WYBRANE ZAGADNIENIA FORMALIZACJI SYSTEMÓW SRK

Wiesław Zabłocki
dr hab. inż., Politechnika Warszawska, Wydział Transportu, ul. Koszykowa 75, 00-662 Warszawa, tel. 22 234 7596, e-mail: zab@wt.pw.edu.pl

Streszczenie. *W publikacji przedstawiono wybrane zagadnienia opisu formalnego na przykładzie opisu funkcji sprzeczności. Zamieszczony przykład opisu formalnego został poprzedzony rozważaniami dotyczącymi opisów nieformalnych i półformalnych w ogólnym odniesieniu do procesu projektowania systemu srk i tworzenia dokumentacji systemu. Proces tworzenia poprawnych i pełnych opisów n-p-f staje się istotny z punktu widzenia warunków bezpieczeństwa. Opracowane dokumenty i formy opisu systemu srk stają się bazowymi dokumentami dowodu bezpieczeństwa. Metoda opisu formalnego sprzeczności dróg przebiegów odwołuje się do analizy właściwości obiektów uczestniczących w drogach przebiegów, tj. uwzględnia szczegółowo właściwości obiektów drogi jazdy, drogi ochronnej i obiektów ochronnych. Zaproponowany przykład metody formalizacji pozwala określić wystarczające warunki sprzeczności. Jednakże proponuje się zachować tablicę zależności z wykazanymi sprzecznościami dróg przebiegów jako podstawową formę klasycznego opisu półformalnego.*

Słowa kluczowe: *ruch kolejowy, systemy sterowania, komputer zależnościowy, droga przebiegu, sprzeczność dróg przebiegu, opis formalny*

1. Wprowadzenie. Sformułowanie problemu

Proces projektowania, produkcji, wdrażania i eksploatacji komputerowych systemów srk ze względu na złożoność oraz spełnianie warunków bezpieczeństwa przy zachowaniu warunków integralności struktury sprzętu i oprogramowania SIL 4, wymaga stosowania szczególnych zasad i procedur. W obszarze wiedzy odnoszącej się do tego procesu istnieje szereg różnych standardów wypracowanychprzez poszczególne ośrodki, środowiska naukowe i przemysłowe, które tworzą własne standardy i nie spełniają wzajemnych warunków kompatybilności. Niezależnie od indywidualnie wypracowanych metod, proces budowy systemu srk może przebiegać metodycznie w oparciu o zalecany schemat zwany cyklem V [6, 7] z uwzględnieniem założeń analizy RAMS [6]. Początek projektowania i budowy systemu zaczyna się od opracowania założeń systemu srk, do których należą dokumenty opisu nieformalnego. W polskich uwarunkowaniach projektowych i inwestycyjnych będą to dokumenty przygotowywa-

ne na etapie zamówień np. SIWZ, OPZ[1] a także inne dokumenty nieformalne, obejmujące analizę specyfikacji lub precyzujące kolejne wymagania systemu srk, zakończone szczegółowym sformułowaniem założeń systemu srk. Po zgromadzeniu dokumentów nieformalnych, projektowane są dokumenty opisu półformalnego. Na podstawie opisu półformalnego tworzony jest opis formalny zawierający specyfikację zbiorów danych oraz relacji zależnościowych. Na podstawie specyfikacji formalnej tworzone są algorytmy i oprogramowanie. Proces tworzenia opisu półformalnego i formalnego może być także zautomatyzowany przy pomocy systemów informatycznych. Przykładowy opis sekwencyjnego tworzenia specyfikacji odniesiony do sterowników, potwierdzający przyjętą zasadę stosowania kolejnych etapów projektowania, przedstawiono np. w [2], zgodnie ze standardem IEC 61131. W procesie tworzenia systemu sterowania uczestniczą inżynierowie i eksperci różnych specjalności w tym specjaliści opracowujący nieformalne opisy w języku naturalnym, specjaliści od techniki i technologii sterowania oraz informatycy i programiści.

Do dokumentów opisu nieformalnego systemu srk należą m. in.:

- wspomniane powyżej SIWZ, OPZ,
- instrukcje np. [4, 16] i inne szczególne dokumenty, zależnie od specyficznych wymagań i celów, dla których tworzony jest system srk,
- opis pracy stacji (technologia pracy stacji),
- plan schematyczny urządzeń srk.

Do dokumentów opisu półformalnego należą m. in.:

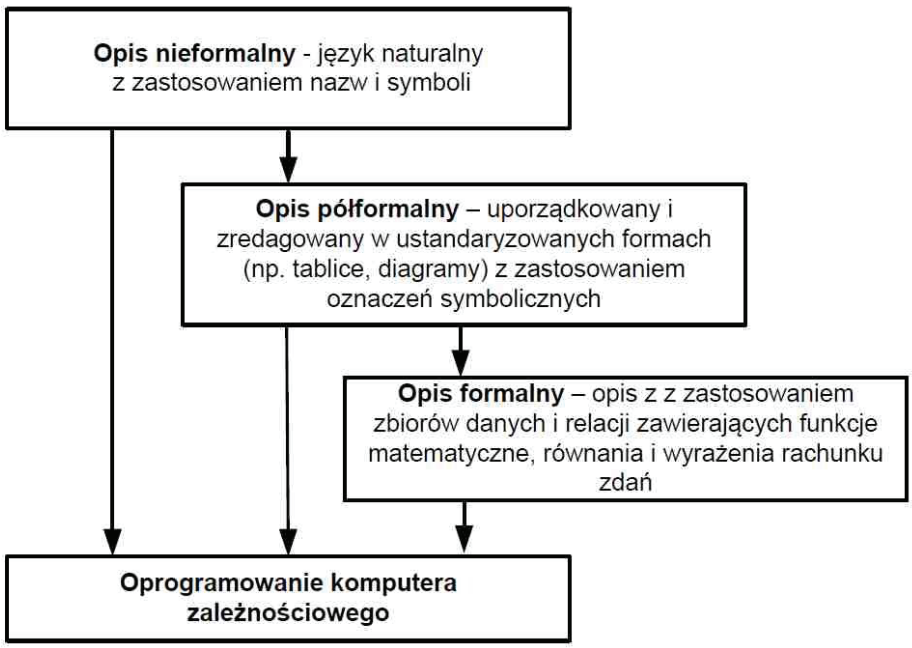
- specyfikacja dróg przebiegów w obszarze stacji z wykazaniem obiektów drogi jazdy i obiektów ochronnych,
- tablica zależności lub/i inne powiązane dokumenty,
- schemat i tablica powiązań elementów układu torowego stacji (tzw. model układu torowego),
- karty dróg przebiegów (przebiegów),
- tabela przebiegów sprzecznych.

Dokumenty opisu formalnego są zbiorami danych i relacji wyrażonych, zależnie od przyjętych standardów, poprzez mniej lub bardziej zaawansowane formy składniowe i redakcyjne. Sekwencja opracowania opisów systemu srk została przedstawiona na rys. 1.

Opracowanie opisów w ujęciu nieformalnym, półformalnym i formalnym (n-p-f), a w konsekwencji projektowanie systemów powinno być zgodne z założeniami i wytycznymi wielu dokumentów i przepisów, w szczególności [12, 13]. Początek procesu projektowania wyznacza dokumentacja opisu nieformalnego, na podstawie której powstaje opis półformalny, który z kolei staje się podstawą opisu formalnego, który jako jedyna forma opisu umożliwia algorytmizacje i stworzenie oprogramowania komputerów zależnościowych. Wszystkie formy opisu n-p-f są obligatoryjnymi dokumentami stosowanymi także do m. in. do celów walidacji, czyli sprawdzania zgodności (spójności), weryfikacji założeń i testowania [2]. Jed-

1 Odpowiednio: **s**pecyfikacja **i**stotnych **w**arunków **z**amówienia i **o**pis **p**rzedmiotu **z**mówienia

nak pomimo jednoznacznie sformułowanych wytycznych odnoszących się do zasad projektowania, praktycznie nie wskazuje się wszystkich merytorycznych elementów opisów. Umożliwia to projektantom realizację różnych koncepcji systemów srk. W [2] wskazano pewne warunki, jakie powinien spełniać każdy opis n-p-f. Do warunków tych należą jednoznaczność informacji, kompletność dokumentacji i zasada generowania kolejnego dokumentu na podstawie dokumentów uprzednio wypracowanych.



Rys. 1. Opisy systemu srk

Generalne zasady analizy wykluczania dróg przebiegów obejmują podstawowe przypadki:

- drogi przebiegów nakładają się,
- drogi przebiegów krzyżują się,
- droga ochronna danej drogi przebiegu obejmuje drogę jazdy innego przebiegu,
- drogi przebiegów różnią się odmiennym położeniem tych samych obiektów nastawczych (zwrotnice, wykolejnice) uczestniczących w tych przebiegach.

Ponadto analiza zasad wykluczania przebiegów sprzecznych, zależnie od specyfiki układu torowego i warunków bezpieczeństwa uwzględnia także:

- wymagane właściwości elementów dróg ochronnych i ochrony bocznej z uwzględnieniem możliwych alternatywnych dróg (tzw. wariantów),
- sprawdzenie warunków sprzeczności w odniesieniu do tzw. sekcji dróg przebiegów, co jest istotne w procesie zwalniania dróg przebiegów.

Przedstawiona powyżej analiza jest znamienna z tego względu, że informacje zawarte w dokumentacji n-p pozwalają dokonać specyfikacji możliwych właściwości elementów, uczestniczących drogach przebiegów przewidzianych dla danej stacji. Kolejnym istotnym zagadnieniem staje się sposób odwzorowania i zapisu specyfikacji w postaci elektronicznej. Oznacza to, że sposób zapisu w formie dokumentu elektronicznego musi posiadać strukturę zapisu umożliwiającą nieskomplikowany sposób odczytu oraz posługiwania się informacjami o pozostałych własnościach systemu srk, objętych opisem nieformalnym lub określonych na planie schematycznym urządzeń srk. W praktyce, nie wszystkie specyfikacje pozwalają na bezpośrednie, zupełne i spójne określanie zbiorów właściwości elementów układu torowego uczestniczących w poszczególnych drogach przebiegów. Jako przykłady takich właściwości, można wskazać funkcje ochronne realizowane przez elementy ochronne, drogi ochronne i elementy ochrony boczneji inne, zwłaszcza, gdy istnieją możliwości alternatywnych obiektów pełniących funkcje ochrony bocznej.

2. Przykład opisu formalnego. Sprzeczność dróg przebiegów

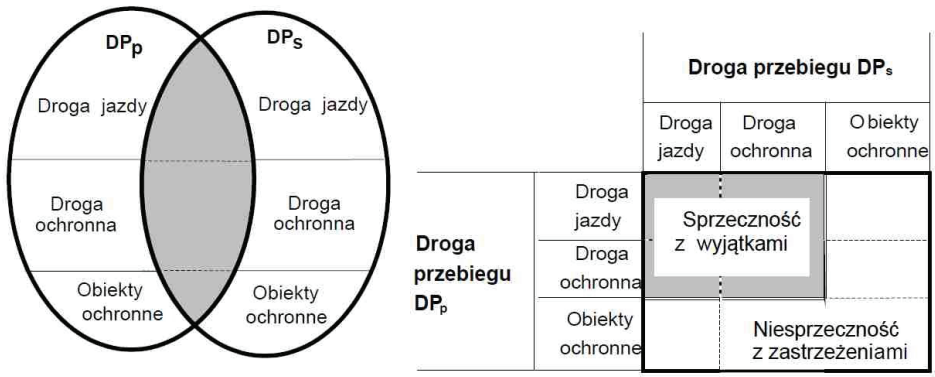
Wyznaczanie sprzeczności dróg przebiegów dokonuje się na podstawie analizy elementów każdej pary różnych dróg przebiegów $\boldsymbol{DP}_{\mathrm{p}}$ i $\boldsymbol{DP}_{\mathrm{s}}$ ze zbioru dróg przebiegów danej stacji, uwzględniając właściwości obiektów w drogach przebiegów oraz warunki sprzeczności lub niesprzeczności. Podstawą analizy jest schemat ilustrujący możliwe związki poszczególnych składników dróg przebiegów należących do $\boldsymbol{DP}_{\mathrm{p}}$ i $\boldsymbol{DP}_{\mathrm{s}}$ (rys. 2).

Analizując szczegółowo: model sprzeczności dróg przebiegów i warunek konieczny sprzeczności oraz posługując się schematem z rys. 2. określa się relacje sprzeczności z uwzględnieniem składników wszystkich dróg przebiegów. Dla przebiegów $\boldsymbol{DP}_{\mathrm{p}}$ i $\boldsymbol{DP}_{\mathrm{s}}$, dla których badane są warunki sprzeczności, poszukuje się obiektów wspólnych kolejno, w odniesieniu do dróg jazdy, dróg ochronnych i obiektów ochronnych. Drodze przebiegu $\boldsymbol{DP}_{\mathrm{p}}$, dla której bada się sprzeczność z drogą $\boldsymbol{DP}_{\mathrm{s}}$, odpowiadają wiersze schematu, zaś obiektom drogi przebiegu $\boldsymbol{DP}_{\mathrm{s}}$ odpowiadają kolumny. Na przecięciu danego wiersza z daną kolumną zaznacza się występowanie wspólnych obiektów dróg przebiegów $\boldsymbol{DP}_{\mathrm{p}}$ i $\boldsymbol{DP}_{\mathrm{s}}$. Oznacza to, że np. elementy drogi jazdy drogi przebiegu $\boldsymbol{DP}_{\mathrm{s}}$ (kolumna $\boldsymbol{DP}_{\mathrm{s}}$) może być elementem uczestniczącym np. w drodze ochronnej drogi przebiegu $\boldsymbol{DP}_{\mathrm{p}}$ (wiersz $\boldsymbol{DP}_{\mathrm{p}}$). Przedstawiony sposób analizy sprzeczności opiera się na tzw. podejściu tradycyjnym. Propozycje opisu formalnego zostaną przedstawione w dalszych rozważaniach.

Analizując na podstawie rys. 2. warunki sprzeczności można wprowadzić funkcję sprzeczności statycznej $\sigma_{\mathrm{sp}}(\boldsymbol{DP}_p, \boldsymbol{DP}_s)$ między dwoma różnymi drogami przebiegów (1).

$$\sigma_{sp}(\boldsymbol{DP}_p, \boldsymbol{DP}_s) = \begin{cases} 1 \text{ dla } \boldsymbol{DP}_p \cap \boldsymbol{DP}_s \neq \varnothing, & \text{sprzeczne drogi przebiegów, zawierają wspólne obiekty dróg jazdy i dróg ochronnych,} \\ 0 \text{ dla } \boldsymbol{DP}_p \cap \boldsymbol{DP}_s = \varnothing, & \text{niesprzeczne drogi przebiegów, nie zawierają wspólnych obiektów dróg jazdy i dróg ochronnych} \end{cases} \quad (1)$$

gdzie: $\boldsymbol{DP}_p$ i $\boldsymbol{DP}_s$ zbiory obiektów dróg przebiegów odpowiednio p i s.



Rys. 2. Przypadek dróg przebiegów zawierających wspólne elementy i schemat do analizy sprzeczności

Określona powyżej funkcja sprzeczności statycznej $\sigma_{sp}(\boldsymbol{DP}_p, \boldsymbol{DP}_s)$ między dwoma różnymi drogami przebiegów wskazuje na sprzeczność, gdy elementy różnych dróg przebiegów zawierają elementy wspólne układu torowego. Jednoznaczne określenie sprzeczności jest wynikiem dokładnej analizy właściwości elementów wspólnych należących do dróg przebiegów $\boldsymbol{DP}_p$ i $\boldsymbol{DP}_s$. W tym celu wprowadza się funkcję σ_r, którą definiuje się następująco:

$$\sigma_{r_{p,n,i,j}} : \sigma_{r_{p,n,i,j}}(p,n,j,i) \longrightarrow \{0,1\} \quad (2)$$

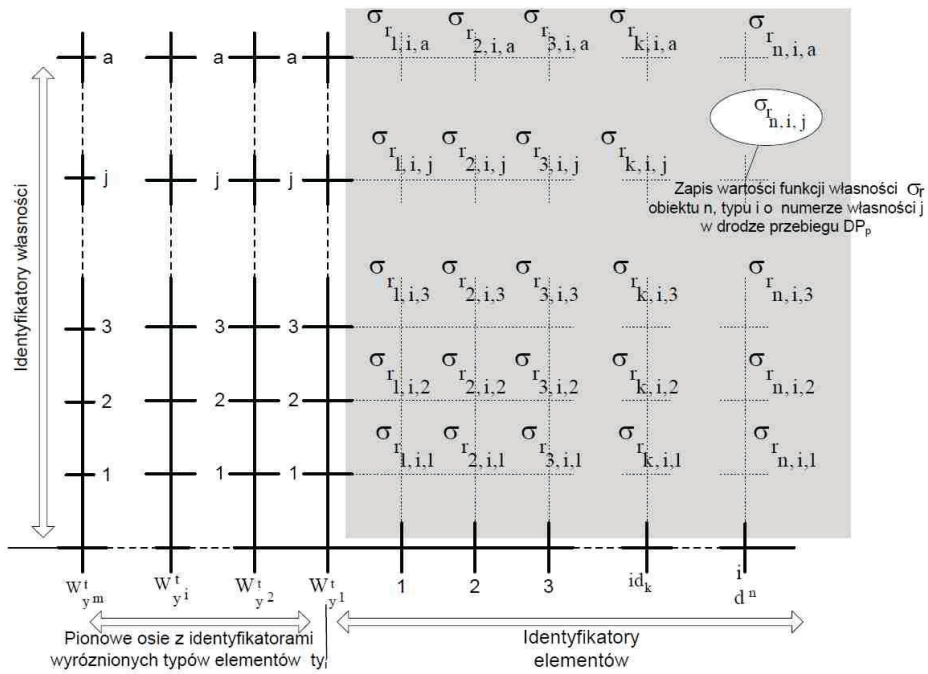
gdy $\sigma_{r_{p,k,i,j}} = 1$ to oznacza, że n – ty obiekt i –go typu **posiada** właściwość j w p – tej drodze przebiegu, tzn. może należeć do drogi jazdy, drogi ochronnej lub obiektów ochronnych, a gdy $\sigma_{r_{p,k,i,j}} = 0$ to oznacza, że n – ty obiekt i –go typu **nie posiada** właściwości j w p – tej drodze przebiegu. Interpretacja n oznaczająca globalny numer elementu infrastruktury sterowania w obszarze stacji jest liczbą naturalną, wielkość i jest także liczbą naturalną reprezentującą typ elementu, np. sygnalizator, zwrotnica, a wielkość p oznacza numer drogi przebiegu. Przykład właściwości elementu typu zwrotnica, należącej do drogi przebiegu może obejmować następujące właściwości oznaczone identyfikatorem j (poniżej wartości j od 1 do 7):

1. położenie przełożone w drodze jazdy,
2. położenie zasadnicze w drodze jazdy,

3. spełnia funkcję ochrony bocznej w położeniu przełożonym,
4. spełnia funkcję ochrony bocznej w położeniu zasadniczym,
5. znajduje się w drodze ochronnej za semaforem końcowym drogi jazdy,
6. należy do sekcji 2,
7. należy do sekcji 1.

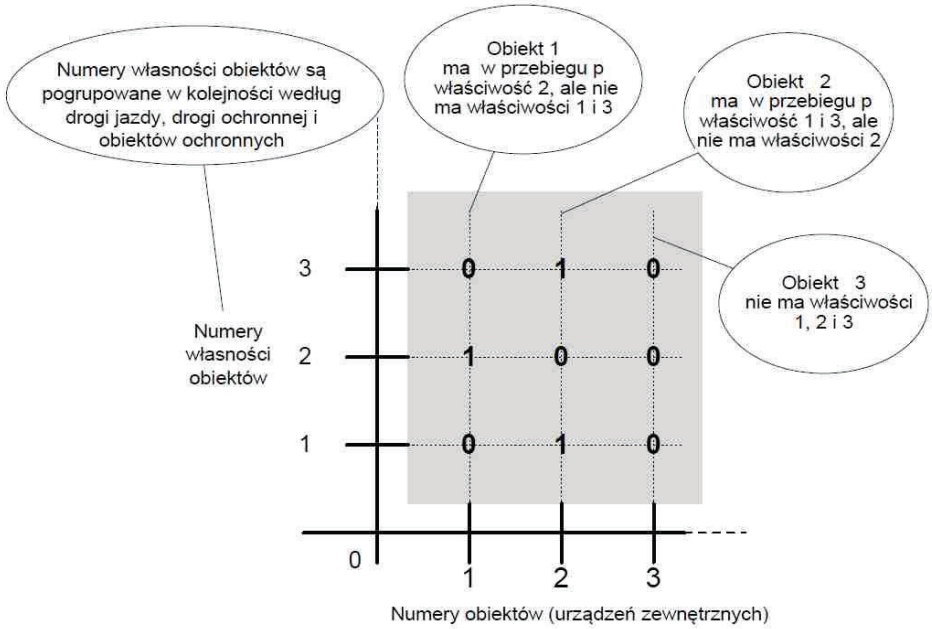
Wymienione właściwości, zależnie do specyfikacji nieformalnej, mogą zostać rozszerzone o kolejne, np. wielkość skosu, promień rozjazdu lub prędkość maksymalną. Analogicznie określa się możliwe właściwości dla pozostałych typów elementów układu torowego, w tym sterowanych i kontrolowanych urządzeń srk.

Przedstawiona na rys. 3. struktura zawierająca wartości funkcji σ_r określające właściwości uczestniczenia pewnego obiektu w pewnej drodze przebiegu zostanie zastosowana do utworzenia tzw. macierzy przebiegu (rys. 4) przechowującej informacje o wymaganych właściwościach obiektów w drogach przebiegów na stacji.

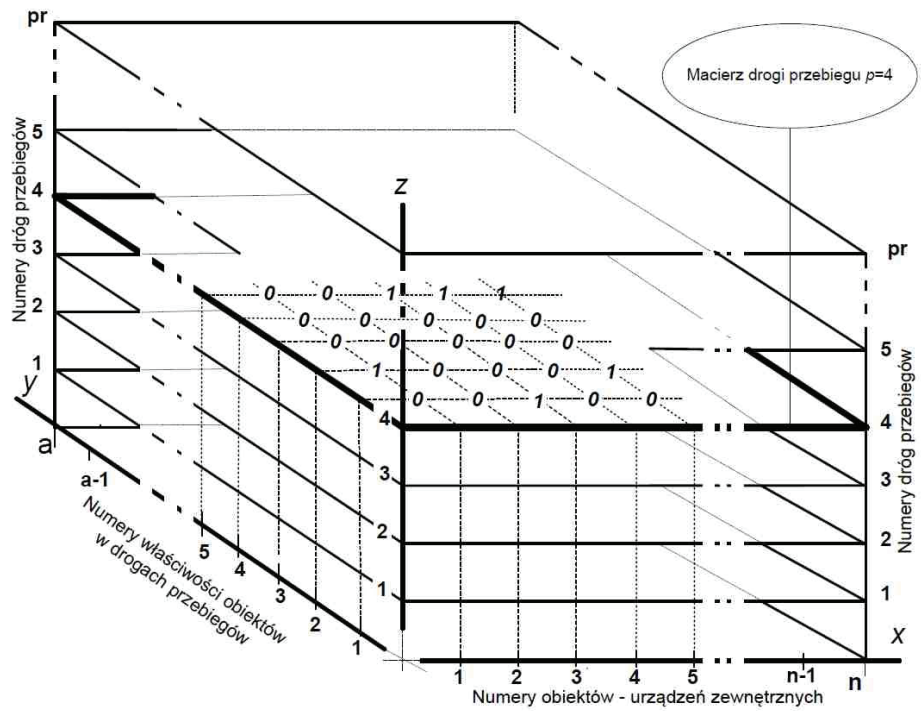


Rys. 3. Zapis wartości funkcji $\sigma_{r_{p,n,i,j}}$ *odwzorowujących właściwości obiektów należących do pewnej drogi przebiegu* p

Uwaga: indeks p *w oznaczeniu* $\sigma_{r_{p,n,i,j}}$ *nie występuje na rysunku*



Rys. 4. Macierz drogi przebiegu zawierająca statyczne informacje o wymaganych właściwościach obiektów w drodze przebiegu p



Rys. 5. Trójwymiarowa macierz statyczna MS złożona z macierzy poszczególnych dróg przebiegów

Układając macierze kolejnych przebiegów z rys. 4 „jedna nad drugą", np. według rosnących numerów dróg przebiegów uzyskuje się strukturę przestrzenną – trójwymiarową macierz MS (rys. 5), wyznaczoną trzema osiami: na osi x oznacza się numery obiektów, na osi y oznacza się numery oznaczające właściwości statyczne, na osi z oznacza się numery dróg przebiegów.

Na podstawie macierzy MS dla obiektu o danym numerze można odczytać właściwości statyczne tego obiektu dla określonej drogi przebiegu, a także we wszystkich drogach przebiegów na stacji. Jeśli dla określonego obiektu dla wskazanej drogi przebiegu występują wymagane właściwości tego obiektu w tej drodze przebiegu, to właściwości te są wyróżnione poprzez wartości „1", właściwości obiektu nieistotne dla danej drogi przebiegu przyjmują wartości „0". Stosując macierz MS i analizując zapisane w tej macierzy informacje o drogach przebiegów i właściwościach dróg przebiegów wyznacza się wartości funkcji sprzeczności $\sigma_{sp}\left(\boldsymbol{DP}_p, \boldsymbol{DP}_s\right)$ zgodnie z zasadą opisaną na początku rozdziału. Funkcję tę określa się następująco:

$$\begin{aligned} &\boldsymbol{DP}_p \subset \boldsymbol{DP},\ \boldsymbol{DP}_s \subset \boldsymbol{DP} \neg \boldsymbol{DP}_p \\ &\boldsymbol{DP} \times \left(\boldsymbol{DP} \neg \boldsymbol{DP}_p\right) = \left\{\left(\boldsymbol{DP}_p,\ \boldsymbol{DP}_s\right) : \boldsymbol{DP}_p \subset \boldsymbol{DP},\ \boldsymbol{DP}_s \subset \left(\boldsymbol{DP} \neg \boldsymbol{DP}_p\right)\right\} \\ &\sigma_{sp} : \left(\boldsymbol{DP} \times \left(\boldsymbol{DP} \neg \boldsymbol{DP}_p\right)\right) \longrightarrow \{0,\ 1\} \end{aligned} \quad (3)$$

$\sigma_{sp} = 1$ dla pary sprzecznych dróg przebiegów, gdy drogi te zawierają wspólne obiekty o właściwościach wykluczających bezpieczną jazdę pociągów, $\sigma_{sp} = 0$ dla pary niesprzecznych dróg przebiegów, gdy drogi te nie zawierają wspólnych obiektów.

3. Zakończenie

Przedstawiony w publikacji przykład opisu formalnego funkcji sprzeczności umożliwia poprzez algorytmizację opracowanie szeregu narzędzi informatycznych istotnych z punktu widzenia procesu projektowania dokumentacji systemu srk z zachowaniem warunków bezpieczeństwa, czyli m. in. opracowanie dowodu bezpieczeństwa. Metoda opisu formalnego sprzeczności dróg przebiegów odwołuje się do analizy właściwości obiektów uczestniczących w drogach przebiegów, tj. uwzględnia szczegółowo właściwości obiektów drogi jazdy, drogi ochronnej i obiektów ochronnych. W chwili obecnej klasyczna tablica zależności jest niezastąpiona, a analiza sprzeczności dróg przebiegów pozostaje istotnym czynnikiem bezpieczeństwa sterowania ruchem. Zagadnienie formalizacji opisu systemów srk, pomimo, że opracowano już wiele bezpiecznych systemów komputerowych jest nadal aktualne. Poszukiwanie nowych form standaryzacji dokumentacji - opisów systemów srk, a w tym i formalizacji opisu - służy minimalizacji ryzyka dotyczącego zachowania warunku integralności systemu na poziomie procesu projektowania.

Przedstawiona metoda formalizacji skoncentrowana na opisie zależności i funkcji sprzeczności obejmuje obszar informacji i funkcji o charakterze statycznym. Nie mniej istotny i bardziej złożony w stosunku do opisu statycznego pozostaje opis formalny części dynamicznej systemu srk. W opisie tym przez analogię do sprzeczności statycznej wprowadza się pojęcie sprzeczności dynamicznej [16]. Niniejsza publikacja jest pewną formą kontynuacji zagadnień podejmowanych w [17].

Bibliografia

[1] Buczyńska D., Wybrane zagadnienie opisu formalnego zależności stacyjnych ze szczególnym uwzględnieniem wykluczeń specjalnych. Praca magisterska, Politechnika Warszawska, Wydział Transportu, Warszawa 2015.
[2] Fischer S., Teixeira H., Engell S., Systematic Specification of a Logic Controller for a Delayed Coking Drum. Proceedings of the 11th International Symposium on Process Systems Engineering, July 2012, Singapore.
[3] Bolignano D., Le Metayer, Loiseaux C., Formal Methods in Practice: The Missing Links. A. Perspective from the Security Area. http://www.systemes-critiques.org/bolignano.pdf, w dniu 2015.11.02.
[4] Instrukcja o prowadzeniu ruchu pociągów Ir-1 (R-1), tekst ujednolicony przyjęty uchwałą Nr 176/2008 oraz zarządzeniami Nr 3/2011 i Nr 13/2014 Zarządu PKP Polskie Linie Kolejowe S.A.
[5] König N. H., The Euro-Interlocking Project Standards for Interlocking Systems in Europe Project. Presentation for Polish Railways, 8 June 2004.
[6] Maciejewski M., Metodyka budowy komputerowych systemów sterowania ruchem kolejowym. Rozprawa doktorska, Politechnika Warszawska, Wydział Transportu, Warszawa 2015.
[7] Maciejewski M., Zabłocki W., Basis of the Formalization and the Algorithmization of the Control Functions in ATC Systems, Communications in Computer and Information Science. Transport Systems Telematics, Nr 104, Springer Verlag, Berlin - Haidelberg 2010, 253 – 262.
[8] Maciejewski M., Zabłocki W., Wybrane problemy tworzenia funkcji i równań zależnościowych w systemach srk. Prace Naukowe, Politechnika Warszawska, seria Transport, z. 72, Warszawa 2010, 87 – 100.
[9] Norma PN-EN 50126: Zastosowania kolejowe. Specyfikowanie i wykazywanie nieuszkadzalności, dostępności i podatności utrzymaniowej i bezpieczeństwa (RAMS).
[10] Norma PN-EN 50128: Zastosowania kolejowe. Łączność, sygnalizacja i systemy sterowania. Programy dla kolejowych systemów sterowania i zabezpieczenia.
[11] Norma PN-EN 50129: Zastosowania kolejowe. Systemy łączności, przetwarzania danych i sterowania ruchem. Elektroniczne systemy sterowania ruchem.

[12] Wymagania bezpieczeństwa dla urządzeń sterowania ruchem kolejowym – DG PKP KA nr KA2b-5400-01/98 z dnia 06.02.1998 r.
[13] Wytyczne techniczne budowy urządzeń sterowania ruchem kolejowym Ie-4 (WTB-E10), Załącznik do zarządzenia Nr 1/2014 Zarządu PKP Polskie Linie Kolejowe S.A. z dnia 14 stycznia 2014.
[14] Zabłocki W., Podstawy opisu formalnego zależności stacyjnych., Prace naukowe TRANSPORT, Politechnika Warszawska, z. 62/2007.
[15] Zabłocki W., Interlocking Functions of ATC Station System. The Archives of Transport, vol. 20, Warszawa 2008.
[16] Zabłocki W., Modelowanie stacyjnych systemów sterowania ruchem kolejowym. Prace Naukowe TRANSPORT, z. 65, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2008.
[17] Zabłocki W., Zagadnienie sprzeczności i wykluczeń specjalnych w technice srk. Zeszyty Naukowo – Techniczne SITK Oddz. w Krakowie, nr 2(104)/2014, ISSN 1231-9155, Kraków 2014, 399 - 406