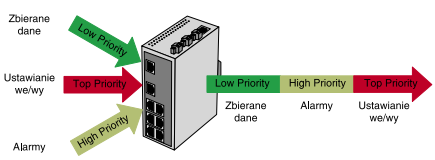
Ethernet w zastosowaniach przemysłowych, część 2

Szybkość i pewność działania sieci łączącej urządzenia jest istotnym kryterium, branym pod uwagę podczas budowania rozproszonych systemów automatycznego sterowania. O tym, jak można zwiększyć bezpieczeństwo ich funkcjonowania, piszemy w artykule.

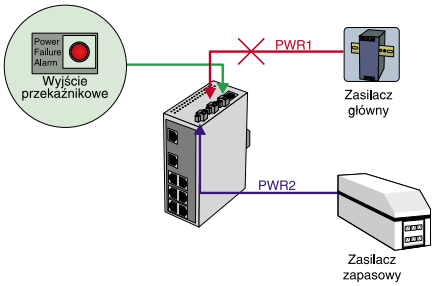
Zwiększenie determinizmu przesyłanych informacji można uzyskać przez stosowanie mechanizmu sieciowego noszącego nazwę *Quality of Service*. Komendy sterujące wejściami i wyjściami sterowników PLC mają zazwyczaj wyższy priorytet (większe znaczenie dla poprawnego działania systemu) niż dane zbierane z obiektu. QoS umożliwia przypisanie do przesyłanych informacji odpowiednich priorytetów, dzięki czemu pakiety przesyłane są w odpowiedniej kolejności (**rys. 1**).

Wszystkie te aplikacje zaliczane do systemów automatyki mają różne wymagania w stosunku do sieci Ethernet i wymagają różnych poziomów zabezpieczeń. Kluczowym zagadnieniem, wspólnym dla wszystkich zastosowań, jest niezawodność połączeń sieciowych. Niezawodność i bezawaryjną pracę sieci można osiągnąć przez redundancję zasilania, redundancję poszczególnych połączeń oraz całych węzłów sieci. Na przykładzie przełączników firmy Moxa postaram się przedstawić praktyczne i efektywne sposoby podnoszenia niezawodności sieci Ethernet w zastosowaniach przemysłowych.

Jednym z podstawowych wymogów w systemach automatyki przemysłowej jest redundancja zasilania (**rys. 2**). Każdy węzeł sieci powinien mieć dwa niezależne źródła zasilania. W przypadku awarii jednego z nich system natychmiast zostaje przełączony na zasilanie awaryjne, co znacznie zmniejsza ryzyko niekontrolowanego wyłączenia. Dlatego



Rys. 1



Rys. 2

każdy, nawet najprostszy, przełącznik firmy Moxa ma redundantne zasilanie. Ponadto w przypadku zaniku jednego ze źródeł zasilania przełącznik sygnalizuje ten fakt operatorowi systemu. Powiadamianie może odbywać się na kilka sposobów: może to być załączenie przekaźnika lub wysłanie do operatora pułapki SNMP lub listu e-mail.

Nie mniej ważnym, a być może ważniejszym zagadnieniem jest redundancja połączeń pomiędzy poszczególnymi segmentami sieci. Redundancja poprzez topologię podwójnej gwiazdy jest bardzo droga w implementacji, natomiast w początkowym stadium rozwoju sieci Ethernet nie można było tworzyć topologii typu *ring*, ponieważ zapętlenie sieci Ethernet jest niedozwolone. Potrzeba stworzenia redundantnej sieci była na tyle duża, że wkrótce został opracowany standard IEEE802.1D, opisujący *Spanning Tree Protocol* (STP) bazujący na topologii typu pierścień. IEEE 802.1D polega na tym, że *Spanning Tree* identyfikuje jeden z przełączników w sieci jako *root switch* i automatycznie blokuje pakiety wędrujące przez połączenie zapasowe. W przypadku gdy jeden z segmentów zostanie odłączony od reszty sieci, STP automatycznie rekonfiguruje pierścień i przechodzi na połączenie zapasowe, które było blokowane. Aktualna topologia pierścienia oraz to, który segment jest blokowany, jest określone liczbą przełączników tworzących pierścień. Mimo że IEEE 802.1D niwelował niektóre ograniczenia sieci Ethernet, to niestety sam wprowadzał nowe ograniczenia, np. długi czas rekonfiguracji pierścienia oraz blokowanie połączeń, gdy dostępne pasmo było zbyt małe dla panującego ruchu w sieci. Z tego powodu został opracowany standard IEEE 802.1W, czyli *Rapid Spanning Tree Protocol* (RSTP). Nowy protokół ma wszystkie zalety 802.1D ale oferuje znacznie lepsze osiągi. Na bazie 802.1W producenci przełączników przemysłowych tworzą własne protokoły umożliwiające tworzenie redundantnych połączeń w sieci Ethernet. Jednym z takich rozwiązań jest opracowany przez firmę Moxa protokół *Turbo Ring*, który gwarantuje nawiązanie zapasowego połączenia w czasie poniżej 300 ms dla 20 przełączników i 120 urządzeń wpiętych do sieci (**tab. 1**). Dla takiej liczby przełączników oryginalny 802.1W potrzebuje około 10 s na rekonfigurację pierścienia.

Konfiguracja protokołu *Spanning Tree* jest dość skomplikowana i uzależniona od liczby przełączników w sieci oraz jej topologii. Trzeba określić przynajmniej kilka parametrów, aby w przybliżeniu wyliczyć czas rekonfiguracji pierścienia. Konfiguracja pierścienia *Turbo Ring* jest bardzo prosta. Wystarczy odpowiednio połączyć przełączniki i uaktywnić funkcję *Turbo Ring*. Opcjonalnie można wskazać, który z przełączników ma być *Ring Masterem* (**rys. 3**), wtedy decydujemy, który segment jest blokowany. Jeśli nie zdefiniujemy *Mastera*, *Turbo Ring* skonfiguruje sieć automatycznie.

W niektórych aplikacjach tworzenie jednego dużego pierścienia może być

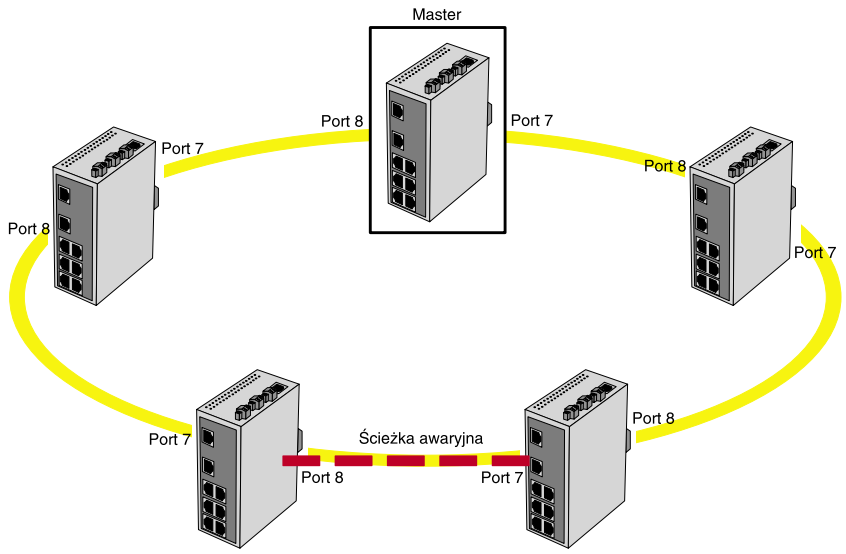
Tab. 1. Zestawienie czasów rekonfiguracji pierścienia sieci w zależności od liczby dołączonych urządzeń i przełączników

Liczba urządzeń wpiętych do sieci	6 x 5=30	6 x 10=60	6 x 15=90	6 x 20=120
Liczba przełączników w pierścieniu	5 EDS	10 EDS	15 EDS	20 EDS
Czas rekonfiguracji pierścienia	< 150 ms	< 200 ms	< 250 ms	< 300 ms

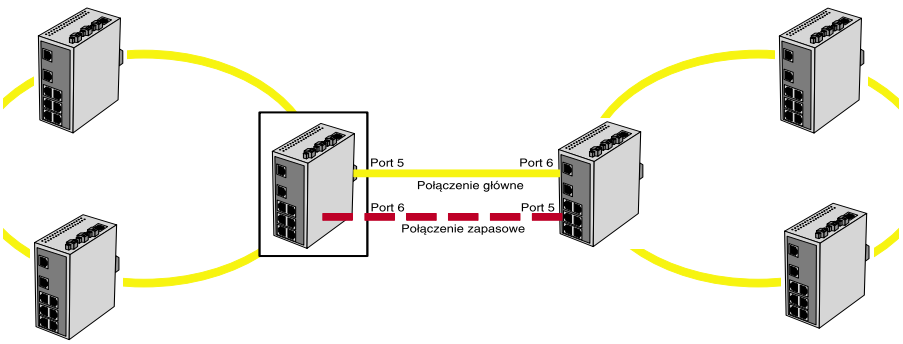
niewygodne np. gdy system jest rozproszony. Z myślą o takiej topologii Moxa oferuje funkcję *Ring Coupling*, która umożliwia łączenie ze sobą pierścieni *Turbo Ring* (**rys. 4**).

Jeśli mamy już redundancję połączeń pomiędzy poszczególnymi węzłami sieci, powstaje pytanie, jak zabezpieczyć się przed awarią *switcha*. Przełączniki firmy Moxa umożliwiają redundancję poszczególnych węzłów sieci przez podłączenie krytycznych urządzeń do dwóch niezależnych przełączników (**rys. 5**). Jest to możliwe tylko wtedy gdy kontroler (np. sterownik PLC) ma podwójny interfejs Ethernet oraz potrafi – w przypadku awarii – przełączyć się na interfejs rezerwowy. Tak wysoki poziom zabezpieczeń stosujemy zazwyczaj tylko dla najważniejszych urządzeń w sieci, głównie ze względu na koszt dodatkowych przełączników.

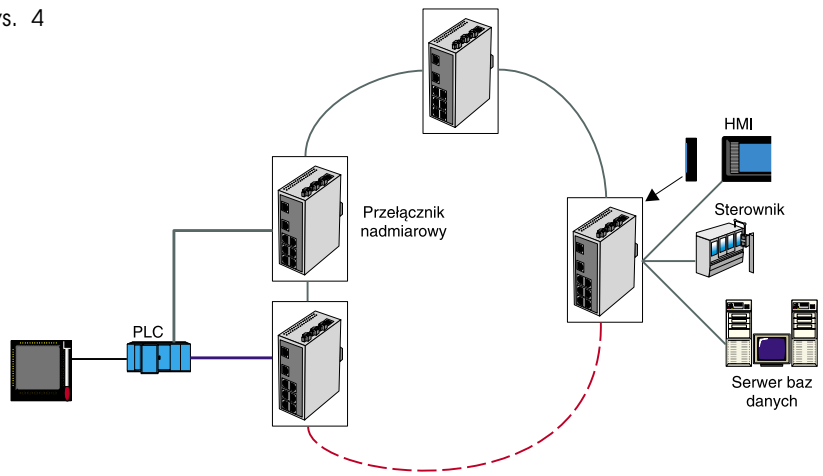
Musimy jednak mieć świadomość że nie jest to sieć zabezpieczona w 100%, ponieważ niektóre urządzenia w przypadku awarii przełącznika utracą połączenie z siecią. W wielu zakładach produkcyjnych awaria sieci często oznacza olbrzymie starty finansowe, niewspółmierne do kosztów



Rys. 3

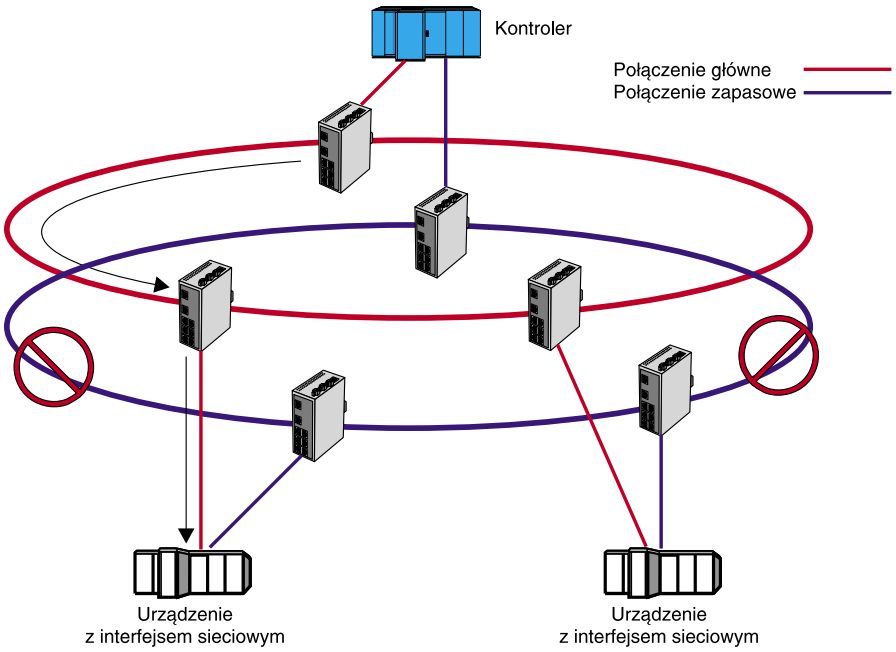


Rys. 4

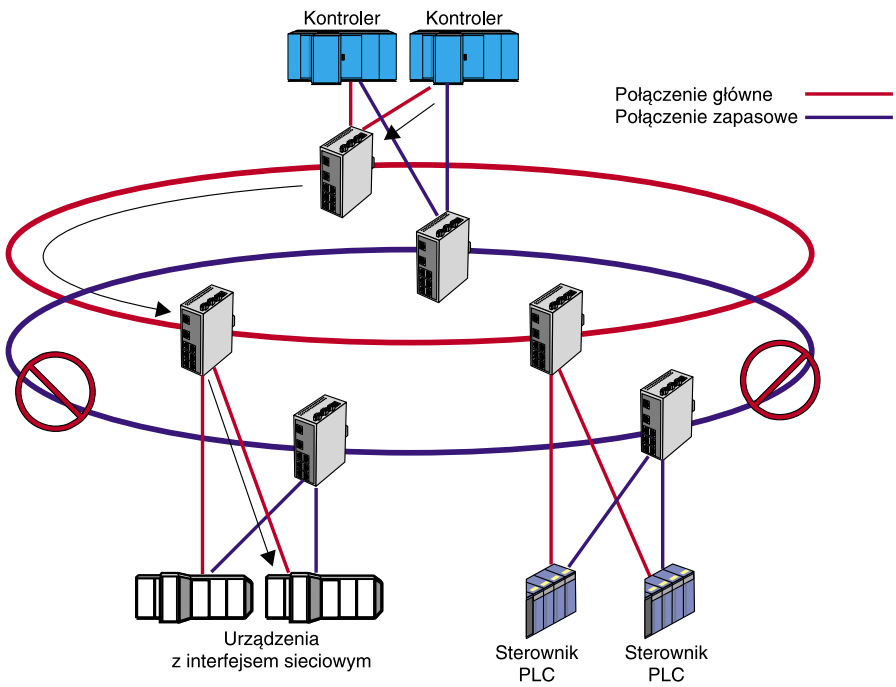


Rys. 5

samej sieci, dlatego w wyjątkowo krytycznych aplikacjach warto rozważyć redundancję całej sieci. Jeśli większość urządzeń jest podłączona do dwóch niezależnych przełączników, od redundancji całej sieci dzieli nas już tylko krok. Za pomocą odpowiedniego okablowania tworzymy 2 niezależne sieci typu pierścień, następnie urządzenia z podwójnym interfejsem Ethernet podłączamy niezależnie do obu sieci (**rys. 6**). Aby taka sieć funkcjonowała poprawnie, urządzenie z dwoma portami A i B musi samodzielnie zdeterminować najbezpieczniejszą drogę przepływu danych.



Rys. 6



Rys. 7

W takiej konfiguracji prawdopodobieństwo awarii sieci jest bardzo małe, ale nasuwa się pytanie, co będzie, gdy uszkodzeniu ulegnie stacja robocza lub sterownik PLC? Aby zabezpieczyć się przed taką ewentualnością, należy zrobić redundancję całego systemu, czyli redundancję połączeń, węzłów, portów i w końcu poszczególnych urządzeń sieciowych (**rys. 7**). Tak wysoki poziom bezpieczeństwa jest rzadko stosowany ze względu na bardzo wysokie koszty. Warto jednak wiedzieć, że jest taka możliwość, ponieważ czasem ze względów bezpieczeństwa, np. gdy w grę wchodzi ludzkie życie, takie zabezpieczenia są niezbędne.

Redundancja całego systemu narzuca jeszcze jeden wymóg w stosunku do urządzeń sieciowych, mianowicie urządzenia muszą zdeterminować które z nich ma być aktywne. Tu z pomocą przychodzi standard IEEE 802.1p/Q, który definiuje wiele narzędzi diagnostycznych do badania stanu sieci i dołączonych do niej urządzeń. Bardzo często same urządzenia przesyłają między sobą w sieci tzw. „oznaki życia", czyli pakiety informujące o ich aktualnym stanie. Takie urządzenia zazwyczaj mają kompletny obraz sieci, aby w sposób inteligentny mogły determinować, które z nich ma być aktywne i z którego portu ma korzystać.

Wybór odpowiedniego poziomu zabezpieczeń zależny jest od faktycznych potrzeb oraz od dostępnego budżetu. W niektórych zastosowaniach prosty niezarządzalny *switch* w wykonaniu przemysłowym będzie rozwiązaniem wystarczającym, natomiast w krytycznych aplikacjach może się okazać, że redundancja poszczególnych węzłów sieci to za mało. Dlatego należy się dobrze zastanowić nad tym, jakie mogą być konsekwencje utraty kontroli nad siecią, ponieważ koszt samej sieci, z pozoru wysoki, może okazać się dużo mniejszy niż ewentualne straty spowodowane utratą połączenia. Ethernet daje bardzo duże możliwości jeśli chodzi o okablowanie, osprzęt sieciowy czy same urządzenia wpięte do sieci. Jednak z tych możliwości trzeba korzystać z rozwagą, cały czas pamiętając, że w przypadku sieci przemysłowej najważniejsze jest, aby cały czas była dostępna i zapewniała komunikację w czasie rzeczywistym.

Cezary Kalista, Elmark

Informacje dodatkowe

Artykuł powstał na bazie materiałów udostępnionych przez firmę Elmark, www.elmark.com.pl, tel. (22) 821-30-54.