Rafał **TUTAJ**

DEVICENET SAFETY – NOWE PODEJŚCIE DO ZABEZPIECZANIA MASZYN

Streszczenie: W referacie zaprezentowano wymagania funkcjonalne nałożone przez normę IEC 61508 i wynikające z nich zmiany jakie zostały wprowadzone do sieci DeviceNet. W szczególny sposób przedstawione zostały modyfikacje protokołowe wpływające na znaczące podniesienie poziomu bezpieczeństwa

Słowa kluczowe: CAN, sieć Device Net Safety, Protokół CIP Safety, detekcja błędów.

1. WPROWADZENIE

Zabezpieczanie maszyn i urządzeń technologicznych było i jest jednym z głównych problemów towarzyszących rozwojowi automatyzacji procesów. Rosnące zapotrzebowanie na produkty przemysłowe wymuszało zwiększanie szybkości pracy elementów, umożliwiając osiąganie lepszej wydajności i efektywności pracy systemu. Jedynym, w zasadzie niezmiennym elementem całego ciągu technologicznego pozostał człowiek. O ile w przypadku procesów ciągłych, wymagających pewnego ustalonego czasu, wynikającego z praw reakcji chemicznych, niewiele dało się zmienić, to w przypadku procesów dyskretnych, takich jak montaż czy produkcja FMCG osiągnięto daleko idący postęp. Skrócenie czasu wytwarzanie produktu spowodowało, iż wszystkie operacje na nim muszą być wykonywane znacznie szybciej. Aby zrealizować zadania maszynowe, wymagane było zastosowanie szybszych silników czy siłowników. Dzięki nowym technologiom udało się sprostać tym założeniom. Wykorzystanie szybkich sterowników PLC wraz z całym zestawem układów serwonapędowych pozwoliło zdjąć z operatorów część obowiązków i funkcji kontrolnych. Jednak obecności człowieka przy maszynie do końca nie udało się wyeliminować. Konieczne jest nadzorowanie podawania materiałów i składników, kontrola poszczególnych faz produkcji i usuwanie ewentualnych zatorów, przezbrajanie i wymiana zużytych elementów. Każde z tych zadań w większości przypadków wymaga ingerencji do wnętrza maszyny. I tu właśnie pojawia się problem bezpieczeństwa. Z jednej strony mamy ciągłe przyspieszanie procesu, w tym także obsługi. Z drugiej ciągle niezmiennego, a więc i omylnego człowieka. Połączenie obydwu zjawisk może być i jest powodem wielu wypadków, o ile urządzenie nie zostanie w odpowiedni sposób zabezpieczone.

Pierwsze systemy ochronne sprowadzały się do centralnych wyłączników zasilania. W przypadku awarii operator odcinał napięcie i czekał aż inne układy i elementy zatrzymają się bądź wytracą energię. Takie rozwiązanie było problematyczne, jeśli w niebezpieczeństwie był jedyny operator. Rozwój technologii PLC w latach 80. spowodował, iż cała logika procesowa została zmieniona z przekaźników i styczników na rzecz uniwersalnego sterownika. Uzyskano dzięki temu daleko idącą elastyczność sterowania. Niestety systemy

Mgr inż. Rafał **TUTAJ** - ELMARK Automatyka, Warszawa

bezpieczeństwa w tym okresie zostały rozbudowane jedynie o funkcję odcinania wyjść (sterownik mógł być dalej zasilany) oraz w wielu przypadkach dodawano czujniki zamknięcia osłon. Każda zmiana w układach zabezpieczeń wymagała w dalszym ciągu poprawek sprzętowych.

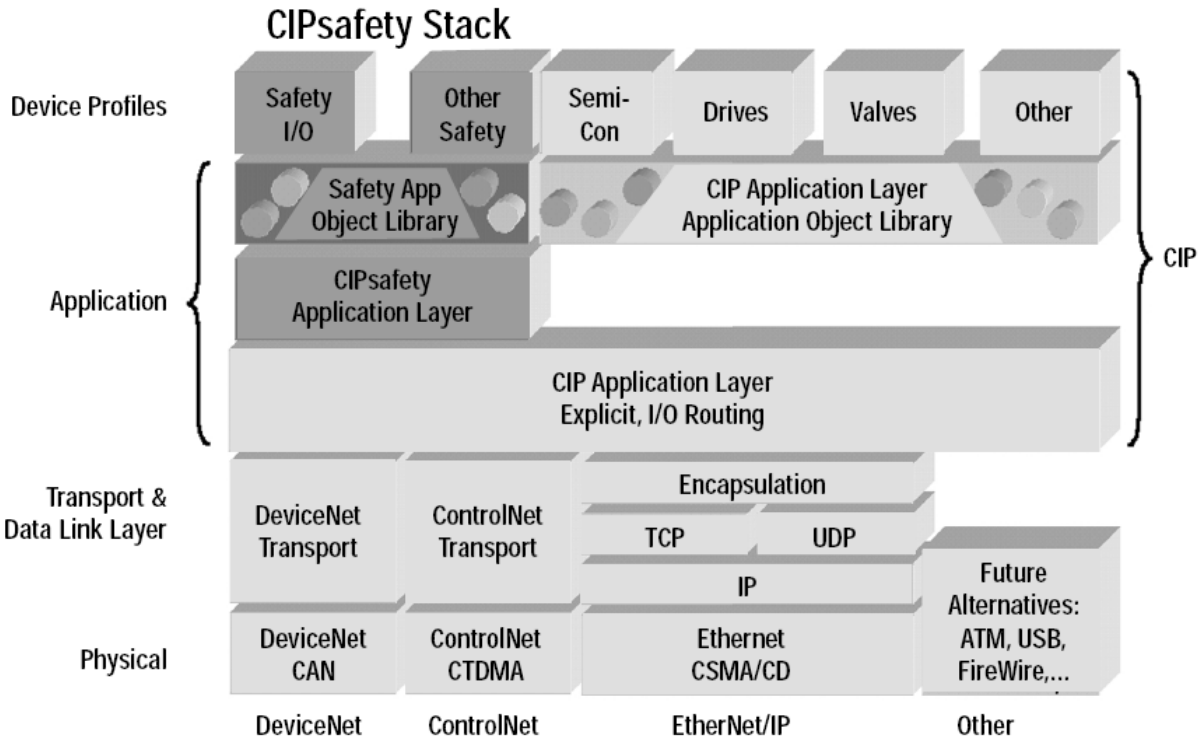
Lata 90. przyniosły niemalże lawinowy rozwój technik sieciowych. Stworzenie takich systemów jak DeviceNet, Profibus czy ControlNet pozwoliło na rezygnację z doprowadzania wszystkich sygnałów do centralnego sterownika. Zastąpiono je modułami we/wy umieszczanymi blisko źródeł i odbiorców sygnałów połączonymi ze sterownikiem kablem magistralowym. Takie rozwiązanie po pierwsze znacznie obniżyło koszty całości, po drugie zwiększyło elastyczność i konfigurowalność systemu, i wreszcie pozwoliło na poprawienie mechanizmów diagnostycznych. Ciągle jednak technologia oraz przepisy nie pozwalały na zastosowanie tego pomysłu w układach bezpieczeństwa.

Początek XXI wieku stał się przełomowym okresem dla zabezpieczeń. Wielu dostawców po ugruntowaniu właściwości sieci rozpoczęło prace nad stworzeniem rozwiązania przenoszącego wspomniane wyżej możliwości do systemów bezpieczeństwa. Wychodząc naprzeciw, organizacje normujące stworzyły międzynarodowy standard określany jako IEC 61508. Zawarta w nim treść definiowała m.in. generalne zasady zabezpieczania urządzeń przy pomocy programowalnych układów elektronicznych, a w szczególności połączonych za pomocą sieci. Jednym z jej elementów jest określenie wiarygodności systemu jako układu bezpieczeństwa. Wyraża się on klasą SIL (Safety Integrity Level) zależną od prawdopodobieństwa wystąpienia błędu wewnętrznego w czasie pracy systemu. Podstawowym zadaniem dla sieciowego systemu bezpieczeństwa nie jest to, by nie było żadnej awarii układu, ale to aby w przypadku ich wystąpienia wszystkie wskazane urządzenia zostały przełączone w odpowiedni znany stan bezpieczny. Dla zdecydowanej większości aplikacji przemysłowych zaleca się stosowanie klasy SIL 3, co oznacza, że w trakcie pracy w pełni obciążonego systemu niezauważony lub źle zidentyfikowany błąd może się pojawić raz na 150 lat ciągłej pracy.

Spełnienie takiego warunku nie jest rzeczą łatwą, stąd większość dostawców zdecydowała się na stworzenie oddzielnych, dedykowanych sieci, wewnątrz których możliwa jest komunikacja wyłącznie z urządzeniami bezpieczeństwa. Dzięki uniwersalnemu protokołowi CIP, stanowiącemu definicję warstw wyższych sieci DeviceNet udało się dodać do istniejącej od 1994 roku koncepcji nowe funkcje, tworząc DeviceNet Safety.

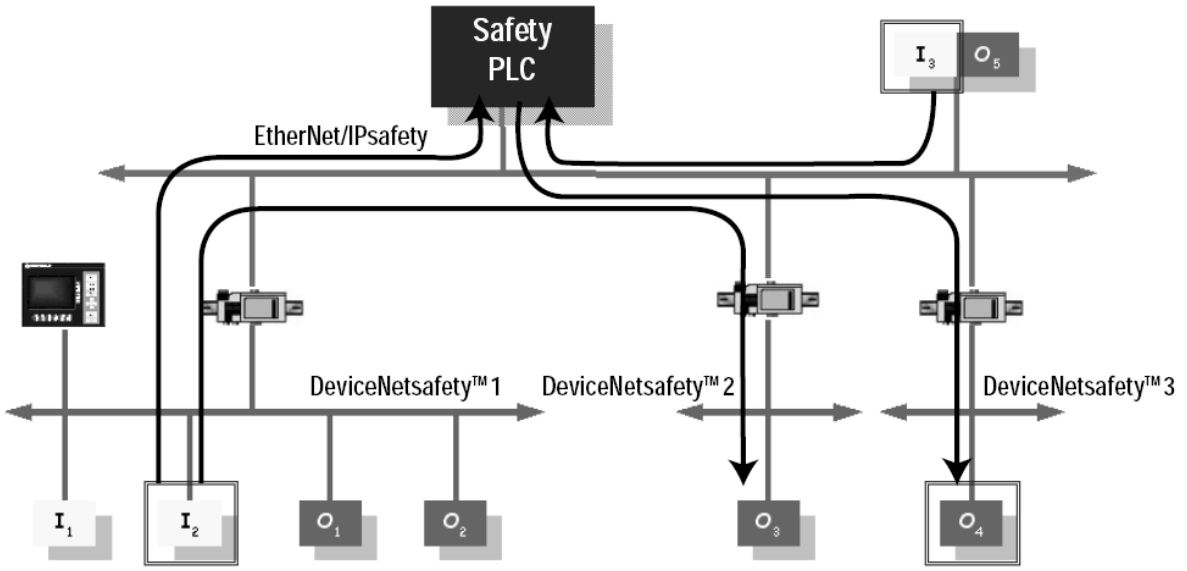
2. DEVICENET SAFETY – NOWE ELEMENTY W STAREJ SIECI

Podstawą do zapewnienia pełnej fukcjonalności wymaganej przez normę IEC 61508 było zbudowanie uniwersalnego protokołu CIPsafety. Common Industrial Protocol jest niezależną od warstwy fizycznej definicją właściwości urządzeń przemysłowych i metod ich komunikowania. Na rysunku 1 przedstawione zostały warstwy sieciowe w odniesieniu do trzech sieci : DeviceNet, ControlNet oraz Ethernet/IP.



Rys.1. Układ warstwowy sieci protokołu CIP

We wszystkich przypadkach odwołanie do poszczególnych atrybutów (np. stan wejścia czy przyspieszenie falownika) jest takie samo, niezależnie od wybranej sieci. Rozszerzając opis funkcji o dodatkowe elementy związane z bezpieczną komunikacją, możliwe stało się zachowanie poprzednich właściwości. W ten sposób w 2005 roku powstała sieć określana jako DeviceNet Safety. Obecnie ukończone zostały prace i testy nad drugim systemem sieciowym : Ethernet/IP Safety. Pozwoli to na budowanie układów hybrydowych, integrujących różne media, których przykład pokazuje rysunek 2

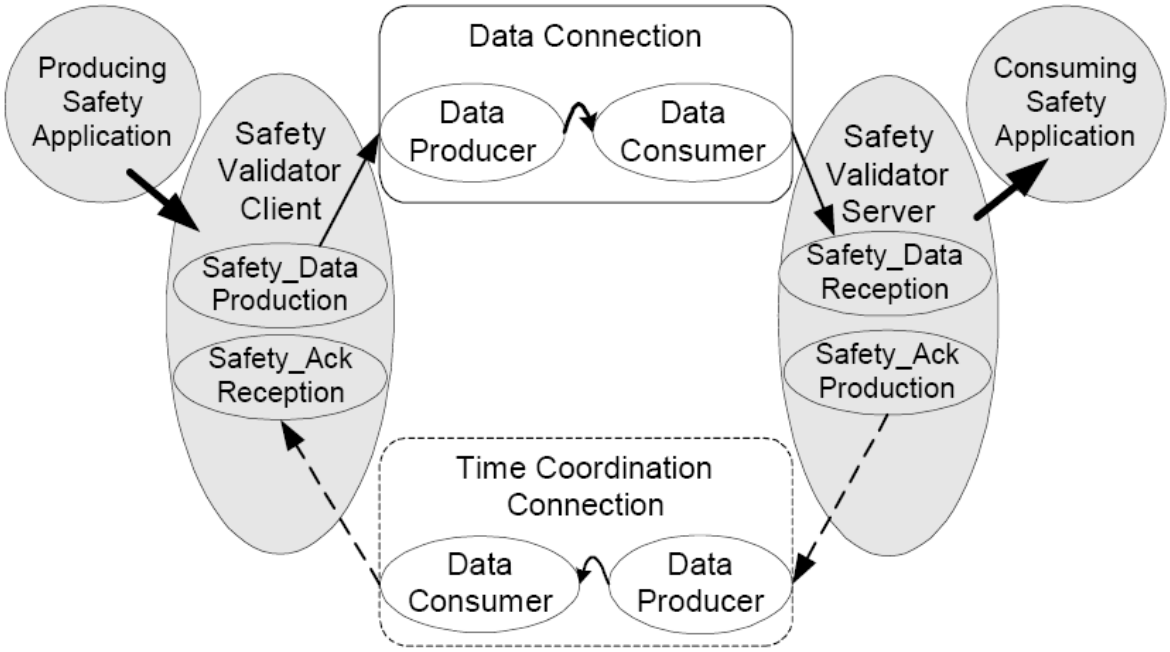


Rys.2. Układ hybrydowy safety złożony z kilku sieci

W ten sposób będzie możliwe dzielenie układów na fragmenty przy zapewnieniu integralności całego systemu bezpieczeństwa.

3. PROTOKÓŁ CIP SAFETY, DETEKCJA BŁĘDÓW

Warstwa aplikacyjna protokołu CIP Safety jest określana przez obiekt Safety Validator (SV). Jest on odpowiedzialny za zarządzanie połączeniami (CIP Safety Connections) i pracuje jako pośrednik pomiędzy obiektami aplikacji i warstwy łącza. Szczegóły zostały pokazane na rysunku 3:



Rys.3. Struktura obiektowa wymiany danych w protokole CIP Safety

W trakcie przesyłania danych pomiędzy producentem (z lewej strony rysunku) i konsumentem (z prawej strony) obiekty Safety Validator pełnią następujące funkcje :

- aplikacja generująca dane (PSA) wykorzystuje fragment klienta SV do utworzenia bezpiecznych danych oraz do zapewnienia koordynacji czasu;
- klient SV wykorzystuje tradycyjne medium DeviceNet do przesłania wszystkich informacji (dane, czas) do odbiorcy;
- aplikacja odbierająca dane (CSA) wykorzystując fragment serwera SV odbiera i sprawdza poprawność danych;
- server SV, wykorzystując nawiązane połączenie zwraca informację o czasie przyjęcia wiadomości do klienta SV.

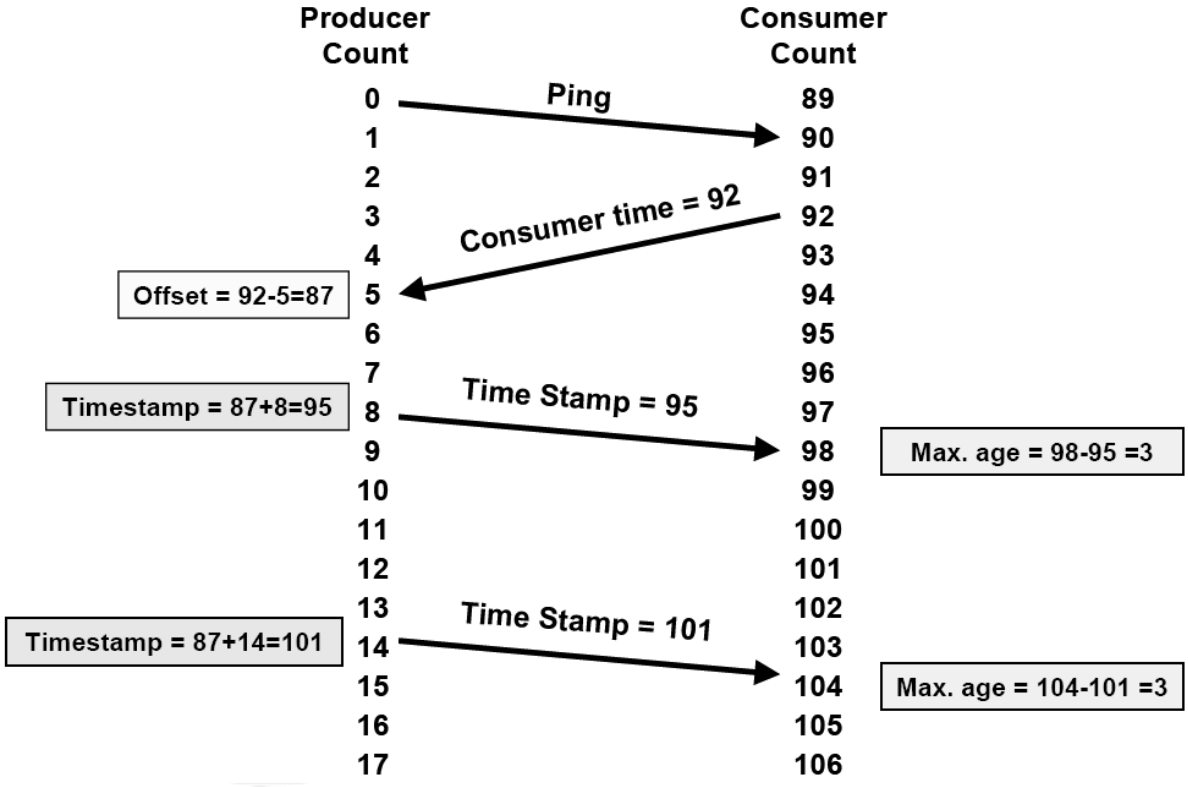
Należy tu zwrócić uwagę, iż podczas wymiany danych elementy łącza (w środku rysunku) nie uczestniczą w procesach związanych z bezpieczeństwem. Nad integralnością danych i detekcją problemów czuwają obiekty SV.

Jak zostało to wspomniane wcześniej, zadaniem CIP Safety nie jest 100-procentowa ochrona czy zapobieganie pojawianiu się błędów. Jedną z głównych funkcji obiektów SV jest ich wykrycie i podjęcie odpowiedniej akcji. W poniższej tabeli pokazane zostało 9 błędów, jakie muszą być wykryte przy pomocy jednej bądź kilku z pięciu metod.

	Metoda wykrycia				
Błąd	Stempel czasowy	Identyfikator ID nadawcy	Safety CRC	Redundancja danych i testy wskrośne	Rozdzielność funkcjonalna
Powtórzenie komunikatu	X		X		
Utrata komunikatu	X		X		
Element obcy w komunikacie	X	X	X		
Niepoprawna kolejność	X				
Uszkodzenie komunikatu			X	X	
Opóźnienie komunikatu	X				
Nałożenie danych z różnych sieci Safety		X			
Nałożenie danych z sieci Safety i sieci standard	X	X	X	X	X
Przekroczenie czasu w układach hybrydowych	X				

3.1 Stempel czasowy

W standardowej sieci DeviceNet wysyłanie danych odbywa się metodą typu broadcast, co oznacza, że nadawca nie otrzymuje bezpośrednio potwierdzenia odebrania danych. Protokół nakłada na układy typu slave przesyłanie, co jakiś czas informacji o własnym stanie lub odpowiadanie w ten sposób na żądanie skanera. Taki sposób weryfikacji jest niewystarczający do zapewnienia pracy na poziomie SIL 3. W sieci DeviceNet Safety każda informacja jest przesyłana z dołączonym stemplem czasowym. Jest to forma bardzo precyzyjnego licznika pozwalającego określić odbiorcy „wiek” otrzymanych danych. W przypadku przekroczenia dopuszczalnego czasu jest podstawa do podjęcia działań specjalnych takich jak żądanie ponownego transferu lub przełączenie w tryb bezpieczny. Szczegóły pokazuje rysunek 4.



Rys.4. Przykład wyliczania wieku danych

Po nawiązaniu połączenia następuje synchronizacja zegarów poprzez komunikat ping. Wszystkie dalsze komunikaty opierają się na czasie liczonym na bazie offsetów określonych podczas nawiązywania połączenia. Każde przesłanie danych jest łączone z przesłaniem stempla, pokazanego na rysunku jako Time Stamp. Z uwagi na możliwy dryft układów nadawczych i odbiorczych, ramka ping jest przesyłana, co jakiś czas, by utrzymać synchronizację zegarów.

3.2 Identyfikator PID (Production IDentifier) i rozdzielność funkcjonalna

Podczas konfiguracji systemu każdy potencjalny nadawca danych (producent) tworzy specjalny numer będący kombinacją numeru seryjnego, numeru połączenia CIP oraz klucza produktu. Odbiorca podczas analizy danych (poprzez obiekt SV) porównuje identyfikatory i w przypadku niezgodności odrzuca informację i/lub przechodzi w stan bezpieczny. Taki mechanizm jest szczególnie ważny w przypadku układów hybrydowych, łączących kilka podsieci, w których może wystąpić błąd złego przekierowania pakietów.

Rozdzielność funkcjonalna jest specjalnym zabiegiem twórców DeviceNet Safety blokującym tworzenie obiektów SV w urządzeniach, które nie mają charakteru układu bezpieczeństwa. Mechanizm ten pozwala na uniemożliwienie hipotetycznego podszywania się – w wyniku błędu – standardowych urządzeń pod elementy safety.

3.3 Suma kontrolna Safety CRC i redundancja

Zadaniem sumy kontrolnej jest zapewnienie kontroli integralności i niezmienności danych. Modyfikacja standardowego algorytmu na potrzeby układów bezpieczeństwa pozwoliła na osiągnięcie odstępu Hamminga na poziomie 4. Dzięki temu wszelkie problemy wynikające zarówno z zakłóceń, jak i błędów przy fragmentacji mogą zostać szybko wykryte.

Dzięki umiejscowieniu safety CRC wewnątrz obszaru danych w komunikatach osiągnięto niezależność od warstwy łącza dodającej własną, wynikającą z sieci sumę kontrolną.

Aby dodatkowo zwiększyć wartość odstępu powyżej 4, zdecydowano się na redundowany transfer danych i sum kontrolnych. Oznacza to, iż w każdym komunikacie przekazywane informacje są dublowane w postaci właściwych danych i ich negacji. Zadaniem obiektu SV jest więc ich wydzielenie, porównanie logiczne i następnie – o ile wynik jest pozytywny – przekazanie do analizy sumy safety CRC.

4. PRZESYŁANIE DANYCH I NAWIAZYWANIE POŁĄCZEŃ

Przesyłanie danych – w swej podstawowej formie DeviceNet – opiera się o ramkę CAN. Jak wspomniano wcześniej, wszelkie zmiany przy transferze – by zachować niezależność od łącza i umożliwić współpracę – zostały wprowadzone w obszarze danych. W sieci DeviceNet Safety wyróżnia się dwa rodzaje komunikatów niosących treść: krótkie i długie.

Pierwszy z nich pozwala na przesłanie do dwóch bajtów informacji. Jest to bardzo przydatna forma, zwłaszcza dla prostych urządzeń jak wyłączniki bezpieczeństwa czy zabezpieczenia osłon. Inna ważna zaleta to minimalizacja ruchu sieciowego. Na rysunku 5 pokazany został przykład takiego komunikatu.

Short Data Section			
Actual Data	Mode Byte	Actual CRC	Comp. CRC
1 - 2 Bytes		CRC-S1	CRC-S2

Rys.5 Krótka ramka DeviceNet Safety

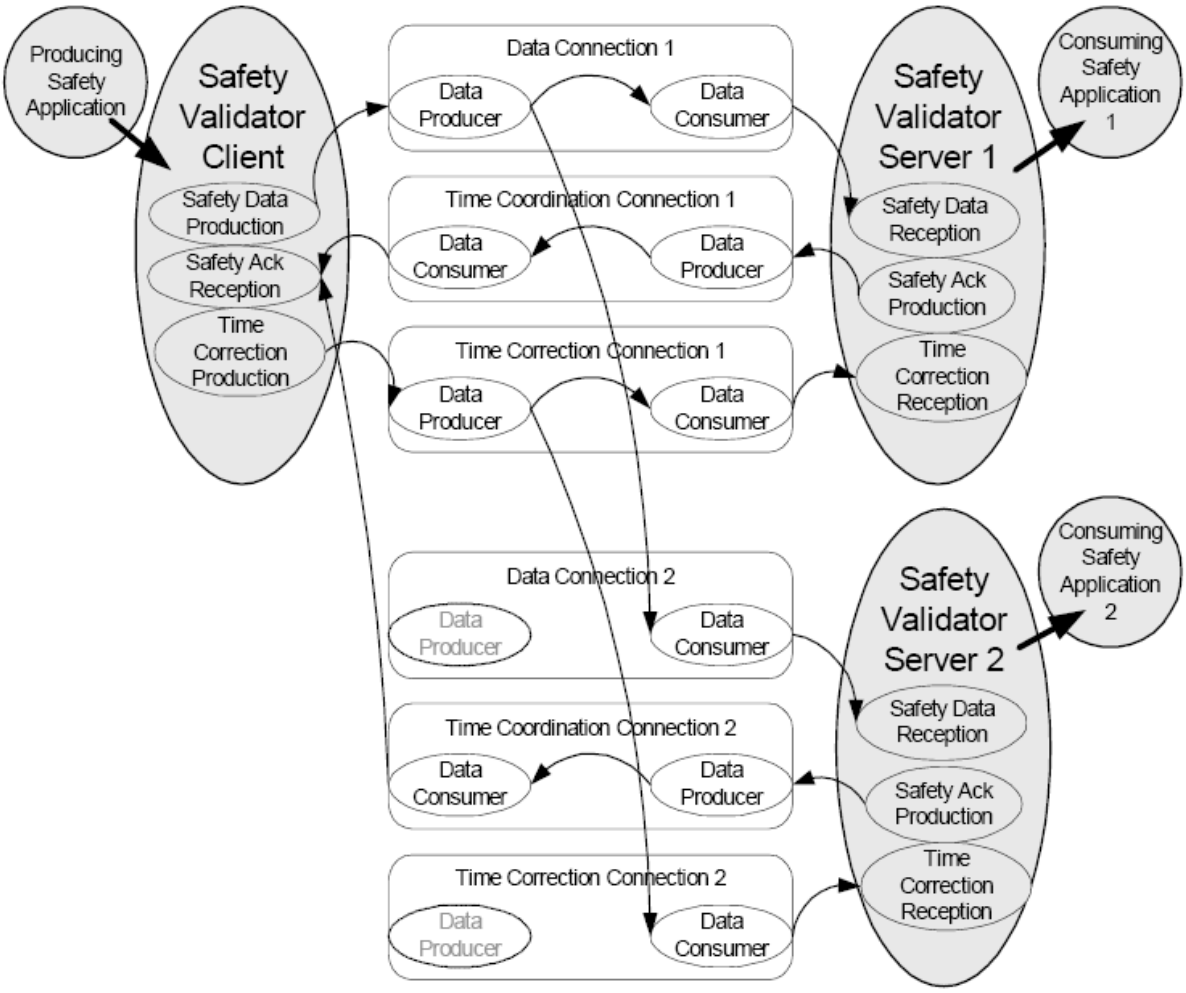
Drugi pozwala na przesyłanie większych ilości danych – aż do 250 bajtów. Tu warto zwrócić uwagę iż standard CAN dopuszcza do 8 bajtów w ramce, a więc do przesłania takiej ilości danych konieczna będzie ich fragmentacja. To jednak jest własność łącza, a więc z punktu widzenia DeviceNet Safety i obiektu SV ciągle operujemy na pojedynczym, długim komunikacie, którego przykład znajduje się na rysunku 6.

Long Data Section				
Actual Data	Mode Byte	Actual CRC	Complemented Data	Comp. CRC
3 - 250 Bytes		CRC-S3	3 - 250 Bytes	CRC-S3

Rys.6. Długa ramka DeviceNet Safety

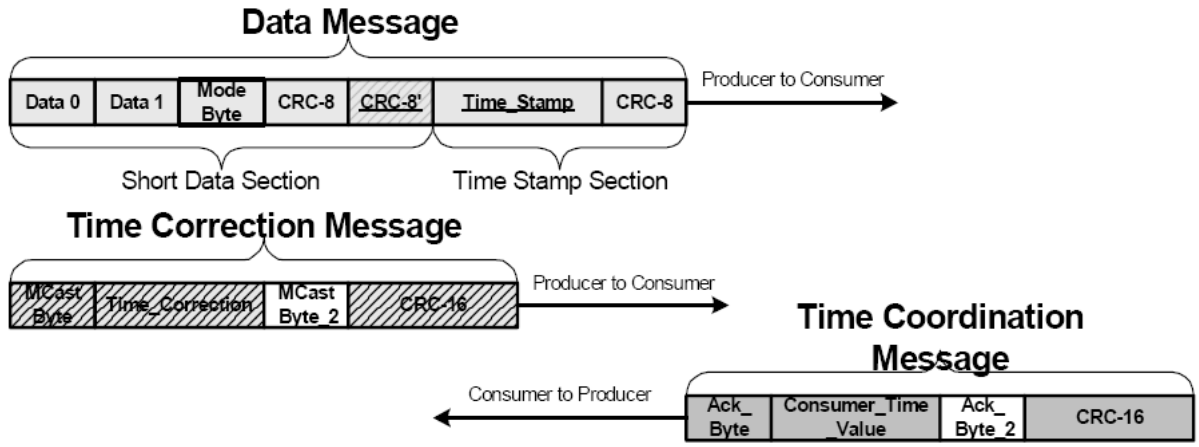
Warto zauważyć, iż w przypadku długich danych redundancji – czyli utworzeniu komplementarnych danych – ulega zarówno suma kontrolna, jak i właściwe dane. Wydłuża to treść, a co za tym idzie czas przesłania, ale zapewnia bardzo wysoką integralność danych.

Do poprawnej pracy sieci istnienie wyłącznie komunikatów z danymi jest niewystarczające i dlatego stworzono cały szereg dodatkowych form pozwalających na synchronizację, diagnostykę i konfigurację. W części 3 niniejszego opracowania pokazany został układ obiektów przy połączeniu typu Single-Cast czyli jeden-do-jednego. Ciekawsze wydaje się spojrzenie na rodzaje komunikatów przez pryzmat połączenia Multi-Cast, a więc takiego, w którym nadawca wysyła do kilku odbiorców jednocześnie. Na rysunku 7 przedstawiony został schemat takiego połączenia.



Rys.7. Schemat obiektowy połączenia typu Multicast

W ten sposób możliwe jest przesłanie danych do 15 urządzeń. Klient SV tworzy w tym przypadku trzy połączenia – danych, koordynacji czasu i korekcji czasu. Dwa pierwsze są wspólne dla wszystkich odbiorców, natomiast – z uwagi na wymogi bezpieczeństwa – korekcja czasu odbywa się indywidualnie dla każdego odbiorcy. Każdemu z powyższych mechanizmów towarzyszy inna forma komunikatu, a przykład takiej synchronizacji został pokazany na rysunku 8.



Rys.8. Wspólna ramka danych i indywidualna synchronizacja czasu

Bardzo ważnym elementem „życia" sieci jest konfiguracja urządzeń. Obecnie praktycznie wszystkie elementy systemów bezpieczeństwa są wyposażane w układy procesorowe z pamięciami typu flash. Dzięki temu twórca czy projektant uzyskuje szereg narzędzi umożliwiających swobodną konfigurację poprzez sieć. Przesłanie typowych ustawień czy parametrów nie jest niczym nowym, więc w tym miejscu pokazane zostaną jedynie elementy związane z podniesieniem bezpieczeństwa.

Sieć DeviceNet Safety zapewnia kilka mechanizmów zabezpieczających system przed zmianami konfiguracji:

- *Safety Network Number* – specjalny numer określający sieć. Jest to modyfikacja PID związana z wersją skanera sieci. Każde urządzenie pracujące ze skanerem przechowuje jego identyfikator w celu sprawdzenia czy zmiany w konfiguracji prowadzone automatycznie przez program sterownika pochodzą z właściwego skanera;
- *Password Protection* – „ludzka" wersja powyższego identyfikatora. Tym razem operator lub inna osoba usiłująca dokonać zmian w ustawieniach musi autoryzować swój dostęp;
- *Configuration Ownership* – każde urządzenie może mieć określone dozwolone źródło zmian w konfiguracji. Może to być sterownik i karta sieciowa lub zdalne urządzenie. W ten sposób – na poziomie komunikatów – można dodatkowo wyeliminować nieautoryzowany dostęp;
- *Configuration Locking* – możliwość przełączenia sieci w stan blokujący wszelkie zmiany ale umożliwiający odczyt wszystkich parametrów. Dzięki temu – po zakończeniu testów i dopuszczeń do ruchu – użytkownik ma możliwość podglądu stanu sieci ale bez możliwości dokonywania jakichkolwiek zmian.

5. ZAKOŃCZENIE

W publikacji przedstawione zostały nowe elementy sieci DeviceNet Safety wprowadzone w celu wypełnienia wymagań normy IEC 61508. Główny nacisk został położony na wyjaśnienie podstaw działania sieciowego systemu bezpieczeństwa. Zdaniem autora ważne jest ich zrozumienie przed rozpoczęciem stosowania, gdyż z poziomu oprogramowania narzędziowego, (które jest przedmiotem szkoleń i prezentacji) wielu elementów nie widać. Autor zachęca do udziału w tego typu spotkaniach jako kontynuacji poznawania sieciowych systemów bezpieczeństwa opartych o sieć DeviceNet Safety.

6. LITERATURA

[1] The Common Industrial Protocol (CIP) and the Family of CIP Networks, PUB 00123R0 ODVA, 2006
[2] VASKO A David.: DeviceNet Safety: Safety networking today and beyond, PUB00110 ODVA, 2005
[3] Machine Safety Guide SAFETY_RM002A_EN_P, Rockwell Automation 2007

DEVICENET SAFETY – NEW APPROACH TO MACHINE SAFETY

Abstract: The paper presents the modification of DeviceNet network according to IEC 61508 requirements. The author concentrates on the main protocol changes, which effect on increase the safety level. Particularly wide are described the schema of connection establishment and error detection tools embedded into the protocol.

Recenzent: dr inż. Zbigniew Raczyński