Bezpieczeństwo elektromagnetyczne węzłów wieloprotokołowych w systemach rozproszonych czasu rzeczywistego

Andrzej Kwiecień, Michał Maćkowski

Streszczenie: Tematyka przedstawiona w niniejszej pracy skupia się na testowaniu zachowania wieloprotokołowego węzła komunikacyjnego w momencie wystąpienia zakłóceń elektromagnetycznych w torze transmisyjnym. Węzeł taki – szczególnie w chwilowych przeciążeniach sieci lub w sytuacjach awaryjnych polegających na uszkodzeniu systemu transmisyjnego lub będących wynikiem zaistniałych na obiekcie przemysłowym zdarzeń – jest w stanie rozładować wzmożony ruch w sieci lub zapewnić bezpieczeństwo transmisji. W pracy wskazano na potencjalne możliwości wykorzystania sprzętu laboratoryjnego do pomiarów EMC (*ElectroMagnetic Compatybility*) w procesie testowania urządzenia i symulowania rzeczywistych zagrożeń (zakłóceń), które mogą wystąpić na obiekcie. Wyniki końcowe wskazują na prawidłowe funkcjonowanie zaproponowanego algorytmu wymian (*query distributor*) i możliwość automatycznego dostosowania topologii systemu w momencie wystąpienia zakłóceń elektromagnetycznych.

Abstract: *The main idea presented in the paper focuses on testing behavior of multi-network interface node while electromagnetic disturbances in transmission line occur. Such node is able to unload an increased traffic in network or provide the security of transmission, especially in cases of temporary overloads, system failure – damage of transmission system, or events occurring in industry area. The authors marked the potential possibilities of using equipment for EMC (Electromagnetic Compatibility) measurements in the process of testing and simulating the real threats (disturbances) that may appear in the object. The final results point out the correct work of developed query distributor system and the opportunities of automatic adjustment of the network topology in case of electromagnetic disturbances.*

1. Wstęp

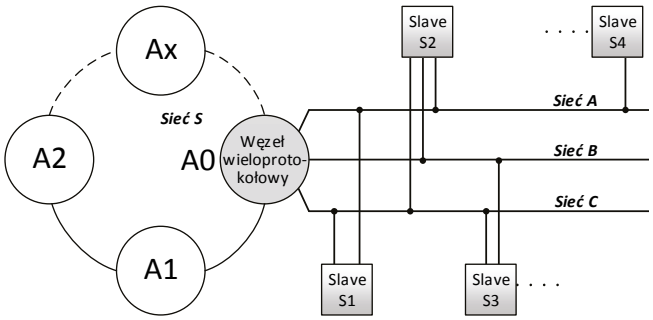
Przemysłowe systemy rozproszone czasu rzeczywistego budowane są w oparciu o kilka modeli dostępu do łącza, takich jak: *Master-Slave*, krążący żeton (*Token Bus*, *Token Ring*) oraz PDC (*Producer-Distributor-Consument*) lub inny, będący połączeniem wymienionych. Wśród handlowych nazw istnieje ich cały szereg, które po części lub w całości mają zaimplementowane modele, o których mowa.

Z punktu widzenia takich problemów, jak niezawodność, którą można podnieść przez zastosowanie redundancji, czy przeciążenie sieci (permanentne lub chwilowe), pojawia się problem zwiększenia elastyczności połączeń sieciowych, aby poprawić parametry czasowe wymian informacji. Wspomniana tu redundancja [1, 2, 3, 4] może być również wykorzystana jako sposób na poprawę parametrów czasowych transmisji [2] i może okazać się dobrym pomysłem na poprawę przepustowości [1, 5]. Należy jednak pamiętać, iż największe korzyści z wykorzystania łącza redundantnego do poprawy parametrów czasowych transmisji mają miejsce wtedy, gdy redundancja z innych powodów (np. niezawodnościowych) już w systemach istnieje [6, 7]. Jest to spowodowane znacznymi kosztami rozwiązań systemów z redundancją.

Jedną z cech charakterystycznych przemysłowych systemów czasu rzeczywistego są wysokie wymagania dotyczące niezawodności działania. W poprzedniej pracy autorów [8] przedstawiono propozycję węzła wieloprotokołowego w systemach rozproszonych czasu rzeczywistego w celu zwiększenia niezawodności komunikacji. Ponadto przedstawiono rozważania nad metodą przyspieszenia wymiany danych w rozproszonych systemach sterowania, z zastosowaniem takich węzłów. Zaproponowana w pracy metoda zakładała konstrukcję sprzętową i programową w oparciu o nowy oryginalny protokół komunikacyjny węzła, który mógłby obsługiwać różne protokoły, pozwalając na jednoczesną wymianę danych różnymi magistralami. Dzięki zaproponowanej metodzie wzrosła nie tylko przepustowość sieci, ale również bezpieczeństwo przesyłania danych.

Interesującym rozwiązaniem jest wykorzystanie węzła wieloprotokołowego. Węzeł taki – szczególnie w chwilowych przeciążeniach sieci lub w sytuacjach awaryjnych polegających na uszkodzeniu systemu transmisyjnego (kabel, światłowód, koprocesor sieciowy itp.) lub będących wynikiem zaistniałych na obiekcie przemysłowym zdarzeń – będzie w stanie rozładować wzmożony ruch w sieci [9, 10] lub zapewnić bezpieczeństwo transmisji.

Na rys. 1 przedstawiono ideę sieci wieloprotokołowej z jednym wyróżnionym węzłem A0, który dodatkowo posiada trzy interfejsy komunikacyjne z sieciami A, B i C. Do sieci A podłączono abonentów S1 i S4, do sieci B abonentów S2 i S3, a do sieci C abonentów S1, S2 i S3. Zakłada się dla porządku, że węzeł A0 jest stacją *Master* dla trzech różnych sieci A, B, C. Oczywiste jest ponadto, że sieci A, B i C mogą posługiwać się różnymi protokołami i różnymi mediami transmisyjnymi.



Rys. 1. Schemat sieci z zaznaczonym węzłem wieloprotokołowym

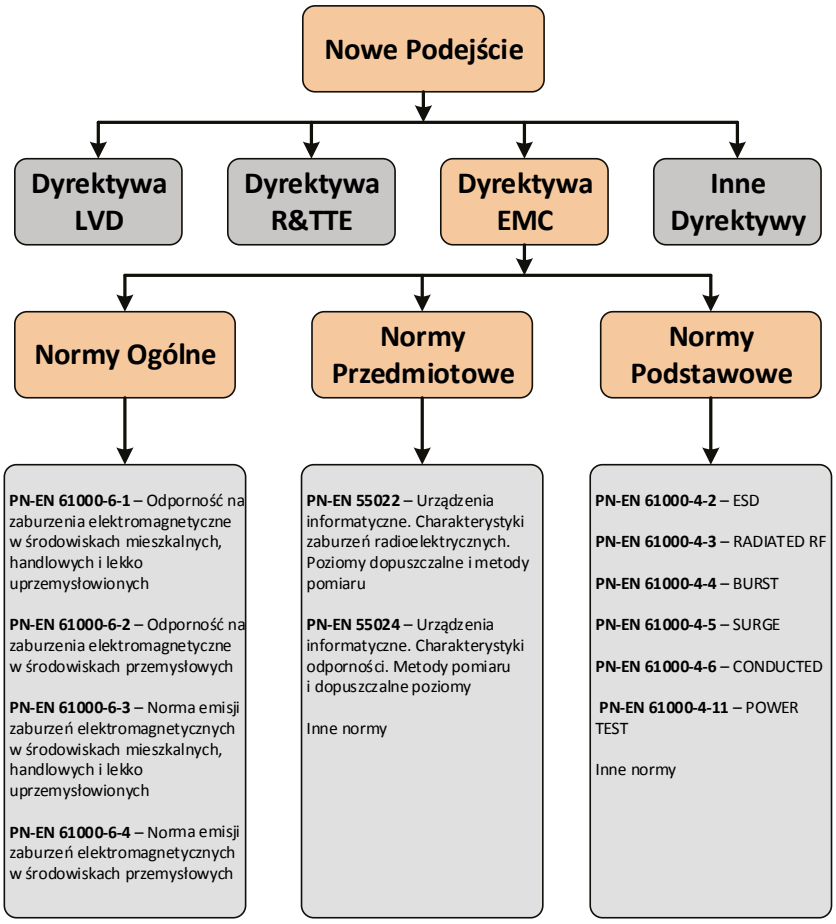
W dalszej części artykułu przedstawiono propozycję rzeczywistego rozwiązania węzła sieciowego wyposażonego w więcej niż jeden interfejs komunikacyjny. Rozwiązanie zostało opracowane na przykładzie 8-bitowego mikrokontrolera AVR ATMega2560, gdzie każdy mikrokontroler wyposażony jest w 4 układy UART umożliwiające komunikację mikrokontrolera z urządzeniami zewnętrznymi. W niniejszej pracy poruszono problem bezpieczeństwa elektromagnetycznego zaproponowanego rozwiązania. Wskazano również na potencjalne możliwości wykorzystania sprzętu laboratoryjnego do pomiarów EMC (*ElectroMagnetic Compatybility*) w procesie testowania urządzenia (*multinetwork interface node*) i symulowania rzeczywistych zagrożeń (zakłóceń), które mogą wystąpić na obiekcie. Testy takie pozwolą nie tylko zweryfikować poprawność budowy zaproponowanej platformy sprzętowej, ale również sprawdzić skuteczność zaproponowanego algorytmu sterowania wymianami (*Query Scheduler*).

2. Kompatybilność Elektromagnetyczna – Dyrektywa EMC

Na początku lat osiemdziesiątych XX w. w krajach należących do ówczesnej Europejskiej Wspólnoty Gospodarczej stwierdzono, że prawo nie jest w stanie nadążać za szybko zmieniającymi się normami technicznymi. W związku z tym w 1985 roku wprowadzono tzw. Nowe Podejście (*New Approach*) do harmonizacji regulacji technicznych. Jego istota sprowadza się do kilku podstawowych reguł:

- Dyrektywy Nowego Podejścia odnoszą się do dużych grup wyrobów i określają wymagania w sposób bardzo ogólny (tzw. wymagania zasadnicze), są one związane tylko i wyłącznie z bezpieczeństwem, zdrowiem czy ochroną środowiska.
- Wszystkie szczegółowe specyfikacje i wymagania techniczne stawiane wyrobom wprowadzanym na rynek zawarte są w zharmonizowanych normach europejskich.
- Tylko produkt, który spełnia wymagania zasadnicze i oznaczony jest znakiem „CE" (fr. *Conformité Européenne),* ma prawo być wprowadzany na rynek dowolnego państwa członkowskiego Unii Europejskiej.

Na rysunku 2 przedstawiono hierarchię dokumentów unijnych z uwzględnieniem Dyrektywy EMC. Dyrektywa Kompatybilności Elektromagnetycznej (*Electromagnetic Compatibility EMC*) w Unii Europejskiej została wprowadzona w 1989 roku. Od tamtego czasu wszystkie urządzenia elektroniczne czy



Rys. 2. Hierarchia dokumentów unijnych dotyczących Dyrektywy EMC

informatyczne wprowadzane na rynek muszą być zgodne z jej wymaganiami zasadniczymi. Definicja samej kompatybilności elektromagnetycznej, zawarta w dyrektywie, określa w sposób bardzo ogólny wymagania stawiane urządzeniom: „Kompatybilność elektromagnetyczna oznacza zdolność urządzenia do zadowalającego działania w środowisku elektromagnetycznym bez powodowania nadmiernych zaburzeń elektromagnetycznych w stosunku do innych urządzeń działających w tym środowisku" [11].

Oznacza to, że każde urządzenie musi wykazywać zdolność do prawidłowego funkcjonowania w momencie, gdy jest ono narażone na zaburzenia elektromagnetyczne, ale jednocześnie nie może emitować zbyt dużych zaburzeń, które mogłyby zakłócać pracę innych urządzeń. Tak więc z jednej strony układ musi być odporny na zaburzenia, a z drugiej strony nie może emitować zbyt dużych zaburzeń. Występuje tutaj zawsze podział na wymaganą odporność EMI (*Electromagnetic Immunity*) oraz dopuszczalną emisyjność (*Electromagnetic Interference*) – są to dwa podstawowe aspekty kompatybilności elektromagnetycznej.

Badania EMC mają na celu dodatkowo zwiększenie niezawodności urządzeń elektronicznych i systemów informatycznych działających w środowisku, w którym występują coraz większe zaburzenia elektromagnetyczne. Bardzo istotną cechą tych badań jest także możliwość określenia wpływu zaburzeń elektromagnetycznych na transmisję danych w sieciach i systemach informatycznych. Dyrektywa Kompatybilności Elektromagnetycznej, najważniejsze normy zharmonizowane z tą dyrektywą, sposoby pomiarów oraz stanowiska badawcze zostały szczegółowo omówione w pracach [12, 13].

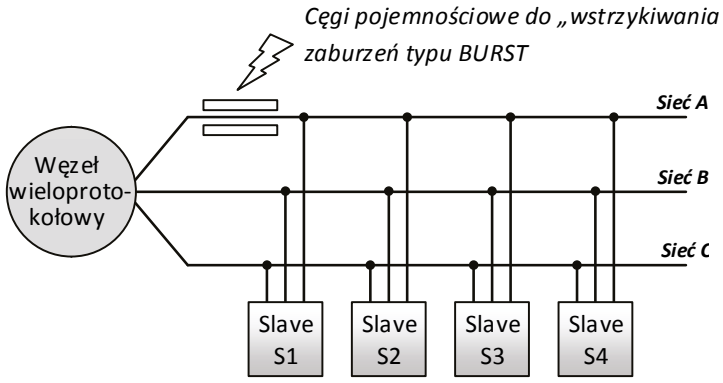
W zaproponowanym rozwiązaniu sprzętowym (punkt 3) węzeł wieloprotokołowy zarządza ruchem trzech interfejsów sieciowych opartych na standardzie RS485. Dlatego w dalszej części omówiono zagadnienia związane z kompatybilnością elektromagnetyczną tego standardu. Aplikacje przemysłowe wymagają komunikacji pomiędzy poszczególnymi modułami, często oddalonymi od siebie. Standard przesyłu danych w sieci RS485 jest najczęściej wykorzystywanym standardem elektrycznym w takich aplikacjach, jak automatyka przemysłowa, kontrola procesów technologicznych. Norma TIA/EIA485A opisuje warstwę fizyczną interfejsu RS485 i zazwyczaj używana jest z jakimś protokołem wyższych warstw, takim jak Profibus, Interbus czy Modbus [14, 15].

W rzeczywistych aplikacjach przemysłowych sieci oparte o RS485 zazwyczaj pracują w trudnych warunkach zakłóceń elektromagnetycznych. Znaczne przepięcia w liniach, spowodowane wyładowaniami atmosferycznymi oraz elektrostatycznymi i innymi zjawiskami, są w stanie uszkodzić porty urządzeń w sieci. Aby sprostały one stawianym wymaganiom i funkcjonowały poprawnie, w realnym systemie, spełnić muszą szereg wymagań stawianych przez normy EMC. Wymogi te dzielą się głównie na trzy kategorie dotyczące wyładowań elektrostatycznych, stanów przejściowych i wyładowań.

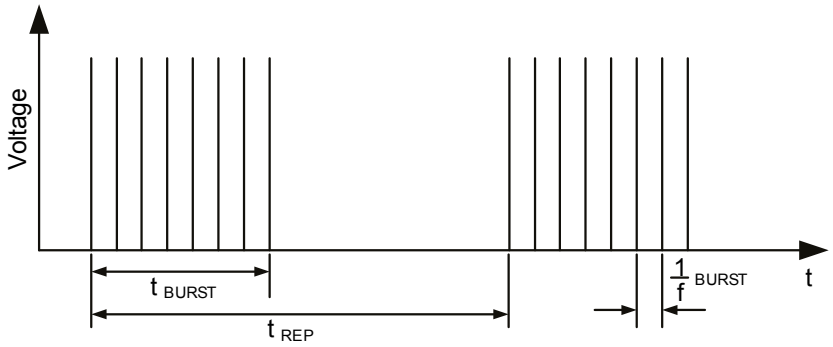
Powstało już wiele prac [16, 17, 18], w których autorzy skupiają się na testowaniu odporności standardu RS485 na zaburzenia elektromagnetyczne oraz przedstawiają środki zaradcze podnoszące jego odporność. Niezależnie od zastosowanego medium transmisyjnego oraz protokołu transmisji danych zawsze istnieje pewien element systemu, który narażony na zaburzenia o odpowiedniej częstotliwości i amplitudzie spowoduje zakłócenie pracy całego systemu lub jego części [19, 20]. Wymuszenie błędów pojawiających się na magistralach danych w wyniku narażenia systemu na działanie sygnałów zaburzających pozwoli na sprawdzenie zachowania zaproponowanego systemu/algorytmu wymian i wyboru tras, jakie mogłoby mieć miejsce w rzeczywistej sytuacji.

3. Stanowisko i procedura badawcza

Do realizacji podstawowych badań empirycznych zaproponowano nowe



Rys. 3. Schemat stanowiska badawczego. Transmisja w sieci A zakłócana jest poprzez cęgi pojemnościowe indukujące zaburzenia



Rys. 4. Parametry impulsów EFT/BURST zgodnie z normą PN-EN 61000-4-4 [21] wykorzystywaną w trakcie prowadzenia badań

stanowisko (rys. 3) z zastosowaniem układów mikroprocesorowych. Ze względu na złożone aspekty proponowanego rozwiązania autorzy zaproponowali tym razem do testów stanowisko badawcze oparte o otwartą platformę programowania mikrokontrolerów Arduino. Dla potrzeb badań eksperymentalnych system składał się z jednego węzła wieloprotokołowego oraz czterech stacji podrzędnych. Wszystkie węzły systemu zbudowane były w oparciu o 8-bitowe układy mikrokontrolerów AVR ATMega2560 firmy Atmel, wyposażone w trzy interfejsy RS485 mogące pracować całkowicie niezależnie. Wszystkie trzy sieci: A, B oraz C wykorzystują do komunikacji tę samą warstwę fizyczną RS485 z protokołem *Master-Slave* Modbus RTU. Układem typu *Master* jest węzeł wieloprotokołowy (*multi network interface node*). Układy typu *Slave* podłączone są do wszystkich trzech sieci.

Z punktu widzenia badań empirycznych rozwiązanie to pozwoli na przetestowanie metod z użyciem różnych form dostępu do łącza, tj. *Master-Slave*, *Token-Ring* itp. Kolejnym atutem przygotowanego rozwiązania jest możliwość rozbudowy układu o komunikację w sieci Ethernet, CAN oraz w bezprzewodową komunikację wg ZigBee. Zaprojektowane stanowisko jest bardzo mocnym punktem omawianego przedsięwzięcia. Z punktu widzenia organizacji jest ono bardzo elastyczne, a rozwiązania, które są w nim stosowane, są nowatorskie i dostępne praktycznie dla każdego w przeciwieństwie do drogich systemów PLC. Bazowanie na otwartej platformie Arduino pozwala na pełne panowanie nad komunikacją w systemie.

W celu wymuszenia błędów na jednej z magistral danych wykorzystano stanowisko laboratoryjne do prowadzenia testów odporności na zaburzenia EFT (*Electrical Fast Transient*) – zgodnie z normą podstawową PN-EN-61000-4-4 (rys. 2). Ten rodzaj narażenia dobrze charakteryzuje zjawiska pochodzące od stanów przejściowych, łączeniowych, towarzyszące przełączeniom obwodów zawierających obciążenia indukcyjne, związane z drganiem styków przekaźników elektromagnetycznych itp. Powstające wówczas impulsy elektryczne cechują się krótkimi, nanosekundowymi czasami narastania. Test odporności na narażenia EFT/BURST jest realizowany za pomocą serii pewnej liczby zakłóceń impulsowych, podawanych z generatora probierczego, sprzężonych odpowiednio do linii zasilania oraz wejść sterujących i sygnałowych badanego obiektu [21].

W trakcie trwania testów magistrala A została umieszczona wewnątrz pojemnościowych cęgów sprzęgających, wykorzystywanych do wprowadzania zakłóceń EFT do linii wejścia/wyjścia. Przebieg i podstawowe parametry czasowe serii impulsów zaburzających zostały przedstawione na rysunku 4. Czas trwania pojedynczej serii impulsów wynosi t_{Burst} = 15 ms, a częstotliwość powtarzania impulsów 5 kHz. Pomiędzy kolejnymi seriami zaburzeń następowała przerwa o czasie ok. 300 ms.

Układ *Master* został przygotowany do realizacji 8 zapytań w odstępach 90 ms. Czas potrzebny na realizację każdego zapytania T_{EX} wynosił 20 ms. W odróżnieniu od standardowej implementacji wymian informacji w sieciach *Master-Slave* w omawianym przypadku harmonogram wymian nie był określony przed uruchomieniem systemu. W opisywanym rozwiązaniu ustalenie harmonogramu wymian jest dynamiczne i bazuje na aktualnym obciążeniu (stanie) magistral komunikacyjnych.

Moduł programowy odpowiedzialny za realizację harmonogramu wymian (*Query Scheduler* – QS) wybiera kolejne wymiany do realizacji na podstawie aktualnego stanu magistral komunikacyjnych oraz znaczników czasowych (*timestamps*) poprzednio zrealizowanych wymian. W przypadku błędów komunikacyjnych w sieci A, będących skutkiem oddziaływania zaburzeń elektromagnetycznych – wymiana informacji ma nastąpić poprzez inne magistrale komunikacyjne, np. B oraz C.

W kolejnym punkcie przedstawiono wyniki oddziaływania przedstawionych zaburzeń na zachowanie węzła wieloprotokołowego.

Tabela 1. Realizacja wymian w trakcie trwania eksperymentu

	Czas pozostały do realizacji kolejnej wymiany								Realizowana wymiana		
	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Magistrala A	Magistrala Bus B	Magistrala Bus C
0	90	90	90	90	90	90	90	90	Q1	Q2	Q3
1	70	70	70	70	70	70	70	70	Q1	Q2	Q3
2	70	70	70	50	50	50	50	50	Q4	Q5	Q6
3	50	50	50	70	70	70	30	30	Q7	Q8	Q1
4	70	30	30	50	50	50	70	70	Q2	Q3	Q4
5	50	70	70	70	30	30	50	50	Q5	Q6	Q1
6	70	50	50	50	70	70	30	30	Q7	Q8	Q2
7	50	70	30	30	50	50	70	70	Q3	Q4	Q1
8	70	50	70	70	30	30	50	50	Q5	Q6	Q2
	...				...					...	
15	50	70	50	50	70	70	30	30	Diag.	Q7	Q8
16	30	50	30	30	50	50	70	70	Diag.	Q1	Q3
17	70	30	70	10	30	30	50	50	Diag.	Q4	Q2
18	50	70	50	70	10	10	30	30	Diag.	Q5	Q6
19	30	50	30	50	70	70	10	10	Diag.	Q7	Q8
20	10	30	10	30	50	50	70	70	Diag.	Q1	Q3
21	70	10	70	10	30	30	50	50	Diag.	Q2	Q4
22	50	70	50	70	10	10	30	30	Diag.	Q5	Q6
	...				...					...	
41	70	10	70	10	30	30	50	50	Q2	Q4	Q5
42	50	70	50	70	70	10	30	30	Q6	Q7	Q8
43	30	50	30	50	50	70	70	70	Q1	Q3	Q2
44	70	70	70	30	30	50	50	50	Q4	Q5	Q6

4. Wyniki badań

W tabeli 1 przedstawiono realizację zdefiniowanej listy wymian. Numery w poszczególnych wierszach określają cykliczność wymian i definiują maksymalny czas, w którym dane zapytanie powinno zostać wysłane. W początkowym etapie czas ten wynosi 90 ms (maksymalny czas pomiędzy realizacją wymiany) i jest taki sam dla wszystkich wymian (wiersz #0). Trzy pierwsze zapytania z listy są wybierane do realizacji (Q1 – Q3), każde realizowane poprzez inną magistralę komunikacyjną (prawa strona tabeli 1). Etap ten można określić jako inicjalizujący pracę systemu, podczas którego tworzony jest wstępny harmonogram wymian.

W kolejnym kroku (wiersz #1) czas na realizację poszczególnych wymian wynosi 70 ms i ponownie realizowane są wymiany Q1 – Q3. Ponownie ustalany jest czas cyklu wymiany, który wynosi 70 ms dla transakcji Q1, Q2 oraz Q3 (wiersz #2, 90 ms – 20 ms). W związku z tym, że pozostałe wymiany nie zostały zrealizowane, czas na ich realizację zostaje pomniejszony i ustawiony na wartość 50 ms. W kolejnym kroku wymiany Q4 – Q6 zostają wybrane do realizacji (wiersz 2 – kolor szary), a czas na realizację pozostałych wymian, które nie miały miejsca, zostaje pomniejszony o kolejne 20 ms.

Procedura ta jest kontynuowana do momentu wystąpienia zaburzeń elektromagnetycznych (wprowadzone zaburzenia typu BURST) na magistrali komunikacyjnej A. Ma to miejsce po czasie 0,28 s od momentu uruchomienia komunikacji (wiersz #15). Układ *Master* wykrywa błędy na magistrali komunikacyjnej i rozpoczyna realizację wszystkich wymian tylko poprzez pozostałe dwie magistrale B oraz C.

W tym samym czasie układ *Master* wysyła pewne wymiany diagnostyczne magistralą A w celu zdiagnozowania końca wystąpienia zakłóceń. Ma to miejsce po czasie 0,8 s od startu systemu (wiersz #41). Od tego momentu wymiany realizowane są ponownie poprzez wszystkie trzy sprawne magistrale. Harmonogram wymian jest dynamicznie modyfikowany i dostosowany do aktualnego stanu systemu z uwzględnieniem maksymalnego (nieprzekraczalnego) czasu trwania wymiany równego 20 ms.

5. Wnioski

Głównym celem niniejszej pracy było sprawdzenie zachowania wieloprotokołowego węzła komunikacyjnego w momencie wystąpienia zakłóceń elektromagnetycznych w torze transmisyjnym. Zaproponowane rozwiązanie uwzględnia zarówno część sprzętową, jak również programową, obejmującą zarządzanie wieloma interfejsami komunikacyjnymi. Celem takiego rozwiązania jest wykorzystanie zalet redundantnych interfejsów komunikacyjnych oraz protokołów

komunikacyjnych czasu rzeczywistego. Umożliwia to zarówno zwiększenie niezawodności systemu, jak i większą wydajność podsystemu komunikacyjnego.

Wyniki badań w poprzednim punkcie wskazują na prawidłowe funkcjonowanie zaproponowanego algorytmu wymian (*query distributor*). W chwili wystąpienia zakłóceń na magistrali A komunikacja pomiędzy węzłami sieci odbywa się tylko poprzez magistrale B oraz C. W takiej sytuacji zmiana topologii sieci jest nieplanowana i została narzucona z powodu wystąpienia błędów. Poza zwiększeniem przepustowości sieci w normalnych warunkach pracy, największą zaletą zaproponowanego rozwiązania jest możliwość automatycznego dostosowania topologii sieci w chwili wystąpienia zakłóceń w systemie, tak by zapewnić możliwość komunikacji ze wszystkimi węzłami sieci.

W przyszłości planowane jest rozbudowanie stanowiska testowego poprzez dodanie innych sposobów komunikacji pomiędzy węzłami w sieci, np. Ethernet, CAN czy w sposób bezprzewodowy. Każde media transmisyjne (np. przewody – skrętki, światłowody itp.) oraz standardy komunikacyjne są podatne na inny rodzaj zaburzeń elektromagnetycznych (częstotliwość, amplitudę). Zbudowanie więc stanowiska opartego na różnych interfejsach komunikacyjnych pozwoli w chwili wystąpienia zakłóceń na wybór tej magistrali (sieci), w której komunikacja będzie najbardziej optymalna i niezakłócona. Wykorzystanie aparatury badawczej w Laboratorium Kompatybilności Elektromagnetycznej pozwala na wytwarzanie zaburzeń elektromagnetycznych, jakie mogą wystąpić na obiekcie przemysłowym. Tym samym możliwe jest sprawdzenie i dostosowanie zachowania omawianego systemu do rzeczywistych warunków, jakie mogą wystąpić na obiekcie, a nie tylko na drodze symulacji, np. programowej.

Literatura

[1] Kwiecień B., Sidzina M.: *The algorithms of transmission failure detection in Master-Slave networks*. [in:] Kwiecień A., Gaj P., Stera P. (ed.): *CN 2012. CCIS*, vol. 291, pp. 289–298. Springer, Heidelberg 2012.

[2] Kwiecień A., Sidzina M.: *Dual bus as a method for data interchange transaction acceleration in distributed Real Time systems*. [in:] Kwiecień A., Gaj P., Stera P. (ed.): *CN 2009. CCIS*, vol. 39, pp. 252–263. Springer, Heidelberg 2009.

[3] Wei L., Xiao Q., Xian-Chun T. et al.: *Exploiting redundancies to enhance schedulability in fault-tolerant and realtime distributed systems. Systems, Man and Cybernetics, Part A: Systems and Humans*, IEEE Transactions on, vol. 39, issue 3, pp. 626–639, 2009.

[4] Neves F.G.R., Saotome O.: *Comparison between redundancy techniques for real time applications*. Information Technology: New Generations, IEEE, pp. 1299–1310, Las Vegas 2008.

[5] Kirrmann H., Weber K., Kleineberg O. et al.: *Seamless and low-cost redundancy for substation automation systems (high availability seamless redundancy, HSR)*. Power and Energy Society General Meeting, IEEE, pp.1–7, 2011.

[6] IEC 62439, Committee Draft for Vote (CDV): *Industrial communication networks: high availability automation networks*, chapter 6, entitled Parallel Redundancy Protocol, 2007.

[7] IEC 62439, Committee Draft for Vote (CDV): *Industrial communication networks: high availability automation networks*, chapter 5, entitled Media Redundancy Protocol based on a ring topology, 2007.

[8] Kwiecień A., Maćkowski M., Sidzina M.: *The concept of using multi-protocol nodes in real-time distributed systems for increasing communication reliability*. [in:] Kwiecień A., Gaj P., Stera P. (ed.): *CN 2013. CCIS*, vol. 370, pp. 177–188, Springer, Heidelberg 2013.

[9] Gaj P.: *The concept of a Multi-Network approach for a dynamic distribution of application relationships*. [in:] Kwiecień A., Gaj P., Stera P. (ed.): *CN 2011. CCIS*, vol. 160, pp. 328–337. Springer, Heidelberg 2011.

[10] Gaj P., Jasperneite J.; Felser M.: *Computer communication within industrial distributed environment-a survey*. Industrial Informatics, IEEE Transactions on, vol. 9, no. 1, pp. 182–189, 2013.

[11] Directive 2004/108/EC of the European Parliament and of the Council (http://europa.eu.int).

[12] Montrose M.I., Nakauchi E.M.: *Testing for EMC compliance: approaches and techniques*. John Wiley and Sons, Institute of Electrical and Electronics Engineers, Canada 2004.

[13] Williams T.: *EMC for product designers*. Elsevier LTD, Oxford 2001.

[14] Pereira C.E., Neumann P.: *Industrial communication protocols*. Springer Handbook of Automation, pp. 981–999, Springer, Heidelberg 2009.

[15] Petr K.: *Advanced industrial communications. Towards intelligent engineering and information technology*. Studies in computational intelligence, vol. 243, pp. 365–376, Springer, Heidelberg 2009.

[16] Zhang W., Lin J., Pen L., et al.: *Application of RS485 for communication and synchronization in distributed electromagnetic exploration system*. Electric Information and Control Engineering (ICEICE), International IEEE conference, pp. 4815–4818, Wuhan 2011.

[17] Ajay Kumar V.: *Overcoming data corruption in RS485 communication*. Electromagnetic Interference and Compatibility, International IEEE conference, pp. 9–12, Madras 1995.

[18] Scanlon J., Rutgers K.: *Safeguard Your RS-485 communication networks from harmful EMC events*. „Analog Devices" 47/2013.

[19] Novak J.: *Electromagnetic compatibility of fieldbus communication. Fieldbus technology.* Industrial network standards for Real-Time distributed control. pp. 413–433, Springer, Heidelberg 2003.

[20] Kryca M.: *Hardware aspects of data transmission in coal mines with explosion hazard*. [in:] Kwiecień A., Gaj P., Stera P. (ed.) *CN 2013. CCIS*, vol. 370, pp. 517–530, Springer, Heidelberg 2013.

[21] Electromagnetic Compatibility (EMC) Part 4-4: Testing and Measurement Techniques-Electrical Fast Transient/Burst Immunity Test (IEC 61000-4-4:2012 (Ed. 3.0))

Praca była współfinansowana ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego (nr umowy o dofinansowanie projektu: UDAPOKL.04.01.0100106/09)

prof. dr hab. inż. Andrzej Kwiecień
dr inż. Michał Maćkowski
Politechnika Śląska, Instytut Informatyki,
e-mail: andrzej.kwiecien@polsl.pl
e-mail: michal.mackowski@polsl.pl

artykuł recenzowany