Eksploatacja i modernizacja systemów sterowania ruchem kolejowym

Szymon SURMA[1], Jakub MŁYŃCZAK[2]

Streszczenie
Artykuł dotyczy tworzenia i utrzymywania stanów magazynowych, pozwalających na maksymalizację gotowości systemu sterowania ruchem kolejowym. Skupiono się na systemie sterowania ruchem kolejowym zbudowanym ze sterowników PLC i elementów elektronicznych. Omówiono zarówno problematykę uzależnienia zapasów od intensywności uszkodzeń podzespołów, jak i czasu dostarczenia części zamiennych. Zwrócono również uwagę na konieczność zmiany podejścia personelu do polityki bezpieczeństwa przez podniesienie świadomości zagrożeń cyberprzestępczością.
Słowa kluczowe: sterowanie ruchem kolejowym, niezawodność, naprawy, zapasy

1. Wstęp

Dostępność w handlu urządzeń składających się na system sterowania, a w szczególności sterowników PLC, może być różna w zależności od przyjętej polityki danego producenta. Jako przykład może tutaj posłużyć „Terminarz zakończenia produkcji systemów SIMATIC S5" [2]. W dokumencie ujęto zakres czasowy od rozpoczęcia w końcu lat 70. produkcji sterowników serii S5, przez czas podjęcia w 2002 r. decyzji o rozpoczęciu procedury zakończenia w latach 2013–2015 wsparcia sprzętowego dla tej rodziny sterowników. Wskazuje to, że czas życia serii S5 wynosi około 35 lat. Należy zwrócić uwagę na to, iż podjęcie w 2000 r. decyzji o budowie systemu sterowania opartego na tej rodzinie sterowników, daje 15 lat dostępności handlowej elementów sterowników. Fakt ten jest znaczącym ograniczeniem dla systemów sterowania ruchem kolejowym, dla których dokumenty dopuszczenia do eksploatacji i dowód bezpieczeństwa obejmują konkretną architekturę systemu, która jest bezpośrednio związana z architekturą danej rodziny sterowników.

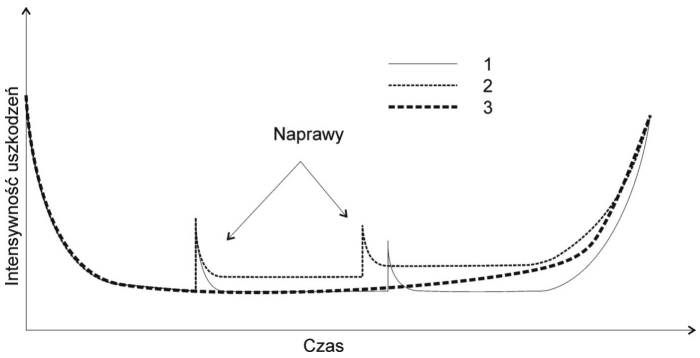
Okres eksploatacji systemu sterowania ruchem kolejowym wymusza na producencie lub dostawcy tego systemu obowiązek zapewnienia odpowiedniej liczby elementów (sterowników) na potrzeby serwisu. Zgodnie z zapisami [6] urządzeń

[1] Dr inż., Politechnika Śląska, e-mail: szymon.surma@polsl.pl, wkład merytoryczny autora 50%.
[2] Dr inż., Politechnika Śląska, e-mail: jakub.mlynczak@polsl.pl, wkład merytoryczny autora 50%.

tych nie powinno poddawać się naprawie, co wynika również z wymagań SIL. Naprawa elementów systemu pociągałaby za sobą konieczność określenia wartości parametru λ naprawionego układu przez zmianę parametrów wymienianych podzespołów, jak i sposobu montażu płytek drukowanych. Zmiana wartości λ dla jednego elementu systemu może wpłynąć na wartość THR całości systemu, a dodatkowo, jeśli naprawy nie były ujęte w dokumentach związanych z dopuszczeniem systemu sterowania do eksploatacji, będzie konieczne ponowne przejście ścieżki dopuszczającej system srk. Z tego powodu naprawy w systemie sterowania wykonuje się przez wymianę na nowe całych podzespołów, dzięki czemu uzyskuje się wartości niezawodności jak dla nowego systemu.

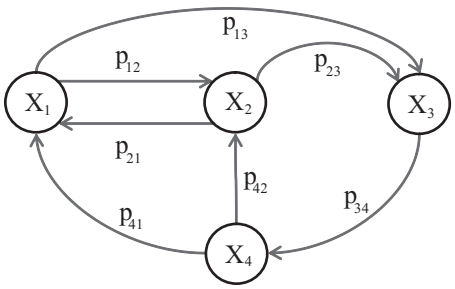
2. Modele niezawodności systemu sterowania oraz wpływ napraw na niezawodność systemu

Naprawa elementów systemu, polegająca np. na wymianie uszkodzonych elementów dyskretnych, implikuje konieczność weryfikacji modeli wykorzystywanych do szacowania niezawodności. Obliczenia intensywności uszkodzeń poszczególnych elementów modelowanego systemu [7] wykonano przy założeniu, że poziom niezawodności elementu podlegającego wymianie będzie taki sam lub wyższy. Nie jest to jednak zgodne ze stanem rzeczywistym z powodu podwyższonej intensywności uszkodzeń poszczególnych elementów systemu na etapie „niemowlęcym". Niemniej, wartość intensywności uszkodzeń systemu po naprawie usterek jest niższa, co jest powodowane wyższą niezawodnością wymienionych elementów. Zmiany wartości λ zilustrowano na rysunku 1. Można stwierdzić, że newralgiczne okresy dla bezpieczeństwa systemu sterowania, następują bezpośrednio po naprawie uszkodzonego elementu systemu.



Rys. 1. Zmiana wartości intensywności uszkodzeń systemu po wymianie uszkodzonego elementu na nowy (1) i po naprawie (2), odniesiona do systemu, w którym nie nastąpiło uszkodzenie elementu (3) [7]

Na rysunkach 1 i 2 pokazano wartości prawdopodobieństw powrotu systemu do stanu zdatności do użytkowania (np. p_{41}). Należy jednak zaznaczyć, iż wartości te nie są brane pod uwagę w procesie określania poziomu niezawodności systemów srk, a ukazanie ich na grafach procesów Markowa jest podyktowane jedynie ilustracją możliwych przejść pomiędzy stanami, w których system sterowania może przebywać. Wartości tych prawdopodobieństw nie będą brane pod uwagę w dalszej części artykułu.



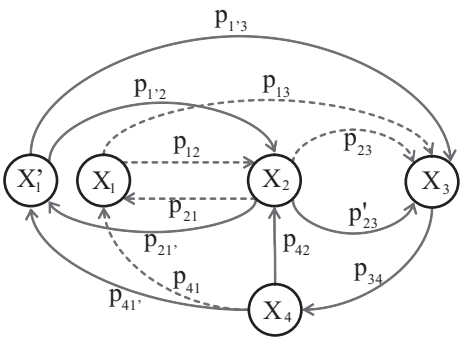
Rys. 2. Model procesu Markowa uwzględniający stan normalnej pracy, usterkę bezpieczną, usterkę niebezpieczną oraz stan oczekiwania na przywrócenie funkcjonalności [7]

Przedstawiony na rysunku 2 model procesu Markowa obejmuje cztery stany systemu sterowania: normalnej pracy X_1, z usterką bezpieczną X_2, z usterką niebezpieczną X_3, oczekujący na przywrócenie funkcjonalności (w naprawie) X_4. System w stanie X_2 może wrócić samoczynnie do stanu X_1 bez ingerencji personelu w zakresie przywrócenia normalnego działania systemu sterowania. Za usterki bezpieczne można przyjąć usterki wynikające z normalnej eksploatacji, np. przepalenie żarówki światła zezwalającego sygnalizatora. Przy usterkach sklasyfikowanych jako X_3 konieczna jest ingerencja personelu w celu ich usunięcia i skasowania indykacji błędu.

Jako przykład można wymienić przepalenie się bezpiecznika na karcie układu mikroprocesorowego lub utratę komunikacji ze sterownikiem PLC. Stan X_4 będzie występował tylko w trakcie napraw systemu, gdy system może być wyłączany oraz testowany. Jak zilustrowano na rysunku 2, nie ma możliwości przejścia pomiędzy stanem X_3 oraz X_1 bez przebywania w stanie X_4, co oznacza, że za każdym razem będzie wymagana ingerencja upoważnionego personelu celem potwierdzenia poprawności działania systemu sterowania. Przewiduje się przywrócenie funkcjonalności systemu sterowania ze stanu X_4 do stanu X_2, który nie jest stanem niebezpiecznym.

Ze względu na charakter pracy systemu w stanie X_4 można przyjąć, że zużycie niektórych podzespołów może odbywać się szybciej niż podczas normalnej eksploatacji (np. dyski twarde komputerów, zasilacze). Jednakże przyjęto założenie,

że praca systemu w trybie jałowym lub wyłączenie systemu sterowania spowodowane usterką, która spowodowała przejście do stanu X_3, kompensuje przyspieszone zużycie elementów w stanie X_4. Przedstawione założenia obejmują przypadek systemu, w którym naprawa polega na wymianie elementów systemu na nowe, pozbawione wad. W przypadku wymiany uszkodzonego elementu na naprawiany, określenie poziomu niezawodności komplikuje się. Do grafu (rys. 2) należy dodać nowy stan X'_1 oraz prawdopodobieństwa przejść między stanami systemu, jak to przedstawiono na rysunku 3. Należy zwrócić uwagę na prawdopodobieństwo p'_{23}, ponieważ przejście ze stanu X_2 do stanu X_3 będzie uzależnione od wartości intensywności uszkodzeń elementu (elementów) po naprawie. Przyjęto założenie, że stany X_2, X_3 oraz X_4 pozostają bez zmian, lecz zmianie ulegną wartości prawdopodobieństw przejść między tymi stanami.



Rys. 3. Model procesu Markowa uwzględniający stan po naprawie elementu systemu [3]

Zilustrowany na rysunku 3 przypadek obejmuje wyłącznie jedną naprawę jednego elementu systemu. Dla każdej kolejnej naprawy należałoby przeprowadzić podobną analizę drogą iteracji, co przy możliwych do zaistnienia usterkach systemu oraz ich kombinacji praktycznie uniemożliwia określenie poziomu niezawodności dla całości systemu drogą dedukcji i wymaga zastosowania programów obliczeniowych. Dlatego w dalszych rozważaniach przyjęto do analizy model zilustrowany na rysunku 2, czyli system z wymianą uszkodzonych elementów na nowe, tak jak jest to obecnie praktykowane.

Dla tak zdefiniowanych stanów pracy systemu sterowania ruchem należy przeprowadzić analizę niezawodności, np. według [5], która posłuży do określenia odpowiedniej liczby personelu obsługi, niezbędnej do utrzymania systemu sterowania w stanie gotowości oraz liczby elementów systemu niezbędnych do bieżącego utrzymania systemu, jak i niezbędnej liczby elementów na potrzeby zapewnienia serwisu po zakończeniu produkcji podzespołów. Liczba niezbędnego personelu do bieżącego utrzymania systemu sterowania w stanie gotowości, jest określana w roboczogodzinach przypadających na dany punkt procesu obsługi systemu.

3. Analiza zapotrzebowania na niezbędną liczbę elementów gwarantujących gotowość systemu sterowania

Poziom intensywności uszkodzeń określony w analizie przeprowadzonej zgodnie z [5], umożliwia określenie przybliżonej liczby elementów systemu sterowania, niezbędnych do utrzymania w stanie gotowości. Na liczbę zapasów części zamiennych będą miały wpływ:

- dostępność elementów na rynku,
- czas dostawy,
- koszt utrzymania zapasów magazynowych.

Konieczne jest również określenie, czy dany element jeszcze jest lub czy nie jest wycofany z produkcji, co wpłynie na poziom zapasów przez konieczność zapewnienia poziomu części zamiennych na pozostały okres życia systemu sterowania.

Określenie zapasu elementów jest możliwe m.in. przez szacowanie usterkowości w zestawieniu z liczbą pracujących elementów. Jeśli wartość MTTF pojedynczego elementu wynosi 10^5 godzin, a liczba pracujących równolegle elementów równa jest 100 sztuk, to średni czas do wystąpienia usterki pojedynczego elementu wyniesie:

$$\mathrm{MTTF}_{100\ \text{elementów}} = \frac{10000}{100} = 100\ \mathrm{h} \approx 4\,\mathrm{dni}.$$

Zakładając, że element jest dostępny „od ręki" w magazynie producenta, a czas dostawy wynosi 1 dzień roboczy, to przy uwzględnieniu okresów dni nieroboczych wynoszący maksymalnie 5 dni (święta i długie weekendy), dostawa elementu jest możliwa w ciągu 6 dni kalendarzowych. Odnosząc to do wartości MTTF dla 100 elementów, na stanie powinny znajdować się 2 elementy. Niemniej, do obliczeń przyjęto wartość uśrednioną MTBF, co implikuje konieczność zapewnienia dodatkowych zapasów związanych z niepewnością równomierności usterkowości. Poziom niepewności jest wartością charakterystyczną dla poszczególnych elementów, a jego wartość jest możliwa do określenia wyłącznie na drodze empirycznej. Do momentu empirycznego określenia zapotrzebowania na części zamienne, można przyjąć założenie, że usterkowość rzeczywista będzie dwukrotnością obliczonej (oszacowanej) wartości średniej.

Wartość intensywności uszkodzeń, określana również przez MTTF (MTBF), charakteryzuje elementy elektroniczne, elektryczne i elektromechaniczne w trakcie pracy, tzn. zainstalowane w systemie. W przypadku konieczności zagwarantowania odpowiedniej liczby elementów zamiennych dla pracującego systemu,

należy zwrócić uwagę na elementy stanowiące zapas magazynowy. Elementy te również mają pewną intensywność uszkodzeń pomimo ich fizycznego nieużytkowania. Wartość intensywności uszkodzeń λ można wyliczyć z wykorzystaniem przywołanej wcześniej metody według [5], z pominięciem pewnych parametrów lub zmniejszeniem ich wpływu przez zmianę wartości prądu, liczby zadziałań przekaźnika, mocy rozpraszanej i temu podobne.

Takie rozwiązanie pozwoliłoby na określenie wartości funkcji niezawodności w momencie wprowadzenia do eksploatacji danego elementu systemu. Nie jest jednak praktykowane, ponieważ nie jest możliwe określenie czasu upływającego między opuszczeniem procesu produkcyjnego do momentu wprowadzenia elementu systemu do eksploatacji. Przyjmując wartości λ lub MTBF, jak dla działającego elementu, niedokładność oszacowania liczby niezbędnych elementów zapasowych może prowadzić do niepotrzebnego podniesienia zapasów magazynowych. Jednym ze sposobów rozwiązania problemu szacowania intensywności uszkodzeń elementów stanowiących zapasy magazynowe, może być przeprowadzenie próby starzenia przyśpieszonego lub prosta obserwacja empiryczna na reprezentatywnej grupie urządzeń.

Potrzeba wykonania badań starzeniowych lub obserwacji grupy reprezentatywnej jest o tyle zasadna, iż w przypadku konieczności zgromadzenia większych zapasów, przy wygaszaniu produkcji elementów systemu sterowania (jak np. sterownik PLC), będzie konieczne oszacowanie zapasów magazynowych zaspokajających zapotrzebowanie do planowanego końca życia systemu sterowania.

Do eksploatacji systemów sterowania należy zaliczyć nie tylko urządzenia, ale również odpowiedni poziom obsługi prowadzonej przez wykwalifikowany lub przeszkolony personel. Zakres umiejętności personelu pracującego z systemem sterowania ruchem kolejowym opartym na systemie komputerowym będzie obejmował elementy, które dotychczas były pomijane, a które odgrywają istotną rolę w zakresie bezpieczeństwa systemu sterowania.

Większość automatyków, dyżurnych ruchu, dróżników i nastawniczych pracujących na PLK nie miała styczności z systemami komputerowymi, a producenci systemów komputerowych dotychczas montowanych bagatelizowali kwestie polityki bezpieczeństwa. Można to wytłumaczyć faktem, iż dotychczas system był bezpieczny, ponieważ jak coś się miało zepsuć, to miało się zepsuć bezpiecznie, czyli zgodnie z zasadą *fail-safe*. W systemach komputerowych zasada *fail-safe* jest realizowana przez bezpieczeństwo funkcjonalne. Zmiana w podejściu do realizacji bezpieczeństwa systemów sterowania prowadzi do konieczności modernizacji polityki bezpieczeństwa, a dokładniej do wprowadzenia nowego zakresu uprawnień dostępu do systemu oraz odpowiedniego przeszkolenia personelu w zakresie bezpieczeństwa sieciowego.

Bezpieczeństwo systemu komputerowego zależy nie tylko od restrykcji w dostępie do pomieszczeń i urządzeń, ale również od dostępności połączeń sieciowych.

Przyłączenie do sieci komputerowej, wchodzącej w skład systemu srk, urządzenia nieautoryzowanego, może umożliwić zdalny dostęp osobie, której celem będzie przejęcie sterowania nad systemem lub wprowadzenie zaburzeń pracy systemu. Oba zdarzenia zaistnieją wyłącznie w przypadku ingerencji osoby z wystarczającą wiedzą z zakresu informatyki, niemniej brak świadomości o potencjalnych zagrożeniach, których źródłem będzie czynnik zewnętrzny, a kanałem dostępu warstwa sieciowa systemu sterowania, jest istotnym czynnikiem obniżającym poziom bezpieczeństwa systemu sterowania ruchem kolejowym.

4. Podsumowanie

Przedstawiona w artykule problematyka powoli zacznie dotyczyć wszystkich producentów systemów sterowania (m.in. ruchem kolejowym), a także Zarządców Infrastruktury Kolejowej. Problem dostępności części zamiennych dotyczy nie tylko systemów sterowania opartych na PCL, ale również większości systemów elektronicznych. Należy pamiętać, że urządzenia elektroniczne (w tym komputerowe) starzeją się zdecydowanie szybciej niż przekaźnikowe lub mechaniczne. A w systemach tych nie da się (pomimo teoretycznych możliwości) naprawiać wielu podzespołów i elementów i trzeba je wymienić na nowe. Aby takiej wymiany dokonać, trzeba mieć na co wymienić. I nie rzadko to nie tylko kwestia dostępności podzespołu lub zamiennika, ale również (a może przede wszystkim) procedur i norm.

Literatura

1. Białoń A., Kazimierczak A., Toruń A.: *Ocena wrażliwości na zakłócenia wybranych urządzeń srk*, X Konferencja Naukowa SEMTRAK, Zakopane, 2002.
2. FAQ – Siemens Polska, 03/03/2008, [on-line] *Terminarz zakończenia produkcji systemów SIMATIC S5*, [dostęp: 10.10.2013], dostępny na WWW http://www.automatyka.siemens.pl/docs/docs_ia/mFAQ.7.1.Zakonczenie_produkcji_S5.pdf.
3. Kasprzyk Z., Siergiejczyk M.: *Zastosowanie metody analizy narażeń części do prognozowania obiektów technicznych na przykładzie pętli przejazdowej stosowanej w systemie poboru opłat*, Problemy Eksploatacji, 2009, s. 193–201.
4. Kisilowski J.: *Podstawy technik pomiarowych*, Skrypty naukowe WSTE, Warszawa, 2005.
5. Mil-HDBK-217f Military Handbook – *Reliability Prediction of Electronic Equipment*, 1995.
6. PN-EN 50129:2007: *Zastosowania kolejowe – Systemy łączności, przetwarzania danych i sterowania ruchem – Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem*.
7. Surma S.: *Tworzenie bezpiecznego systemu sterowania ruchem kolejowym za pomocą zintegrowanego środowiska programistycznego,* Rozprawa doktorska, Katowice, 2013 [na prawach rękopisu].
8. *Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym* Warszawa, CNTK, Zakład sterowania ruchem kolejowym, 1998.

Operation and Modernization of the Railway Safety Installations

Summary
The paper takes up the question of forming and maintaining stocks necessary to guaranty maximum operational readiness of safety installation. Attention was focused on the safety installation system consisting of Programmable Logic Controllers (PLC) and electronic components. Issues relevant to the interrelationship between necessary stores and the rate of component damages as well as delivery time of spare parts were raised. The Authors have also emphasized the need for changing the attitudes of the staff towards safety policies through improvement in awareness of the threats arising out of the cyber-crime.

Key words: Railway safety installation, PLC Controllers, safety policy

Эксплуатация и модернизация систем управления железнодорожным движением

Резюме
Тематику статьи составляют вопросы образования запасов заменяемых деталей и ведения инвентарного учёта для того, чтобы удержать максимальную готовность системы управления железнодорожным движением. В статье внимание обращено на систему управления железнодорожным движением, построенную из командо-контроллеров PLC и электронных компонентов. Обсуждается проблематика как зависимости запасов от интенсивности повреждений подузлов, так и продолжительности поставки заменяемых деталей. Авторы обратили также внимание на необходимость изменения подхода персонала к политике безопасности путём повышения осведомлённости об угрозе киберпреступности.

Ключевые слова: управление железнодорожным движением, командо-контроллеры PLC, безопасность, угроза киберпреступности