mgr inż. Grażyna Barna
Instytut Pojazdów Szynowych „TABOR"

Wprowadzenie do problematyki niezawodności i bezpieczeństwa mikroprocesorowych systemów sterowania pojazdów szynowych

W artykule podano podstawowe definicje pojęć istotnych dla omawianego zagadnienia i przedstawiono charakterystykę systemu sterowania. Opisano różnicę pomiędzy mikroprocesorowymi a konwencjonalnymi systemami sterowania pojazdów szynowych. Poruszono podstawowe zagadnienia związane z bezpieczeństwem i niezawodnością systemu sterowania.
Artykuł powstał w wyniku realizacji projektu badawczego Komitetu Badań Naukowych nr 8 T12C 019 21 pt. „Zastosowanie najnowszych technik informatycznych i elektronicznych w hierarchicznych systemach sterowania i diagnozowania trakcyjnych pojazdów szynowych".

1. Wstęp

Przedmiotem artykułu są dwie zasadnicze właściwości mikroprocesorowych systemów sterowania trakcyjnych pojazdów szynowych: niezawodność i bezpieczeństwo. Program zapewnienia bezpieczeństwa i niezawodności systemów wymaga uwzględnienia na każdym etapie powstawania systemów (koncepcji, projektowania, opracowywania, eksploatacji oraz likwidacji) zagadnień związanych z bezpieczeństwem i niezawodnością. Podstawą tego programu jest przeprowadzenie analizy zagrożeń dla bezpieczeństwa i niezawodności. Polega ona na określeniu i ocenie zagrożeń dla danego systemu, co z kolei pozwala na opracowanie najskuteczniejszych środków ich kontrolowania. Aby skutecznie przeprowadzić taką analizę należy w pierwszym rzędzie zrozumieć istotę i strukturę analizowanego systemu [3].

System definiowany jest jako:

> *„zespół urządzeń współpracujących w celu wypełnienia określonej misji"* [1].

Misja rozumiana jest tu jako:

> *„obiektywny opis podstawowego zadania wykonywanego przez system"* [9].

Elementem nazywa się:

> *„obiekt, w którym z punktu widzenia analizy bezpieczeństwa nie uwzględnia się struktury wewnętrznej"* [3].

Bardziej szczegółowa definicja systemu przedstawiona jest w [9]:

> *„System można zdefiniować jako zespół podsystemów i części składowych, połączonych ze sobą w zorganizowany sposób, w celu osiągnięcia określonej funkcjonalności. Funkcjonalność jest przypisana podzespołom i częściom składowym wchodzącym w skład systemu, przy czym zachowanie i stan systemu zmienia się, jeżeli zmienia się funkcjonalność podzespołów i części składowych. System odpowiada na wymuszenia wejściowe wytwarzając określone wielkości wyjściowe, komunikując się przy tym z otoczeniem.*
>
> ...
>
> *Celem systemu kolejowego jest zapewnienie określonego poziomu usług przewozowych, w określonym czasie, bezpiecznie."*

Zgodnie z [9], precyzyjne określenie zasięgu pojęcia *system* zależy od konkretnego zastosowania. W artykule przyjęto, że pojęcie to oznacza pociąg złożony z pojazdów szynowych ze wszystkimi układami wchodzącymi w jego skład, w tym również z układem sterowania. W tym kontekście innym adekwatnym synonimem tego pojęcia może być *jednostka transportowa*.

W dalszej części artykułu *systemami komputerowymi* lub *systemami mikroprocesorowymi* nazywane będą komputerowe systemy sterowania i diagnostyki pojazdów szynowych.

System komputerowy definiowany jest jako:

> *„jeden lub więcej komputerów, urządzenia peryferyjne i oprogramowanie przeznaczone do przetwarzania danych."*

Zdefiniowane w ten sposób systemy (jednostki transportowe) mogą być rozpatrywane jako elementy wchodzące w skład szerszego systemu, który w niniejszym opracowaniu nazywany będzie *systemem kolejowym*.

2. Charakterystyka systemu sterowania wynikająca ze specyfiki obiektu sterowanego

Mikroprocesorowy system sterowania osadzony jest w specyficznym środowisku, którym jest pojazd szynowy. Właściwości systemu sterowania wynikające ze specyfiki obiektu sterowanego są następujące:

System wbudowany

System wbudowany może również fizycznie być częścią sterowanego systemu. Tak właśnie dzieje się w przypadku omawianego systemu sterowania, który jest fizycznie umieszczony na pojeździe szynowym. Bezpośrednią konsekwencją tego faktu są warunki środowiskowe jego pracy.

Pracujący w trudnych warunkach środowiskowych

Sterowniki mikroprocesorowe, wchodzące w skład systemu sterowania, narażone są na niekorzystne warunki środowiskowe: drgania, wstrząsy, niskie temperatury, zakłócenia elektromagnetyczne.

System czasu rzeczywistego

System czasu rzeczywistego (ang. real-time system) jest to taki system przetwarzania informacji, który musi odpowiedzieć na zewnętrzną informację pojawiającą się na wejściu w skończonym oraz określonym czasie. Innymi słowy mówiąc, usługi świadczone przez ten system muszą być poprawne zarówno w odniesieniu do wartości jak i do czasu [4].

Krytyczny ze względu na bezpieczeństwo

System krytyczny ze względu na bezpieczeństwo (ang. safety critical), jest to system, którego uszkodzenie może pociągnąć za sobą poważne konsekwencje, np. śmierć lub zranienie ludzi, znaczne straty materialne, uszkodzenia środowiska, itp.

System o strukturze rozproszonej

W przemysłowych systemach sterowania możliwe jest zastosowanie struktury scentralizowanej albo zdecentralizowanej (rozproszonej). W scentralizowanym systemie sterowania stosuje się jeden sterownik, do którego doprowadza się sygnały z czujników, a wyprowadza sygnały wyjściowe do urządzeń wykonawczych. System taki można stosować w przypadku, gdy odległości pomiędzy sterowanymi urządzeniami są niewielkie, a prowadzenie dużej ilości przewodów nie stwarza problemów. W większości sterowanych układów poszczególne sterowane urządzenia znajdują się jednak w pewnych odległościach od siebie. Przy zastosowaniu scentralizowanego systemu sterowania połączenia przewodowe będą długie, co po pierwsze zwiększa koszt, po drugie zajmuje miejsce, po trzecie powoduje zwiększenie podatności na zakłócenia. Pojazdy szynowe są takimi układami, ponieważ pojazd lub pociąg, którym należy sterować, ma zazwyczaj długość od kilkunastu do kilkudziesięciu metrów, a urządzenia rozłożone są wzdłuż całej jego długości. W pojazdach szynowych istotne są wszystkie trzy względy, przy czym dwa ostatnie są ważniejsze niż w systemach stacjonarnych. Wynika to z faktu, że po pierwsze wymiary pojazdu są ograniczone, w związku z czym ograniczona jest również ilość przewodów, które można poprowadzić, po drugie na niewielkiej przestrzeni zgromadzona jest znaczna ilość urządzeń energoelektronicznych, w związku z czym poziom zakłóceń jest wysoki.

Z zastosowania rozproszonego systemu sterowania wynika kilka istotnych korzyści oraz zagrożeń dla bezpieczeństwa i niezawodności systemu. Po stronie korzyści wymienić należy fakt, że poszczególne procesy obsługiwane są przez osobne mikroprocesory, co ogranicza konieczność tworzenia programów wielozadaniowych, nieuniknionych w przypadku jednoprocesorowego systemu scentralizowanego. Oprócz tego występowanie w systemie wielu procesorów umożliwia, przy odpowiednim zaprojektowaniu tego systemu, zrealizowanie redundancji programowej z wykorzystaniem do tego celu rezerw obliczeniowych procesorów, a także redundancji sprzętowej. Dodatkowo możliwe jest stosowanie urządzeń posiadających własne sterowniki mikroprocesorowe, które zostają wówczas dołączone do sieci (o ile są w stanie obsłużyć wybrany protokół transmisji).

Z drugiej strony w rozproszonym układzie sterowania wzrastają wymagania dotyczące jakości oprogramowania. Jest to szczególnie istotne w sytuacji, gdy w systemie sterowania realizowana jest wspomniana wcześniej redundancja: w istotny sposób wzrasta wówczas stopień złożoności programu, gdyż należy przewidzieć wiele sytuacji awaryjnych i odpowiednie sposoby reakcji.

3. Mikroprocesorowe systemy sterowania trakcyjnych pojazdów szynowych a systemy konwencjonalne

W układach sterowania i diagnostyki pojazdów trakcyjnych można wyodrębnić trzy generacje:

- sterowanie przekaźnikowo-stykowe,
- sterowanie z wykorzystaniem układów elektronicznych,
- sterowanie z wykorzystaniem układów mikroprocesorowych.

W przypadku systemów pierwszych dwóch generacji (systemy konwencjonalne), algorytmy działania realizowane są na drodze sprzętowej. W systemach trzeciej generacji algorytmy zrealizowane są w postaci oprogramowania zapisanego w jego pamięci nieulotnej. W układach tego typu możliwa jest zmiana działania układu przez zmianę samego oprogramowania bez konieczności wprowadzania zmian sprzętowych.

Obecnie powszechnie znane są zalety komputerowych systemów sterowania w stosunku do systemów konwencjonalnych (sprzętowych) oraz korzyści płynące z ich zastosowania. Przykładem może być precyzyjne sterowanie parametrami jazdy, zwiększenie przyczepności dzięki kontroli poślizgu oraz zmniejszenie kosztów utrzymania i skrócenie czasów przestoju dzięki systemowi diagnostyki. Mniej oczywiste jest natomiast, w jaki dokładnie sposób zastosowanie układów mikroprocesorowych wpływa na podstawowe atrybuty systemu sterowania, takie jak niezawodność i bezpieczeństwo. Z tego względu przedstawiono związki pomiędzy zastosowaniem mikroprocesorowego systemu sterowania a niezawodnością i bezpieczeństwem systemu.

Zastosowanie mikroprocesorowych systemów sterowania może zwiększyć niezawodność i bezpieczeństwo pojazdów szynowych dzięki systemowi diagnostyki. Dzieli się ona na tzw. diagnostykę wewnętrzną i zewnętrzną.

Diagnostyka wewnętrzna polega na monitorowaniu funkcji realizowanych przez układ sterowania i określaniu stanu mechanicznych i elektrycznych części najważniejszych podzespołów wchodzących w skład pojazdu [4, 8, 10], w tym również systemu komputerowego. Informacje diagnostyczne wykorzystywane są na kilka sposobów. Przede wszystkim wykorzystywane są bezpośrednio do sterowania pojazdem. Przykładowo, w przypadku uszkodzenia niektórych urządzeń następuje automatyczne zatrzymanie pojazdu. Oprócz tego informacje diagnostyczne istotne dla prowadzenia pojazdu (komunikaty o uszkodzeniach oraz środki zaradcze) prezentowane są na bieżąco maszyniście. Może on też, przy pomocy panelu operatorskiego, uzyskać dostęp do innych interesujących go danych. Jednocześnie dane diagnostyczne zapisywane są w pamięci nieulotnej, skąd mogą zostać odczytane przez personel warsztatowy, oraz przy pomocy interfejsu diagnostycznego zostać przeniesione do komputera PC. Umożliwia to dalsze przetworzenie danych i poddanie ich szczegółowej analizie, która ma na celu ocenę stanu poszczególnych podzespołów. Dzięki temu można wykryć pogorszenie stanu urządzeń i elementów na wczesnym etapie. W najbardziej zaawansowanych technicznie rozwiązaniach, (np. w pociągach TGV i ICE), informacje o uszkodzeniach przesyłane są z pociągu do warsztatów naprawczych drogą radiową. Jest to wykonywane automatycznie lub na żądanie obsługi podczas jazdy lub postoju (przerw podczas jazdy).

Diagnostyka zewnętrzna polega na przeprowadzaniu okresowych badań diagnostycznych w warsztacie.

Komputerowe systemy sterowania trakcyjnych pojazdów szynowych różnią się w zasadniczy sposób od systemów realizowanych przy pomocy układów przekaźnikowych lub z zastosowaniem układów logicznych o niskiej skali integracji, ponieważ funkcje, które w konwencjonalnych systemach sterowania realizowane były na drodze sprzętowej, w systemach komputerowych realizowane są w sposób programowy. Dzięki temu możliwe stało się zrealizowanie nowych, niedostępnych dotychczas funkcji, mających znaczący wpływ na poprawienie niezawodności oraz bezpieczeństwa, jednocześnie jednak pojawiły się nowe, nieznane wcześniej problemy.

Z punktu widzenia niezawodności i bezpieczeństwa, podstawowe różnice pomiędzy konwencjonalnym a komputerowym systemem sterowania to [1]:

- inne klasy uszkodzeń,
- stopień złożoności systemu,
- dowolność struktury,
- brak niezależności elementów,
- brak fizycznych ograniczeń zachowania systemu,
- łatwość zmian.

Mikroprocesorowe systemy sterowania również ulegają uszkodzeniom, ale mechanizm i skutki tych uszkodzeń są inne niż w konwencjonalnych układach sterowania [2]. Uszkodzenia związane ze sprzętem powodują najczęściej całkowitą awarię komputera nawet wówczas, gdy mają charakter przejściowy. W układach konwencjonalnych prowadzą one natomiast na ogół jedynie do zakłóceń lokalnych. Oprócz tego mechanizm awarii powodowanych przez oprogramowanie nie ma charakteru fizycznego, ale polega na ujawnieniu się w czasie eksploatacji błędów oprogramowania, które nie zostały wykryte i usunięte na poprzednich etapach jego powstawania i wdrażania [8].

Klasyczne mechanizmy zapewnienia bezpieczeństwa stosowane w układach konwencjonalnych nie dają się bezpośrednio przełożyć na komputerowy system sterowania [1]. Przykładowo, w przypadku systemu mikroprocesorowego niewystarczające stają się tradycyjne metody testowania. Aby przetestować układ w pełni sprzętowy, wystarczy sprawdzić jego działanie dla ograniczonej liczby kombinacji sygnałów wejściowych. Nie jest jednak możliwe pełne przetestowanie programu [8].

Podsumowując, metody projektowania zapewniające bezpieczeństwo stosowane w przypadku systemów sterowania konwencjonalnego w wielu przypadkach nie nadają się do bezpośredniego zastosowania do systemów sterowania komputerowego [1]. Należy w związku z tym opracować i stosować inne metody, dostosowane do tych systemów. Jedną z możliwości jest wdrażanie jakości na etapie projektowania systemu, np. stosowanie odpowiednich metod tworzenia oprogramowania, zapewniających jego wysoką jakość.

4. Niezawodność i bezpieczeństwo mikroprocesorowych systemów sterowania pojazdów szynowych

Z punktu widzenia automatyki system podzielić można na układ sterujący oraz obiekt sterowany, przy czym właściwości każdego z tych dwóch elementów mogą być analizowane oddzielnie

Z punktu widzenia analizy niezawodności i bezpieczeństwa podział taki jest również prawdziwy, ale niewystarczający, ponieważ system sterowania nie jest odizolowanym systemem, ale wchodzi w skład większej całości, jaką jest pojazd trakcyjny, który z kolei jest częścią większej całości, którą jest pociąg. Celem zaś jest niezawodność i bezpieczeństwo całego systemu. W odniesieniu do bezpieczeństwa zagadnienie to jest w bardzo ciekawy sposób przedstawione w [1].

> *„Bezpieczeństwo jest atrybutem całego systemu a nie zawartego w nim komputera lub tym bardziej oprogramowania. (...) System komputerowy jest bezpieczny (tak jak większość systemów sterujących rozpatrywanych w izolacji). Natomiast sygnały generowane przez komputer mogą być użyte do sterowania innymi urządzeniami, które poprzez oddziaływanie na swoje środowisko mogą spowodować wypadek. W tym kontekście można powiedzieć, że system komputerowy ma wpływ na bezpieczeństwo całego systemu, więc jest* podsystemem związanym z bezpieczeństwem. *W skrócie mówi się o bezpieczeństwie systemu komputerowego jako takiego. Jest to powszechnie przyjęte uproszczenie, jednak nie należy zapominać, że bezpieczeństwo ma sens tylko jako atrybut całego systemu."*

W przypadku niezawodności, biorąc pod uwagę jej definicję, można już mówić o niezawodności systemu sterowania jako takiego. Należy jednak pamiętać, że również w tym przypadku dążenie do zwiększenia niezawodności systemu sterowania jest jedynie środkiem prowadzącym do osiągnięcia celu, którym jest niezawodność całego systemu.

W tym miejscu pojawia się problem ekonomicznego aspektu zagadnienia, który z oczywistych względów musi być brany pod uwagę. Problem ten poruszany jest przez wielu autorów (np. [4, 5, 7]).

Podsumowując, rozpatrywanie bezpieczeństwa i niezawodności systemu sterowania należy przeprowadzać na dwóch płaszczyznach. Po pierwsze należy odpowiedzieć na pytanie, co należy zrobić, aby system sterowania był sam w sobie jak najbardziej bezpieczny i niezawodny. Po drugie, należy rozpatrzyć związek pomiędzy niezawodnością i bezpieczeństwem systemu sterowania pojazdu trakcyjnego, a niezawodnością i bezpieczeństwem jednostki transportowej.

5. Podsumowanie

Rozwój technologii komputerowej umożliwia zwiększenie niezawodności i bezpieczeństwa, jednak do wykorzystania zalet płynących z jego zastosowania wymagany jest wysokiej jakości system sterowania [4]. Aby system sterowania komputerowego był konkurencyjny w stosunku do systemów konwencjonalnych, musi być niezawodny, bezpieczny i dyspozycyjny [9].

Z przedstawionych rozważań wypływają dwa wnioski: po pierwsze, niewłaściwie zaprojektowany mikroprocesorowy system sterowania może doprowadzić zamiast do zwiększenia – do zmniejszenia niezawodności i bezpieczeństwa. Pojawia się również problem ekonomiczny: nieefektywnie działający układ diagnostyczny przyczyni się do powstania nakładów finansowych związanych z jego stworzeniem, nie spowoduje natomiast zmniejszenia kosztów związanych z utrzymaniem pojazdów [4].

Dlatego też zaprojektowanie bezpiecznego i niezawodnego mikroprocesorowego systemu sterowania pojazdu trakcyjnego wymaga opracowania i stosowania odpowiednich metod projektowania, dostosowanych do jego specyfiki.

Literatura

[1] *Górski J., Bezpieczeństwo przemysłowych zastosowań komputerów, III Krajowa Konferencja Naukowo-Techniczna Diagnostyka Procesów Przemysłowych, Jurata, 7-10 wrzesień, 1998,*

[2] *Hedtke R., Systemy mikroprocesorowe, WNT, Warszawa 1987,*

[3] *Jaźwiński J., Ważyńska-Fiok K., Bezpieczeństwo systemów, Wydawnictwo Naukowe PWN, Warszawa, 1993,*

[4] *Johansson R., Dependability characteristics and safety criteria for an embedded distributed brake control system in railway freight trains, Chalmers Lindholmen University College, Göteborg Sweden, Report no.8, August 2001,*

[5] *Kadziński A., Wprowadzenie do zagadnień bezpieczeństwa systemów kolejowych pojazdów szynowych, XII Konferencja Naukowa „Pojazdy Szynowe'96", Poznań-Rydzyna, 21-24 październik 1996, t. 2,*

[6] *Kopetz H., Niezawodność oprogramowania, WNT, Warszawa, 1980,*

[7] *Magiera J., Bezpieczeństwo w systemach transportowych, XIV Konferencja Naukowa „Pojazdy Szynowe 2000", Kraków-Arlamów, 9-12 październik 2000, t. 3,*

[8] *Żurakowski Z., Atestacja systemów komputerowych wbudowanych w pojazdy szynowe, X Konferencja Naukowa „Pojazdy Szynowe", Wrocław, 14-16 września 1994, t. 2, 258-269,*

[9] *Polska Norma, PN-EN 50126, Zastosowania kolejowe – Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa, 1992,*

[10] *ORE Question B 166 Fault diagnostics for and on trains, Report RP 1 Application of diagnostic techniques to railway vehicles (Survey Report) 1987.*