Waldemar Nowakowski, Zbigniew Łukasik, Krzysztof Łukomski

Wiarygodność komputerowych systemów automatyki kolejowej

JEL: L94 DOI: 10.24136/atest.2018.376
Data zgłoszenia: 19.11.2018 Data akceptacji: 15.12.2018

Rozwój technologii informacyjnych powoduje, że znajdują one zastosowanie w różnych obszarach życia gospodarczego i społecznego. Przyczynia się to również do szybkiego rozwoju technologicznego systemów automatyki kolejowej, które obecnie są systemami komputerowymi. Postęp, jaki niewątpliwie należy odnotować, musi iść w parze z utrzymaniem przez te systemy wysokich standardów jakościowych, wynikających głównie z konieczności zapewnienia bezpieczeństwa. Stan taki można osiągnąć m.in. poprzez integrację prac związanych z niezawodnością i bezpieczeństwem, a więc poprzez dążenie do uzyskania wiarygodności (dependability) systemów. W artykule poruszony został problem wiarygodności systemów automatyki kolejowej rozumianej jako pewność ich działania, która pozwala mieć uzasadnione zaufanie do zadań, które te systemy realizują.

Słowa kluczowe: bezpieczeństwo, niezawodność, systemy automatyki kolejowej.

Wstęp

Zagadnienie odporności komputerów na uszkodzenia (*fault-tolerant computing*) jest integralnym procesem ich rozwoju. Potrzeba ta początkowo wymuszona była niską jakością elementów, z których były konstruowane komputery. Dlatego też wprowadzono metody poprawy ich niezawodności, tj.: kodowe metody zabezpieczenia przed błędami, metody powtarzania z głosowaniem, redundancję sprzętową oraz metody tolerancji błędów oprogramowania. Rozwój tych metod skutkował również uwzględnieniem wpływu poprawności specyfikacji na wiarygodność systemu [2].

Wiarygodność komputerowego systemu sterowania, w tym również systemu automatyki kolejowej, charakteryzowana jest przez takie atrybuty jak:

- niezawodność (*reliability*) – czyli zdolność do zachowania stanu zdatności (wypełniania określonych funkcji) w określonym przedziale czasu i w określonych warunkach użytkowania,
- gotowość (*availability*) – zdolność systemu do utrzymywania się w stanie umożliwiającym wypełnianie wymaganych funkcji w danych warunkach, w danej chwili lub w danym przedziale czasu,
- obsługiwalność (*maintainability*) – zdolność systemu do utrzymywania lub odtwarzania w danych warunkach eksploatacji stanu, w którym może on wypełniać wymagane funkcje przy założeniu, że obsługa jest przeprowadzana w ustalonych warunkach z zachowaniem ustalonych procedur i środków,
- integralność (*integrity*) – atrybut ten ma związek z poufnością i w szerokim znaczeniu jest to zabezpieczenie przed niewłaściwymi zmianami prowadzącymi do niezgodności systemu z pierwotną specyfikacją, np. w wyniku nieupoważnionego dostępu do oprogramowania i danych.
- bezpieczeństwo (*safety*) – pod pojęciem tym rozumie się brak niedopuszczalnego ryzyka.

W dalszej części główna uwaga została skupiona na podstawowych atrybutach wiarygodności, jakim jest zapewnienie bezpieczeństwa i niezawodności przez systemy automatyki kolejowej.

1. Bezpieczeństwo i niezawodność systemów automatyki kolejowej

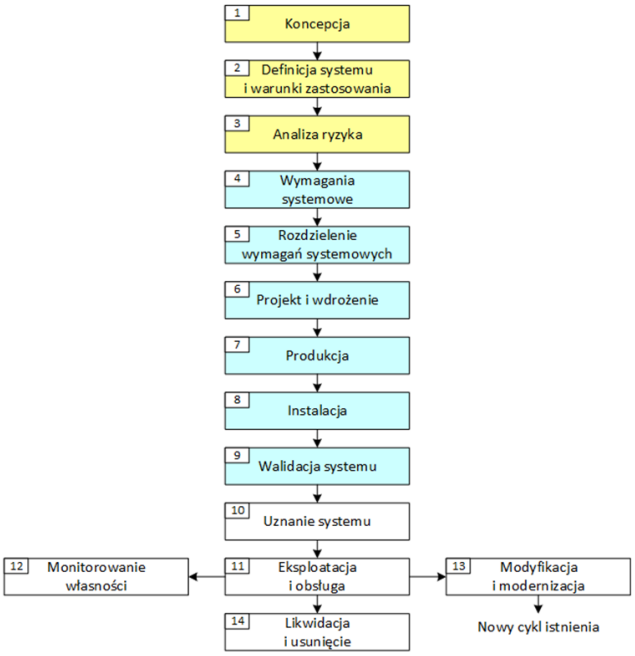
Współczesne systemy sterowania budowane są jako systemy elektroniczne. W celu zapewnienia przez te systemy niezbędnego poziomu bezpieczeństwa w 1998 roku Międzynarodowa Komisja Elektrotechniczna IEC (*International Electrotechnical Commission*) opublikowała dokument IEC 61508, pt.: "Bezpieczeństwo funkcjonalne elektrycznych / elektronicznych / programowalnych systemów elektronicznych związanych z bezpieczeństwem". Normy te określają standardy w zakresie bezpieczeństwa funkcjonalnego dla sprzętu i oprogramowania, stanowiąc warunki ramowe dla różnych sektorów gospodarki.

Systemy automatyki kolejowej są systemami związanymi z bezpieczeństwem. Dlatego też, na bazie norm IEC 61508, Europejski Komitet Normalizacyjny Elektrotechniki CENELEC (*fr. Comité Européen de Normalisation Electrotechnique*) opracował normy dla branży kolejowej. W ich skład wchodzą następujące dokumenty, które zostały zatwierdzone przez Polski Komitet Normalizacyjny (PKN) [16, 17, 18, 19]:

- PN-EN 50126. Zastosowania kolejowe - Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa.
- PN-EN 50128. Zastosowania kolejowe - Systemy łączności, przetwarzania danych i sterowania ruchem - Oprogramowanie kolejowych systemów sterowania i zabezpieczenia.
- EN 50129. Zastosowania kolejowe - Systemy łączności, przetwarzania danych i sterowania ruchem - Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem.
- EN 50159. Zastosowania kolejowe - Systemy łączności, sterowania ruchem i przetwarzania danych - Łączność bezpieczna w systemach transmisyjnych.

Zalecenia zawarte w normach CENELEC posłużyły do opracowania przez Europejską Agencję Kolejową wspólnych wymagań bezpieczeństwa dla branży kolejowej CST (*Common Safety Targets*) oraz wspólnej metody oceny bezpieczeństwa CSM (*Common Safety Method*) [8]. Metody i techniki zawarte w normach CENELEC są również przywołane w standardzie IRIS (*International Railway Industry Standard*), który został opracowany pod patronatem UNIFE (Europejskie Zrzeszenie Przemysłu Kolejowego) i przy współudziale największych producentów przemysłu kolejowego (m.in. Bombardier Transportation, Alstom Transport, Siemens Transportation). IRIS upraszcza proces weryfikacji poziomu jakości świadczonych usług oraz standaryzuje wymagania jakościowe stawiane firmom związanym z rynkiem kolejowym. Oprócz wymagań wynikających z normy ISO 9001:2008 dotyczących systemu zarządzania jakością w organizacji, które w pełni obowiązują w standardzie IRIS, zawiera on również wytyczne wynikające z norm CENELEC [14].

PN-EN 50126 jest ogólną normą dotyczącą wszystkich zastosowań kolejowych, podczas gdy pozostałe normy CENELEC dotyczą głównie systemów automatyki kolejowej. Zawarto w niej opis analizy RAMS (akronim od słów: *Reliability, Availability, Maintainability, Safety*). Dotyczy ona również aspektów ogólnych cyklu istnienia systemu (*system life cycle*) i związanych z nim zadań (rys. 1).



Rys. 1. Przykładowy cykl istnienia systemu (opracowanie własne na podstawie [16])

Z cyklu istnienia systemu automatyki kolejowej wynikają następujące działania, mające na celu uzyskanie przez ten system wymaganego poziomu bezpieczeństwa [1]:
- zdefiniowanie systemu i jego funkcjonalności (przyjęcie celów dotyczących budowy systemu, opracowanie specyfikacji systemu, stworzenie strategii obsługi, zidentyfikowanie wszelkich ograniczeń spowodowanych otoczeniem, w którym system ma funkcjonować),
- przeprowadzenie analizy ryzyka,
- określenie wymagań systemowych (przeanalizowanie wymagań wynikających z dokumentów normatywnych, określenie kryteriów akceptacji systemu),
- zdefiniowanie wymagań dla elementów systemu (określenie wymagań dla podsystemów i elementów systemu, zdefiniowanie kryteriów ich oceny i akceptacji),
- przeprowadzenie procesu projektowania i wdrażania (wykonanie projektu, zbudowanie prototypu systemu oraz wykonanie niezbędnych kontroli i walidacji).

Norma PN-EN 50126 przedstawia zarządzanie RAMS jako proces systematyczny, dostosowany do typu systemu, przeprowadzany w celu określenia wymagań dla RAMS i wykazania, że wymagania te zostały spełnione. Nie określa jednak: celów szczegółowych, kryteriów ilościowych, wymagań lub rozwiązań dla specyficznych zastosowań kolejowych. Nie definiuje również zasad dotyczących certyfikacji wyrobów kolejowych na zgodność z wymaganiami niniejszej normy oraz nie określa procesu zatwierdzenia i dopuszczania do eksploatacji systemów przez właściwy organ ds. bezpieczeństwa [6, 13].

1.1. Metody zapewnienia bezpieczeństwa rozwiązań sprzętowych

Wymagania dotyczące odbioru i zatwierdzania elektronicznych systemów (podsystemów lub urządzeń) automatyki kolejowej związanych z bezpieczeństwem zostały zdefiniowane w normie PN-EN 50129. Uwzględniono w niej cały cykl istnienia systemu (rys. 1), który można przedstawić za pomocą modelu V. Lewa strona tego modelu określana jest mianem tworzeniem systemu, zaś prawa ma związek z jego instalacją, odbiorem i eksploatacją (rys. 2).

W model V cyklu istnienia systemu można wyodrębnić trzy grupy etapów [1]:
- wstępna analiza (etapy 1, 2 i 3);
- stworzenie systemu, podsystemu i / lub wyposażenia (etapy 4-9),
- uruchomienie i użytkowanie systemu (etapy 10-14).

Norma PN-EN 50129 definiuje bezpieczeństwo jako brak niedopuszczalnego ryzyka. System uznaje się za bezpieczny, jeżeli ryzyko związane z jego działaniem jest do przyjęcia. Dla systemów automatyki kolejowej zdefiniowano cztery poziomy nienaruszalności bezpieczeństwa SIL (*Safety Integrity Level*). Poziom SIL określany jest miarą liczby zadziałań do wystąpienia usterki / błędu definiowaną poprzez współczynnik tolerowanego zagrożenia THR (*Tolerable Hazard Rate*). Najmniej restrykcyjne wymagania dotyczą poziomu SIL1, najbardziej restrykcyjne poziomu SIL4 (tab. 1).

Tab. 1. Poziomy nienaruszalności bezpieczeństwa SIL [16]

Współczynnik Tolerowanego Zagrożenia (THR)	Poziom Nienaruszalności Bezpieczeństwa (SIL)
$10^{-9} \le THR < 10^{-8}$	4
$10^{-8} \le THR < 10^{-7}$	3
$10^{-7} \le THR < 10^{-6}$	2
$10^{-6} \le THR < 10^{-5}$	1

Norma PN-EN 50129 zakłada konieczność wykazania bezpieczeństwa systemu w dokumencie nazywanym dowodem bezpieczeństwa (*safety case*). Szczególną rolę w tym dokumencie pełni raport bezpieczeństwa technicznego (*technical safety report*). Zawiera on bowiem oszacowanie współczynnika THR dla systemu, a tym samym określa poziom nienaruszalności bezpieczeństwa, który ten system spełnia. Współczynnik tolerowanego zagrożenia może być wyznaczony z zależności [4]:

$$THR = \prod_{i=1}^{n} \frac{\lambda_i}{t_{d_i}^{-1}} \cdot \sum_{i=1}^{n} t_{d_i}^{-1} \qquad (1)$$

gdzie: n - liczba kanałów, λ_i - intensywność uszkodzeń (*failure rate*) dla kanału i, t_{dt} - czas reakcji systemu na błąd od czasu powstania (*safe down rate*) dla kanału i.

Gdyby architektura systemu była oparta tylko na jednym kanale przetwarzania informacji, to na podstawie wzoru (1), wartość THR byłaby równa λ, czyli równa średniej wypadkowej intensywności uszkodzeń w systemie. Dlatego też, w celu zmniejszenia współczynnika THR, stosuje się systemy nadmiarowe (*redundant systems*), w których porównuje się informacje w równoległych kanałach przetwarzania (najczęściej „2 z 2" lub „2 z 3") [3]. Na wartość współczynnika THR wpływa intensywności uszkodzeń kanału przetwarzania, która to wielkość zależy od struktury i rodzaju tworzących go elementów. Wzór do szacowania niezawodności eksploatacyjnej dyskretnych elementów półprzewodnikowych, z których system jest zbudowany ma postać [3, 4]:

$$\lambda_p = \lambda_b (\pi_T \cdot \pi_A \cdot \pi_R \cdot \pi_S \cdot \pi_C \cdot \pi_Q \cdot \pi_E) \qquad (2)$$

gdzie: λ_p - intensywność uszkodzeń podczas eksploatacji, $\lambda_b = \lambda_0 * \pi_{ST}$ - bazowa intensywność uszkodzeń, zależna od parametru λ_0 oraz obciążenia temperaturowego i elektrycznego π_{ST}, π_T - współczynnik temperaturowy, π_A - współczynnik uwzględniający rodzaj aplikacji, π_R - współczynnik uwzględniający maksymalne dopuszczalne parametry elementu, π_S- współczynnik uwzględniający obciążenia napięciowe, π_C - współczynnik uwzględniający wpływ obecności kilku złączy w jednej obudowie lub konstrukcji elementu, π_Q - współczynnik jakościowy, π_E - współczynnik uwzględniający oddziaływanie czynników środowiskowych innych niż temperatura.

Parametry dla różnych typów elementów półprzewodnikowych, niezbędne do oszacowania intensywności uszkodzeń, można ustalić m.in. na podstawie bazy danych MIL-HDBK-217F [11]. Kolejnym parametrem we wzorze (1) jest czas reakcji systemu na błąd w kanale, który dla systemów z cyklicznym testowaniem wynosi:

$$t_d = \frac{T}{2} + NT \quad (3)$$

gdzie: T - czas cyklu testowania, NT - czas reakcji systemu na błąd od czasu wykrycia (*negation time*).

Określenie liczbowej wartości wskaźnika THR nie jest jedynym sposobem oceny ryzyka systemów automatyki kolejowej. Przydatne okazują się również inne metody wskazane w normie PN-EN 50129, takie jak analiza za pomocą procesów Markowa, czy analiza drzewa niezdatności FTA (*Fault Tree Analysis*) [11].

1.2. Metody zapewnienia bezpieczeństwa oprogramowania

Wymagania techniczne rozwoju oprogramowania programowalnych systemów elektronicznych aplikacji kolejowych określa norma PN-EN 50128 [17]. Dokument ten znajduje zastosowanie we wszelkich obszarach związanych z bezpieczeństwem, w tym: oprogramowania aplikacyjnego, systemów operacyjnych, narzędzi wspomagających, oprogramowania układowego. Oprogramowanie użytkowe obejmuje oprogramowanie wysokiego poziomu, oprogramowanie niskiego poziomu i oprogramowanie do specjalnych zastosowań (np. język drabinkowy programowalnego sterownika logicznego). Standard ten zaleca wdrożenie cyklu istnienia V, od etapu specyfikacji oprogramowania do testowania oprogramowania. Norma ta identyfikuje działania, które należy podjąć w celu uzyskania ustalonego poziomu wiarygodności. Wprowadza zalecenia, takie jak rozdzielenie oprogramowania i jego parametrów, certyfikacji narzędzi, potrzebę dokumentowania oprogramowania oraz konieczność konserwacji i wdrażania nowych wersji oprogramowania.

Zapewnienie bezpieczeństwa oprogramowania oparte jest na następujących działaniach [1]:

- przeprowadzaniu audytów mających na celu zapewnienie odpowiedniej jakości oprogramowania SQA (software quality-assurance) założonej w projekcie,
- przeglądzie planów (plan kontroli oprogramowania, plan testów, plan weryfikacji i walidacji (V&V)),
- przeglądzie wytworzonych elementów (dokumentów, kodu źródłowego, procesu parametryzacji, scenariuszy testów i wyników, oceny poziomu bezpieczeństwa),
- formułowaniu uwag i potencjalnych niezgodności,
- formułowaniu oceny oprogramowania w formie sprawozdania końcowego.

Poziomów nienaruszalności bezpieczeństwa SIL w przypadku oprogramowania jest cztery i noszą one nazwę SSIL (*Software Safety Integrity Level*):

- SSIL 0: oprogramowanie nie jest związane z bezpieczeństwem, ale konieczne jest przeprowadzenie kontroli jakości (SQA) i zarządzanie konfiguracją. Dla poziomu SSIL 0 programista (*designer / implementer*) może być jednocześnie osobą sprawdzającą (*verifier / validator*).
- SSIL 1, 2: oprogramowanie jest związane z bezpieczeństwem na poziomie średnim, który wymaga w celu zagwarantowania bezpieczeństwa, wdrożenia zasad produkcji oprogramowania. Przy tym poziomie bezpieczeństwa musi być rozdzielna rola programisty tworzącego kod programu i osoby weryfikującej poprawność.
- SSIL 3, 4: oprogramowanie jest związane z wysokim poziomem bezpieczeństwa, co wymusza nie tylko wdrożenie zasad produkcji oprogramowania, ale również użycia odpowiednich zasobów i metod (wykorzystanie metod formalnych, wykorzystanie testów dynamicznych, użycie certyfikowanych środowisk programistycznych, wykorzystanie metod symulacyjnych do walidacji modelu i / lub wyboru testów, itp.).

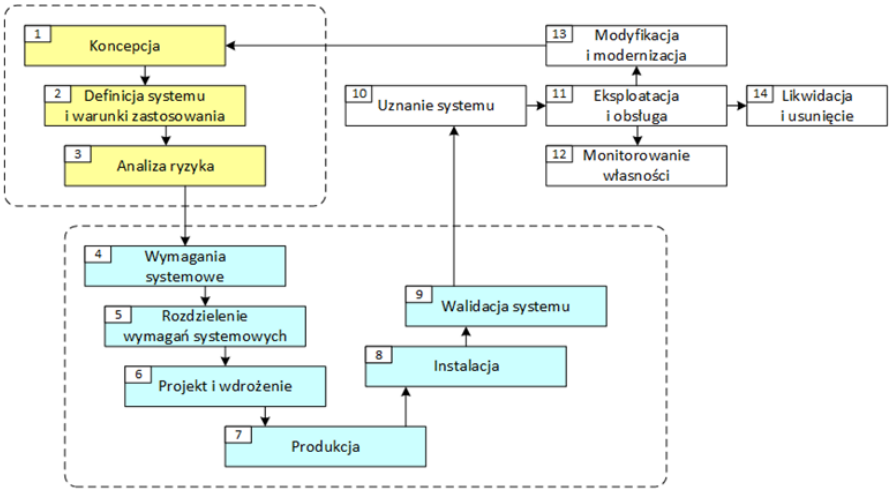
Tab. 2. Wybrane metody zapewnienia jakości oprogramowania (fragment tabeli A.5 [17])

Technika	SSIL0	SSIL1, SSIL2	SSIL3, SSIL4
1. Dowód formalny	-	R	HR
2. Analiza statyczna	-	HR	HR
3. Analiza dynamiczna i testy dynamiczne	-	HR	HR
4. Metryki	-	R	R
5. Identyfikowalność	R	HR	M
6. Analiza skutków błędów oprogramowania	-	R	HR
7. Pokrycie testu dla kodu	R	HR	HR
8. Testy funkcjonalne i testy „black-box”	HR	HR	M
9. Testy wydajności	-	HR	HR
10. Testy interfejsów	HR	HR	HR

gdzie: „M” - oznacza, że ta technika jest obowiązkowa, „HR” - oznacza, że ta technika jest bardzo polecana, „R” - oznacza, że ta technika jest polecana, „–” - oznacza brak rekomendacji.

Norma zawiera wiele zaleceń w formie tabelarycznych zestawień dla różnych obszarów dotyczących oprogramowania systemów automatyki kolejowej, w tym m.in.:

- zapewnienia jakości oprogramowania (tab. 2),
- zarządzania wymaganiami,



Rys. 2. Model V cyklu istnienia systemu (opracowanie własne na podstawie [16, 18])

– przygotowania danych,
– metod projektowania oprogramowania (tab. 3),
– modelowania i formalizacji,
– konserwacji i wdrażania oprogramowania.

Tab. 3. Wybrane metody projektowania oprogramowania (fragment tabeli A.4 [17])

Technika	SSIL0	SSIL1, SSIL2	SSIL3, SSIL4
1. Metody formalne	R	R	HR
2. Modelowanie	R	HR	HR
3. Metodologia strukturalna	R	HR	HR
4. Podejście modułowe	HR	M	M
5. Komponenty	HR	HR	HR
6. Standardy projektowania i kodowania	HR	HR	M
7. Programowanie z możliwością analizy	HR	HR	HR
8. Silna typizacja	R	HR	HR
9. Programowanie strukturalne	R	HR	HR
10. Język programowania	R	HR	HR
11. Podzbiór języka	–	–	HR
12. Programowanie obiektowe	R	R	R
13. Programowanie proceduralne	R	HR	HR
14. Metaprogramowanie	R	R	R

1.3. Metody zapewnienia bezpieczeństwa transmisji danych

Nowoczesne systemy automatyki kolejowej powszechnie stosują technologie teleinformatyczne. Rozproszona struktura tych systemów wymusza potrzebą wykorzystywania sieci komputerowych, a tym samym niezbędne jest zapewnienie bezpieczeństwa danych zarówno w procesie sterowania ruchem kolejowym, jak również w procesie diagnostycznym [15]. Wymogi bezpieczeństwa dla transmisji danych, jakie muszą być spełnione przez systemy automatyki kolejowej, określna norma PN-EN 50159 [19]. Identyfikację zagrożeń związanych z transmisją danych powinno rozpocząć się od wydzielenia tych elementów systemu, dla których zapewnienie bezpieczeństwa jest kluczowe. Następnie elementy te należy przeanalizować pod kątem ich podatności na zagrożenia [12].

Jednym z aktualnych obszarów badań jest zapewnienie bezpieczeństwa transmisji danych w rozproszonych systemach automatyki kolejowej wykorzystujących otwarty układ transmisyjny (np. bezprzewodowa transmisja danych, sieć Internet). Bezpieczeństwo wymiany informacji należy wówczas oprzeć na następujących działaniach [15, 16]:
– podejściu do systemu transmisji jako systemu niezaufanego, niezależnie od tego jakie stosuje on wewnętrzne zabezpieczenia,
– użyciu bezpiecznych funkcji transmisyjnych,
– użyciu bezpiecznych funkcji dostępu.

Głównym zagrożeniem bezpieczeństwa systemów automatyki kolejowej, wynikającym z niezaufanego systemu transmisyjnego, jest niepowodzenie w uzyskaniu przez odbiorcę ważnego i autentycznego telegramu. Stan taki może być spowodowany przez [7, 19]:
– powtórzenie telegramu (*repetition*),
– skasowanie telegramu (*deletion*),
– utworzenie telegramu przez nieautoryzowanego nadawcę (*insertion*),
– zmianę kolejności telegramów (*resequence*),
– uszkodzenie telegramu (*corruption*),
– opóźnienie w odebraniu telegramu (*delay*),
– maskaradę (*masquerade*).

Zagrożenia te, w przypadku otwartych układów transmisyjnych, są wynikiem m.in. nieznanej liczby użytkowników, którzy mogą chcieć uzyskać dostęp do sieci oraz nieznanej liczby oraz rodzaju sprzętu, który może zostać włączony do sieci. Stwarza to potencjalne zagrożenie dla bezpieczeństwa systemów, głównie możliwości pojawienia się danych o nieznanych formatach, jak również nieznanych ilościach, a także możliwości wystąpienia ataków sieciowych ze strony nieautoryzowanych użytkowników. W celu ograniczenia zagrożeń należy uwzględnić następujące warunki:
– autentyczność telegramów,
– integralność telegramów,
– określony czas przesyłania telegramów,
– kolejność telegramów.

Istnieje szereg metod zapewnienia bezpieczeństwa danych w systemach z otwartym układem transmisji, które określane są jako funkcje bezpieczeństwa [5, 19]:
– numerowanie telegramów (*sequence number*),
– stosowanie w telegramach znaczników czasu (*time stamp*),
– zdefiniowanie maksymalnego czasu oczekiwania na odpowiedź (*time-out*),
– dodawanie do telegramów identyfikatora nadawcy i odbiorcy,
– stosowanie komunikatów zwrotnych (*freedback message*),
– wykorzystywanie procedur autoryzacji (*identification*),
– stosowanie kodów bezpieczeństwa (*safety code*),
– szyfrowanie danych (*cryptographics*).

Zestawienie zagrożeń i funkcji bezpieczeństwa zalecanych w normie PN-EN 50159 przedstawiono w tabeli 4.

Tab. 4. Zestawienie zagrożeń i metod ochrony [19]

	A	B	C	D	E	F	G	H
Powtórzenie	X	X						
Skasowanie	X							
Brak autoryzacji	X			X	X	X		
Zmiana kolejności	X	X						
Uszkodzenie							X	X
Opóźnienie		X	X					
Maskarada					X	X		X

gdzie: A - numerowanie telegramów, B - stosowanie w telegramach znaczników czasu, C - zdefiniowanie maksymalnego czasu oczekiwania na odpowiedź, D - dodawanie do telegramów identyfikatora nadawcy i odbiorcy, E - stosowanie komunikatów zwrotnych, F - wykorzystywanie procedur autoryzacji, G - stosowanie kodów bezpieczeństwa, H - szyfrowanie danych.

Podczas wyboru metody transmisji danych, dla każdego z systemów bezpieczeństwa, należy odpowiedzieć na pytanie: czy możliwy jest nieautoryzowany dostęp? Jeśli w całym cyklu istnienia systemu automatyki kolejowej (rys. 1, 2) wykluczymy nieautoryzowany dostęp, wówczas nie musimy stosować technik kryptograficznych, a wyłącznie kody integralności danych, które zabezpieczą transmisję przed przypadkowymi błędami. Takie rozwiązanie stosuje się dla sieci lokalnych (LAN). Telegramy zabezpieczone w ten sposób oznaczane są w normie PN-EN 50159, jako typ A0. Natomiast inne podejście należy zastosować, gdy przyjmiemy założenie braku pewności wykluczenia nieautoryzowanego dostępu. Wówczas zaleca się stosowanie technik kryptograficznych z użyciem tajnego klucza. Jednym z możliwych rozwiązań jest dodanie kryptograficznego kodu bezpieczeństwa, np. w postaci zaszyfrowanego kodu integralności. Mówimy wówczas o telegramie typu A1. Kolejny z możliwych sposobów ochrony danych polega na szyfrowaniu całej wiadomości, czyli danych i np. kodów integralności. Tego typu telegramy oznaczono symbolem B0. W metodzie z zaszyfrowaną wiadomością koszt obliczeniowy rośnie wraz ze wzrostem wielkości wiadomości. Bardzo ważnym zagadnieniem jest wówczas odpowiedni dobór algorytmu szyfrującego, który charakteryzuje się nie tylko dobrymi właściwościami zabezpieczającymi, ale również dużą wydajnością [10]. Ostatnim z typów telegramów jest typ B1, w którym występuje zarówno niezaszyfrowany kod integralności danych,

jak również kryptograficzny kod bezpieczeństwa. W przypadku telegramów typu A1 i B1 mamy do czynienia z algorytmem charakteryzującym się niskim kosztem obliczeniowym. Można powiedzieć, że koszt ochrony danych jest stały i nie rośnie wraz z wielkością wiadomości, gdyż zależy wyłącznie od wielkości kodu integralności (np. kodu CRC lub skrótu wiadomości). Jest to niewątpliwie zaleta tej metody. Należy jednak zwrócić uwagę, że nie zapewnimy w ten sposób poufności danych w otwartych układach transmisyjnych, a jedynie umożliwimy wykrycie przypadkowej lub celowej modyfikacji danych.

Podsumowanie

Obiekty techniczne, z funkcjonowaniem których może być związane duże ryzyko, określa się mianem systemów krytycznych (*safety-critical systems*) lub systemów związanych z bezpieczeństwem (*safety-related systems*). Do grupy tej należą m.in systemy automatyki kolejowej. Aby zapobiec sytuacjom niebezpiecznym i ich następstwom stawia się przed tymi systemami duże wymagania w zakresie zapewnieni wiarygodności. W artykule zdefiniowano pojęcie wiarygodności systemów krytycznych. Omówiono również metody dotyczące zapewnienia wiarygodności systemów automatyki kolejowej, głównie w odniesieniu do jej dwóch atrybutów, czyli bezpieczeństwa i niezawodności.

Bibliografia:

1. Boulanger J. L., CENELEC 50128 and IEC 62279 Standards. ISTE Ltd and John Wiley & Sons, 2015.
2. Laprie J. C., Dependability - Its Attributes, Impairments and Means. Predictably Dependable Computing Systems. (B. Randell et al.), pp. 3-24, 1995.
3. Lewiński A., Obecne i przyszłościowe systemy sterowania ruchem kolejowym, TTS Technika Transportu Szynowego Nr 2-3, str. 28-35, 2013.
4. Lewiński A., Perzyński T., Bester L., Computer aided safety analysis of railway control systems. Journal of KONBiN, No. 2 (26), pp. 137-150, 2013.
5. Łukasik Z., Nowakowski W., Bezprzewodowe systemy sterowania ruchem kolejowym. Infrastruktura Transportu, nr 4/2013, str. 22-25, 2013.
6. Łukasik Z., Nowakowski W., Systemy automatyki kolejowej – nowe podejście w dopuszczaniu do eksploatacji. Infrastruktura Transportu, nr 5/2014, str. 10-12, 2014.
7. Łukasik Z., Nowakowski W., Wymiana informacji w systemach związanych z bezpieczeństwem. Logistyka 6/2008, 2008.
8. Łukasik Z., Nowakowski W., Zarządzanie bezpieczeństwem w transporcie kolejowym. Infrastruktura Transportu, nr 6/2013, str. 46-48, 2013.
9. Nowakowski W., Information security and privacy protection in emergency management software systems. Logistyka 4/2015, str. 8072-8077, 2015.
10. Nowakowski W., Bojarczak P., Łukasik Z., Performance analysis of data security algorithms used in the railway traffic control systems. Slovak Computer Sciences and Informatics Journal, Volume 1, pp. 281-287, 2017.
11. Nowakowski W., Ciszewski T., Młyńczak J., Łukasik Z., Failure Evaluation of the Level Crossing Protection System Based on Fault Tree Analysis. Macioszek E. & Sierpiński G. (Eds.), Book Series: Lecture Notes in Network and Systems, Volume 21, pp. 107-115, Springer-Verlag Berlin Heidelberg 2018.
12. Nowakowski W., Łukasik Z., Ciszewski T., Bezpieczeństwo transmisji danych w systemach sterowania ruchem kolejowym. Technika Transportu Szynowego (TTS), nr 12/2016, str. 473-478, 2016.
13. Nowakowski W., Czubak D., Prawo wspólnotowe i wymagania TSI dotyczące dopuszczenia do eksploatacji systemów kolejowych. Rynek Kolejowy 4/2015, str. 67-69, 2015.
14. Nowakowski W., Szczygielska A., Rola standardu IRIS w poprawie bezpieczeństwa transportu kolejowego. Technika Transportu Szynowego (TTS), nr 9/2012, str. 2751-2756, 2012.
15. Nowakowski W., Szczygielski M., Analiza bezpieczeństwa transmisji w systemie zabezpieczenia przejazdów SZP-1. Technika Transportu Szynowego (TTS), nr 9/2012, str. 2757-2761, 2012.
16. PN-EN 50126:2002, Zastosowania kolejowe - Specyfikacja niezawodności, dostępności, podatności utrzymaniowej i bezpieczeństwa. PKN 2002.
17. PN-EN 50128:2011, Zastosowania kolejowe - Systemy łączności, przetwarzania danych i sterowania ruchem - Oprogramowanie kolejowych systemów sterowania i zabezpieczenia. PKN 2011.
18. PN-EN 50129:2007, Zastosowania kolejowe - Systemy łączności, przetwarzania danych i sterowania ruchem - Elektroniczne systemy sterowania ruchem związane z bezpieczeństwem, PKN 2007.
19. PN-EN 50159:2011, Zastosowania kolejowe - Systemy łączności, sterowania ruchem i przetwarzania danych - Łączność bezpieczna w systemach transmisyjnych. PKN 2011.

Dependability of computer railway automation systems

IT development contributes to the fact that this technology is used in many fields concerning the economic and social life. It also contributes to a fast technological development of railway automations systems that are computer systems nowadays. Progress that undoubtedly must be noted, has to be followed by maintaining by these systems high quality standards, resulting mainly from ensuring safety. Such condition can be achieved, among others, through integrating works connected with reliability and security, by aiming at achieving dependability of the systems. This article presents the problem of the dependability of railway automation systems understood as their operating reliability, which allows to trust tasks accomplished by these systems.

Keywords: safety, reliability, railway automation systems.

Autorzy:

dr hab. inż. **Waldemar Nowakowski** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, w.nowakowski@uthrad.pl

prof. dr hab. inż. **Zbigniew Łukasik** – Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Wydział Transportu i Elektrotechniki, z.lukasik@uthrad.pl

mgr inż. **Krzysztof Łukomski** – Zakłady Automatyki KOMBUD S.A., krzysztof.lukomski@kombud.com.pl