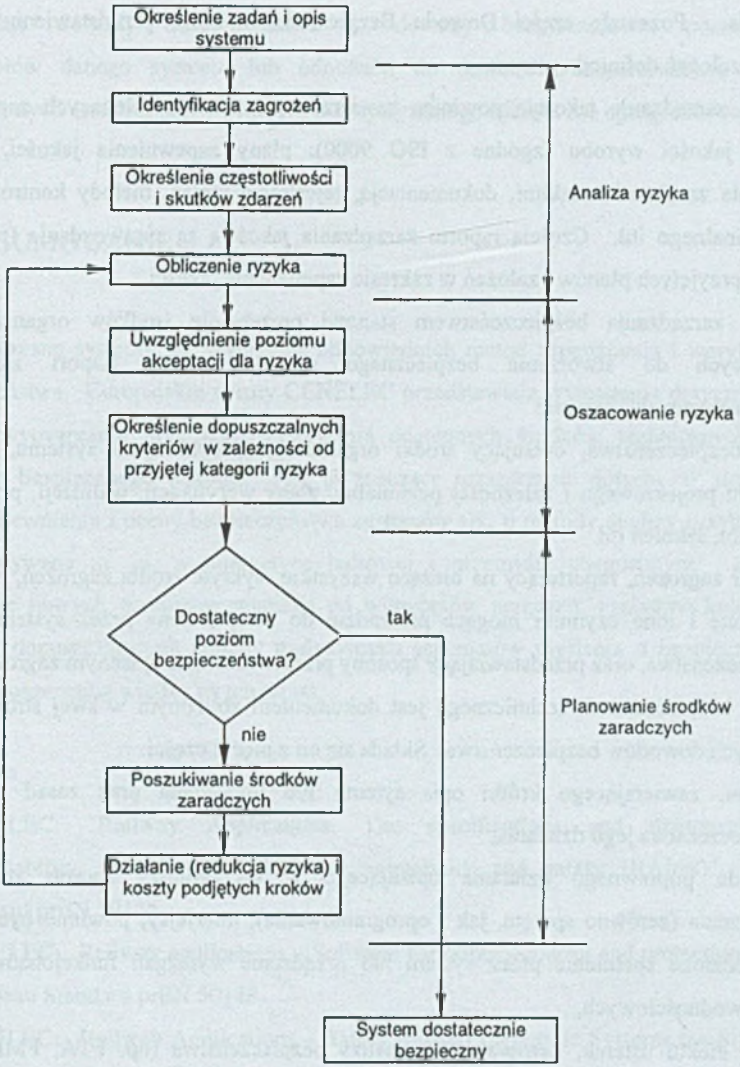
Część 2: Raport zarządzania jakością

Część 3: Raport zarządzania bezpieczeństwem

Część 4: Raport bezpieczeństwa technicznego

Część 5: Odnośne Dowody Bezpieczeństwa

Część 6: Podsumowanie



Rys. 1.Cykl planowania bezpieczeństwa systemu [4]
Fig. 1. System-safety planning cycle

Definicja systemu powinna szczegółowo określać przedmiot projektu, dla którego opracowywany jest Dowód Bezpieczeństwa, wymagania funkcjonalne, niezawodnościowe, środowiskowe i bezpiecznościowe (w tym definicję stanu bezpiecznego, klasę SIL-Safety Integrity Level i parametry ilościowe) dla tworzonego systemu. Wymagania systemu muszą być zgodne z wymogami odpowiednich norm krajowych lub międzynarodowych, a w przypadku braku szczegółowych uwarunkowań powinny zostać zaakceptowane przez przyszłego odbiorcę systemu (zarząd kolejowy) i organ dopuszczający urządzenie do

stosowania. Pozostałe części Dowodu Bezpieczeństwa służą przedstawieniu sposobu realizacji założeń definicji systemu.

Raport zarządzania jakością powinien zawierać opis procedur służących zapewnieniu wysokiej jakości wyrobu (zgodne z ISO 9000): plany zapewnienia jakości, sposoby zarządzania zasobami ludzkimi, dokumentacją, rejestrację zmian, metody kontroli jakości wyrobu finalnego itd. Częścią raportu zarządzania jakością są sprawozdania (raporty) z realizacji przyjętych planów i założeń w zakresie zapewnienia jakości.

Raport zarządzania bezpieczeństwem stanowi prezentację środków organizacyjnych prowadzących do stworzenia bezpiecznego systemu. Na Raport zarządzania bezpieczeństwem składają się:

- Plan bezpieczeństwa, opisujący środki organizacyjne, cykl życia systemu, strukturę zespołu projektowego i zależności personalne, plany weryfikacji, walidacji, przeglądów projektu, szkoleń itd.
- Rejestr zagrożeń, raportujący na bieżąco wszystkie wykryte źródła zagrożeń, zmiany w projekcie i inne czynniki mogące prowadzić do niespełnienia przez system założeń bezpieczeństwa, oraz przedstawiający sposoby przeciwdziałania opisanym zagrożeniom.

Raport bezpieczeństwa technicznego jest dokumentem zbliżonym w swej strukturze do tradycyjnych dowodów bezpieczeństwa. Składa się on z pięciu części:

- wstępu, zawierającego krótki opis sytemu lub urządzenia oraz zasad uzyskania bezpieczeństwa jego działania,
- dowodu poprawnego działania opisującego w szczegółowy sposób architekturę urządzenia (zarówno sprzętu, jak i oprogramowania), interfejsy; powinno być również dowiedzione spełnienie przez system lub urządzenie wymagań funkcjonalnych oraz niezawodnościowych,
- opisu efektu usterek, zawierającego analizy bezpieczeństwa (np. FTA, FMEA) oraz przedstawiającego sposoby przeciwdziałania usterkom i błędom (w tym systematycznym),
- opisu działania przy zewnętrznych oddziaływaniach, dowodzącego (np. w drodze testów) spełnienia przez system wymagań środowiskowych, oraz opisy metod umożliwiających spełnienie tych wymagań,
- opisu bezpiecznych warunków stosowania, zawierającego szczegóły dotyczące procedur oznakowania, montażu, odbioru technicznego, utrzymania i demontażu urządzenia,
- opisów testów sprawdzających bezpieczeństwo.

Odnośne dowody bezpieczeństwa to dowody bezpieczeństwa poszczególnych podzespołów danego systemu lub odnośniki do dowodów bezpieczeństwa wcześniej dopuszczonych urządzeń, jak również wykorzystywanego sprzętu lub oprogramowania.

4. PODSUMOWANIE

Nowoczesne systemy srk wymagają odpowiednich metod zapewnienia i weryfikacji ich bezpieczeństwa. Europejskie normy CENELEC przedstawiają wymagania dotyczące całego procesu wytwarzania oraz wykorzystywania dostępnych środków technicznych w celu uzyskania bezpiecznego wyrobu. Jest to znaczące rozszerzenie dotychczas stosowanych metod zapewnienia i oceny bezpieczeństwa systemów srk, o metody analizy ryzyka, znane i wykorzystywane m. in. w energetyce jądrowej i przemyśle chemicznym. Efektywne stosowanie nowych przepisów wymaga od wytwórców urządzeń, zarządów kolejowych i jednostek dopuszczających zmiany tradycyjnych schematów myślenia o bezpieczeństwie i ciągłego poszerzania wiedzy na ten temat.

Literatura

1. CENELEC: "Railway Applications. The specifications and demonstration of dependability, reliability, availability, maintability and safety (RAMS)"; European Standard prEN 50126.
2. CENELEC: „Railway applications – Software for railway control and protection systems" European Standard prEN 50128.
3. CENELEC: „Railway Applications – Safety Related Electronic Systems for Signalling"; European Prestandard ENV 50129.
4. Bundesministerium für Verkehr, Bonn: „Risikoorientierte Sicherheitsnachweise im Eisenbahnbetrieb" – Leitfaden (Stand Oktober 1996); Ernst Basler+Partner, Zollikon 1996.