Aspekty bezpieczeństwa komputerowych systemów przemysłowych

Piotr Gaj

Streszczenie: Współczesny człowiek uzależnił się od działania systemów informatycznych. Wpływają one zarówno pośrednio jak i bezpośrednio na jego egzystencję. Objawia się to spektakularnie, gdy coś w takim związku idzie źle. Zdarza się słyszeć o awariach, szkodach, stratach i innych negatywnych skutkach materialnych, ludzkich i środowiskowych wynikających z błędów obsługi, zdarzeń losowych lub nieprawidłowości działania różnych systemów technicznych. W komputerowo wspomaganych systemach przemysłowych, z racji ich oddziaływania z fizycznymi procesami, należy zwrócić szczególną uwagę na względy założeń działania takich systemów i bezpieczeństwa ich funkcjonowania. Celem artykułu jest przegląd kluczowych zagadnień związanych z bezpieczeństwem systemów przemysłowych.

Słowa kluczowe: systemy przemysłowe, systemy rozproszone, niezawodność, bezpieczeństwo integralności, bezpieczeństwo funkcjonalne, rzetelność, dostępność, konserwacja, defekty, błędy, niepowodzenia

Abstract: *Modern human is addicted to computer systems and its offered facilities. Various systems affect both directly and indirectly on its existence. This can be seen dramatically when something goes wrong in such a relationship. It happens to hear about the failures, damages, losses and other negative effects of the physical, personal and environmental impacts resulting from improper handling, fate reasons or malfunctions of various technical systems. The computer-aided industrial systems, due to their interaction with the physical process, it must be kept a special care in regards to assumptions of such systems and their safe operation. The paper reviews the basic aspects of security systems.*

Keywords: *industrial systems, distributed systems, dependability, security, safety, reliability, availability, maintainability, faults, errors, fails*

1. Wstęp

Każdego inżyniera produkcji interesuje poprawne prowadzenie procesu przemysłowego. Aby było to możliwe, należy brać pod uwagę nie tylko technologię, automatyzację i informatyzację całości, ale i zagadnienia bezpieczeństwa eksploatacji wszystkich elementów układu. Zapewnianie bezpieczeństwa dla procesu przemysłowego wiąże się z zapewnieniem prawidłowego działania samego procesu, jak i zapewnieniem prawidłowego oddziaływania z nim systemu kontroli. Przekłada się to bezpośrednio na konstrukcje takich systemów oraz ich odporność na zagrożenia eksploatacyjne. Przez pojęcie „system" rozumie się zestaw współpracujących urządzeń realizujących zestaw usług na potrzeby jakiegoś konkretnego procesu technologicznego. W systemach mogą pracować podsystemy oraz mogą się one składać na elementy innych systemów. Użytkownikiem systemu, czyli odbiorcą usługi, może być zarówno człowiek, jak i inny system. W dalszej części artykułu rozpatruje się komputerowe systemy automatyki jako systemy informatyczne (ISP), nie wnikając w technologie czy funkcjonalną stronę automatyzacji procesów. Systemy tego rodzaju wykorzystywane są w różnych obszarach zastosowań. Są to zarówno obszary automatyki przemysłowej, automatyzacji procesów, automatyki budynków, jak i obszary systemów samochodowych, dystrybucji energii, metropolitalnych i innych. Obserwując przestrzeń ostatnich kilkudziesięciu lat, można stwierdzić, że zaangażowanie ISP w różnych dziedzinach gospodarki stale rośnie. W tym kontekście mówi się o właściwych do realizacji takich systemów technologiach informatycznych (ang. *proper design*) oraz o niezawodności działania (ang. *dependability*). Rozważenie tych zagadnień na etapie projektowania instalacji lub jej modernizacji może zapewnić spokojną pracę i niezawodne działanie procesu. Lekceważenie ich – wcześniej czy później doprowadzi do problemów.

W kwestii wykorzystywanych technologii należy brać pod uwagę wsparcie, jakie dają one dla pracy układu w środowisku przemysłowym. Nie każda technologia informatyczna, szczególnie komunikacyjna, daje odpowiednie środki aby maksymalizować bezpieczeństwo działania systemu. Technologie powinny być dobrze dobrane na etapie projektowania. Błędy na tym etapie są z reguły nienaprawialne. Dlatego przy decyzjach o wyborze osoby decydujące oraz działy IT dostarczające opinii powinny brać pod uwagę konkretną specyfikę procesu i wymogi z nią związane. Szczególnie kwestie dotyczące charakterystyki czasowej przetwarzania i wymiany danych. W przypadku braku odpowiedniej kadry wskazany jest konsulting techniczny.

W kwestii zapewnienia odporności systemu na zagrożenia prowadzące do destabilizacji ruchowej procesu należy rozpatrywać zagrożenia zasobów (ang. *security*), czyli niepożądanego dostępu do urządzeń i danych, oraz zagrożenia funkcjonalności (ang. *safety*), czyli obsługi sytuacji niewłaściwych z punktu widzenia działania danej technologii. Podsystem bezpieczeństwa w tym przypadku może stanowić element ISP, jak również ISP może współpracować z niezależnym systemem bezpieczeństwa. Może on być rozbudowywany i zmieniany wraz z rozwojem systemu. Funkcje zapewniania odpowiedniego poziomu bezpieczeństwa prowadzenia i przebiegu procesu przemysłowego są jednymi z kluczowych funkcji systemów kontrolujących procesy przemysłowe. Komputerowe wsparcie,

jakie istnieje w ISP, daje duże możliwości w tej dziedzinie, gdyż oprócz mechanicznych, elektrycznych czy elektronicznych zabezpieczeń w ISP można zastosować wsparcie „inteligentne", wynikające z działania programów.

2. Konstrukcja systemu

Aby zwiększyć bezpieczeństwo na poziomie konstrukcji systemu, ISP powinny mieć odpowiednie mechanizmy wbudowane w oprogramowanie, sprzęt i komunikację. Mechanizmy te są bezpośrednio związane z użytymi technologiami informatycznymi dotyczącymi działania systemów operacyjnych, programów i sieci komputerowych. Istotny jest również dobór urządzeń i ich zadań w systemie.

2.1. Cechy

Poza szeregiem innych, istnieje kilka cech ISP, które bezpośrednio wiążą się z bezpieczeństwem funkcjonowania systemu. Są to:

- **Niezawodność** (rzetelność, ang. *dependability*)

  Ogólna cecha współczesnych rozproszonych ISP. W kwestii bezpieczeństwa na cechę niezawodności składa się pewność działania oraz integralność systemu. Pewność działania zależy od prawidłowego zadziałania ISP w odpowiedzi na informację wejściową (ang. *safety*), a zapewnienie integralności systemu wiąże się z klasycznym pojęciem bezpieczeństwa (ang. *security*) i kontrolą dostępności (ang. *availability*) [1, 2].

  Bezpieczeństwo w rozumieniu pewności (ang. *safety*), czyli że działanie ISP jest poprawne względem założeń, jest to cecha określająca konieczność eliminacji niedopuszczalnego ryzyka urazu fizycznego lub uszkodzenia zdrowia ludzi, bezpośrednio lub pośrednio w wyniku uszkodzenia mienia lub środowiska [3]. Jest to jedna z najważniejszych cech działania przemysłowego systemu rozproszonego. Zapewnienie prawidłowego działania spoczywa na projektantach i programistach. Błędy w tej dziedzinie mogą się pojawić tylko z powodu błędnych założeń, błędnych algorytmów lub błędów w kodzie. Zabezpieczanie prawidłowego działania względem innych zagrożeń spoczywa na systemach bezpieczeństwa.

  Bezpieczeństwo w rozumieniu klasycznym (ang. *security*) jest cechą zabezpieczania informacji przed nieautoryzowanym ujawnieniem, przekazaniem, modyfikacją lub zniszczeniem, niezależnie od tego, czy przyczyna zagrożenia wynika z przypadku czy celowego działania. Problem kontroli integralności nie dotyczy tylko sieci komputerowej i jej izolowania od środowisk pozasystemowych. Dotyczy on wszelkich środków zapobiegających nieupoważnionej interakcji z systemem.

- **Spójność informacyjna** (ang. *data & time consistency*)

  Cecha określająca przestrzenną i czasową spójność informacji. Zdolność do zachowania wartości danych przy współdzieleniu informacji i współistnieniu jej reprezentacji w różnych elementach systemu.

  Ze względu na rozproszenie terytorialne w systemie występują fizycznie odseparowane źródła informacji. Istotne jest zapewnienie, aby wartości danej u źródła i w dowolnym innym miejscu systemu nie różniły się przez czas dłuższy niż pewny gwarantowany czas graniczny. Dla przykładu wartość pomiaru temperatury V w węźle i: V_i dokonanego w momencie czasu t: V_i^t powinna być zaktualizowana we wszystkich innych elementach systemu, zainteresowanych tą wartością, w czasie mniejszym niż T_G. Innymi słowy dopuszcza się istnienie różnic w lokalnej wartości danej tylko przez określony czas. Powyżej tego czasu wartość V_i^t musi być zaktualizowana we wszystkich innych komputerach.

$$V_i^t(t_p) = V_j^t(t_q) \text{ gdy } \bigwedge_{i,j} i \neq j \bigwedge_{q>p} t_q - t_p \geq T_G$$

$$\bigvee_{i,j} i \neq j \bigvee_{q>p} t_q - t_p < T_G \text{ że } V_i^t(t_p) \neq V_j^t(t_q)$$

  i, j – elementy systemu wymieniające informacje;
  p, q – momenty w czasie działania systemu.

- **Punktualność** (zdeterminowanie czasowe, ang. *time-constrainig*)

  Cecha określająca sposób wykonywania działań względem czasu. Do klasyfikacji ISP można przyjmować klasyfikację systemów pochodzącą z teorii systemów czasu rzeczywistego (ang. RTS – *Real Time Systems*) [4]. Jeśli system pracuje

z ograniczeniami czasowymi, to każdy jego element uczestniczący w przetwarzaniu informacji musi podlegać tym ograniczeniom. W praktyce większość systemów przemysłowych działa z ograniczeniami czasowymi, przeważnie w kategorii firm-RTS, rzadziej w hard-RTS, a bardzo rzadko w soft-RTS. Praca pod rygorem ograniczeń czasowych wiąże się z wykonywaniem zadań w czasie określonym przez parametr czasu granicznego (ang. *timeout*).

- **Tolerancja awarii** (ang. *fault-tolerant*)
  Cecha określająca zdolność do działania mimo awarii. Zakłada się, że wystąpienie awarii elementu systemu lub wystąpienie błędu działania może zostać obsłużone przez inny element systemu, jego element zapasowy (ang. *redundancy*) lub specjalne funkcje oprogramowania. W praktyce systemy tolerujące awarie są droższe, ale w przypadku aplikacji krytycznych, od których zależy życie, zdrowie lub znaczące mienie, ich wykorzystanie jest konieczne [2].
- **Trwałość** (utrzymywalność, ang. *sustainability*)
  Cecha określająca zdolność systemu do pracy bez przerw i utrzymania procesu w ciągłym ruchu. Dotyczy to nieplanowanych postojów wynikających z utrzymania i pielęgnacji systemu oraz procesu, a także ich awarii. Cecha wiąże się z tolerancją awarii, jednak opisuje system szerzej, gdyż oprócz awarii dotyczy takich działań, jak administracja, modyfikacja aplikacji i konfiguracji, zmiana reguł komunikacji, diagnostyka itp. Jest to cecha, która szczególnie jest istotna w ISP. W wielu przypadkach zatrzymanie procesu nie jest możliwe, jest kosztowne lub wymaga wiele czasu. Dlatego ISP obsługujący taki proces musi wykazywać cechę trwałości działania, aby nie doprowadzić do utraty pewności działania. Jednym z przykładów użytecznej funkcji systemu zwiększającej trwałość jest możliwość aktualizacji kodu PLC bez zatrzymywania aplikacji lub wymiany modułów bez wyłączania zasilania.

2.2. Oprogramowanie

W ISP funkcjonuje oprogramowanie będące w bezpośrednim oddziaływaniu z procesem i urządzeniami AKP, oprogramowanie oddziałujące z elementami systemu lub innymi systemami oraz oprogramowanie oddziałujące z człowiekiem. Człowiek jako istota dość nieprzewidywalna nie wymaga obsługi zdeterminowanej czasowo. Ważne jest, aby systemy interfejsowe typu HMI czy SCADA nie gubiły danych i nie zmieniały kolejności zdarzeń. Jest to potrzebne do poprawnej diagnostyki i wglądu w stan procesu. Jeśli jednak chodzi o pozostałe grupy programów to powinny wykazywać się zdolnością do pracy na bieżąco (nadążnie) z działaniem elementów, z którymi współpracują. Sposób reakcji wynika z ogólnej teorii systemów czasu rzeczywistego oraz danych ograniczeń czasowych wymaganych przez technologię. Kluczowa jest tutaj zdolność do zarządzania czasem wykonywania zadań i jego kontroli oraz sposób reakcji na błędy przekroczenia dopuszczalnego czasu obsługi.

Dla poprawnego działania względem czasu ISP muszą być odporne pesymistycznie, czyli odporne na tzw. lawinę zdarzeń (ang. *worst case*). Zjawisko to zachodzi, gdy do obsługi w systemie jest zgłaszana maksymalna liczba zdarzeń w oknach czasowych związanych z nadążnością systemu, a obsługa każdego z nich zajmuje maksymalny dopuszczalny czas im przydzielony. W praktyce łatwo jest stworzyć pseudo RTS, gdyż w normalnej pracy większość urządzeń komputerowych ma wystarczająco dużo zapasu mocy obliczeniowej, a sieci wystarczająco dużo wolnego pasma, aby nadążać za otoczeniem. Problem pojawia się właśnie w sytuacjach stresowych, gdy rośnie liczba zdarzeń lub występuje niekorzystna koincydencja współzależności.

Administracja oprogramowania i jego utrzymanie w ISP charakteryzują się pewnymi problemami, które nie występują w systemach biznesowo-biurowych. Dotyczą one:

- Zachowania stanu (ang. *retentiveness*). Jest to właściwie problem programistyczny związany z zapamiętywaniem stanu aplikacji na okoliczność restartu, awarii lub wyłączenia zasilania. Jednak zakładając, że program jest poprawny, a sprzęt umożliwia zachowanie, to należy dbać, aby mechanizmy zachowywania działały. Dotyczy to cyklicznych wymian baterii, kontroli dysków i pamięci, a także rozsądnej gospodarki zasobami o ograniczonej żywotności.
- Aktualizacji (ang. *upgrade*, *patching*). W ISP często nie jest możliwa aktualizacja oprogramowania, ze względu na fakt, że pakietów aktualizacji nikt nie przygotowuje, a nawet jeśli, to nie można jej przeprowadzić w dowolnym momencie. ISP charakteryzuje się pracą ciągłą, a aktualizacje wymagają zatrzymania działania oprogramowania na bliżej nieokreślony czas. Dlatego wszelkie aktualizacje muszą być planowane na odpowiedni czas przed planowanym jej wykonaniem. Ponadto, ze względu na możliwość wprowadzenia nieznanych wcześnie zaburzeń wynikających z nowego kodu, należy aktualizacje wykonywać tylko w sytuacji, gdy aktualna wersja nie spełnia wymagań funkcjonalnych lub stwarza zagrożenia.
- Stosowania metod szyfrowania i protokołów bezpiecznego przekazywania danych. W ISP stosuje się urządzenia, które nie mają zbyt dużych mocy przetwarzania oraz wielkich zasobów pamięci. Nie wszystkie algorytmy bezpieczeństwa da się zaimplementować. Dlatego aplikacja mechanizmów tego rodzaju jest ograniczona lub w ogóle nie występuje.

2.3. Urządzenia

Do obsługi procesów przemysłowych stosowane są specjalizowane komputery klasy PLC, DCS, IPC lub inne. Mają one interfejsy dostosowane do procesu i urządzeń AKPiA (aparatura kontrolo-pomiarowa i automatyki) oraz są w stanie zapewnić terminowe (punktualne) wykonanie zadań przetwarzania danych. Wykorzystanie takich urządzeń nie wprowadza konstrukcyjnych zagrożeń bezpieczeństwa. Problem pojawia się, gdy w ISP umieszczone zostają komputery przeznaczone dla człowieka. W swym założeniu są to komputery dedykowane do pracy biurowej klasy PC, MAC, notebook, tablet itp. Ich zastosowanie w innym kontekście nie jest poprawne i może prowadzić do dużej awaryjności systemu. W ISP stosowane są one do realizacji interfejsowych stacji roboczych dla człowieka. Najczęściej są to stacje kontrolno-wizualizacyjne (ang. *SCADA*), monitorujące, raportujące i wszelkie inne do budowania zrozumiałego dla człowieka interfejsu z procesem i systemem (ang. *HMI*).

Typowymi błędami zastosowań komputerów osobistych są:

- przydzielanie zadań wymagających fizycznej obecności takiego urządzenia w środowisku procesu. Powoduje to szybkie zużycie elementów wirujących oraz awarie spowodowane pracą w trudnych warunkach środowiskowych;
- przydzielanie zadań wymagających cech trwałości, niezawodności oraz przede wszystkim punktualności działania. Komputer osobisty klasy biurowej nie ma konstrukcji odpornej na zagrożenia środowiskowe. Ponadto do pracy w czasie rzeczywistym musi być wyposażony w system operacyjny czasu rzeczywistego [4], co w praktyce, ze względu

na koszty i konieczność specjalistycznych szkoleń, zdarza się dość rzadko.

Ponadto w przypadku użycia PC istnieje dodatkowe zagrożenie zastosowań, dość oczywiste, choć często niedostrzegane lub ignorowane. Jest nim czynnik ludzki i fizyczna dostępność interfejsów komputera PC. Pracownicy, szczególnie ci niekoniecznie świadomi zagadnień informatycznych i zagrożeń opisanych w niniejszym artykule, bardzo często będą ingerować w oprogramowanie komputera, starając się uatrakcyjnić sobie pracę lub zmienić czynniki wpływające na ocenę ich pracy. Innymi słowy będą instalowali gry i modyfikowali oprogramowanie nadzorcze. Powoduje to niepożądane efekty w postaci zachwiania integralności systemu oraz przekłamania danych. Nieszczęśliwym trafem zakładowe działy IT przeważnie nie interesują się komputerami PC, które są wykorzystane w strukturach ISP. Efektem są permanentne infekcje różnego rodzaju, osłabienie wydajności komputerów oraz upadki systemu. Jest to o tyle zastanawiające, że od tych „nielubianych" systemów zależy funkcjonowanie produkcji, a więc i całej reszty biznesu.

Komputery PC powinny być stosowane tylko do realizacji wzmiankowanych wcześniej interfejsów z użytkownikiem przy zachowaniu zabezpieczeń wynikających z cechy niezawodności systemu. Aktualnie do podstawowych zabezpieczeń należą:

- system operacyjny z logowaniem użytkowników (autoryzacja użytkownika komputera i autoryzacja użytkownika oprogramowania) wraz z dobrą administracją. Pisanie o „dobrej" administracji wykracza poza zakres artykułu, ale założono, że Czytelnik jest świadom, iż np. hasła typu „1234" nie są dobre);
- oprogramowanie typu *firewall* (blokowanie niepożądanego ruchu sieciowego);
- oprogramowanie antywirusowe (blokowanie ataków złośliwego oprogramowania);
- przydzielanie przeszkolonych administratorów do zarządzania i pielęgnacji komputera (instalowanie aktualizacji, utrzymanie dysków, czyszczenie, diagnostyka itp.).

Wygodnie jest, aby komputer mógł być zarządzany zdalnie, ale wówczas należy zatroszczyć się o odpowiednie zabezpieczenie dostępu. Zabezpieczenia należy zawsze dopasowywać do bieżącego stanu zagrożeń, nie ufając, że stare, sprawdzone sposoby będą zawsze wystarczające.

Dobrze, aby konto administratora było wykorzystywane tylko do celów administracyjnych, tylko przez administratorów i zgodnie z wiedzą informatyczną. Praktyczne obserwacje autora przerażają. W większości przypadków hasła są trywialne, nazwy użytkowników również, na koncie administratora pracuje niemal każdy, uprawnienia są dawane z tzw. „zapasem na wszelki wypadek, jakby coś nie chciało działać", czyli wszystkie, jakie tylko można. Dotyczy to każdego elementu systemu i stanowi ogromną i potencjalnie bardzo niebezpieczną dziurę w bezpieczeństwie systemu, umożliwiając hackerom prowadzenie szpiegostwa gospodarczego, zakłóceń i zatrzymań procesu, uszkodzeń produktów itp. Dlatego komputer klasy PC należy otoczyć szczególną troską i przemyśleniem, o ile występuje on w danym ISP.

Dobór urządzeń powinien również uwzględniać sytuacje awaryjne i ich obsługę. Najczęściej do zabezpieczania przed upadkiem (awarią) systemu z powodu awarii jego komponentów używa się układów redundantnych [5], opisanych szerzej w podrozdziale 3.3, lub wbudowanych mechanizmów zwiększających odporność na upadki [2].

2.4. Sieci

ISP są systemami przeważnie rozproszonymi terytorialnie. Wymaga to przekazywania danych pomiędzy rozproszonymi aplikacjami systemu z uwzględnieniem ograniczeń czasowych. Współcześnie przekazywanie odbywa się najczęściej z użyciem komputerowych sieci przemysłowych. Istnieją trzy generacje takich sieci [6, 7]. Klasyczne rozwiązania stanowią sieci polowe (miejscowe, systemowe, ang. *fieldbus*), bardziej nowoczesne i uniwersalne są sieci klasy RTE (Ethernet przemysłowy, ang. *Real Time Ethernet*), natomiast do najbardziej wyrafinowanych aplikacji stosuje się sieci trzeciej generacji, oparte o rozwiązania heterogeniczne [7]. W każdym przypadku istnieją specjalne protokoły umożliwiające zdeterminowaną w czasie obsługę danych na medium. Sama warstwa fizyczna z dostępem swobodnym (np. RS485 czy Ethernet) nie wystarczy do zapewnienia transmisji z ograniczeniami czasowymi [8]. Stosowanie „zwykłych" sieci prowadzi do niewydolności komunikacyjnej w sytuacjach stresowych (odbiegających od typowych), do występowania nieprzewidywalnych opóźnień w obsłudze danych oraz w skrajnym przypadku do utraty danych. Zatem wysoce niezbędne jest, aby w ISP do komunikacji między węzłami stosować komputerowe sieci przemysłowe. Ich wykorzystanie umożliwia uzyskanie zdeterminowanego w czasie dostępu do medium, a co za tym idzie, zdeterminowaną w czasie wymianę danych między węzłami systemu.

Determinizm czasowy działania sieci wynika z protokołu warstwy łącza lub aplikacji ISO/OSI. Musi być to protokół kontrolujący w czasie dostęp do medium, a dodatkowo umoż-

liwiający zdefiniowanie zależności komunikacyjnych pomiędzy aplikacjami. Najczęściej zależności takie buduje się na podstawie predefiniowanego globalnego scenariusza wymian (ang. *time schema*, *scenario*). Scenariusz definiowany jest na poziomie warstwy aplikacji. Istnieje kilka modeli sieci umożliwiających implementacje protokołów kontrolujących dostęp do medium (np. *Master-Slave*, *Token Passing*, *PDC*, *TDMA*, *SCNM*, *DOMA* i inne) i kilka umożliwiających zestawienie połączeń na poziomie aplikacji (*Client-Server*, *Producer-Consumer*, *Publisher-Subscriber* itp.) [8, 9, 10].

Przy wyborze konkretnego standardu sieci należy rozważyć zagadnienia:

- zbioru wymaganych usług – w ISP przeważnie wymaga się zapewnienia transakcji cyklicznych oraz acyklicznych. Wszystkie sieci przemysłowe dostarczają takich usług. Różnica może polegać na sposobie zestawiania połączeń aplikacyjnych i uzyskiwanej charakterystyce czasowej takich transakcji [11];
- charakterystyk czasowych obsługi informacji – dobrze jest określić potrzeby przez określenie zbioru obsługiwanej informacji i wymagań względem czasu. Do obiektywnej analizy można wykorzystać pojęcie sprawności użytecznej [12, 13] lub inne analizy [14, 9, 10];
- topologii sieci – topologia jest często narzucana przez standard, choć w wielu przypadkach projektant może decydować o doborze topologii. Wybór topologii pociąga za sobą złożoność okablowania, jak i podatność na upadek systemu w przypadku awarii medium;
- technologii łączenia – wybór właściwego medium dla środowiska i występujących w nim zaburzeń, jak również zagadnienia podłączeń (punkty przyłączeniowe, minimalne i maksymalne odległości, terminatory, technologie przełącznikowe, rozdzielające, wzmacniające itp.) są kluczowe dla zapewnienia poprawnego działania sieci.

Dla zapewnienia pewności działania (ang. *safety*), z punktu widzenia konstrukcyjnego, sieci muszą posiadać zabezpieczenia fizyczne i logiczne umożliwiające pracę w środowisku przemysłowym. Są to:

- odpowiednie kable (uziemiane ekrany, wzmocnione konstrukcje mechaniczne, parametry elektryczne itp.);
- odpowiednie łączówki (uziemiane obudowy, wyższa klasa IP niż dla rozwiązań biurowych, zabezpieczenia przed odpięciem, wypadnięciem, zabezpieczenia przed błędnym podpięciem, zabezpieczenia wolnych gniazd, podstawowa diagnostyka itp.);
- odpowiednia detekcja i korekcja ramek (preambuły, postambuły, sumy kontrolne, praca cykliczna i/lub retransmisja, kodowanie i transmisja odporna na zaburzenia EMC, itp.);
- identyfikacja i obsługa przekroczeń czasów granicznych na warstwie łącza i aplikacji (ang. *timeouts*, mechanizmy statusów jakości danych użytecznych);
- kontrola ruchu pochodzącego spoza systemu (infrastruktura z priorytetami i/lub klasyfikacją ruchu, np. odpowiednie przełączniki, firewalle w węzłach interfejsowych);
- działanie przełączników musi być zgodne ze stosowanymi protokołami. Często sieci RTE wymagają priorytetyzacji ruchu (np. sieci VLAN IEC802.1Q) lub konkretnych metod przekazywania danych na portach (np. *Store and Forward*, *Cut Through*, *Time Triggered*);
- działanie programów antywirusowych wymaga cyklicznej aktualizacji i wprowadza opóźnienia w przetwarzaniu danych. Należy zapewnić możliwość aktualizacji takiego oprogramowania oraz upewnić się, że złożone analizy (np. heurystyczne) nie zaburzają pracy węzła systemu. W przeciwnym wypadku należy zrezygnować z jego działania i skanować system okazjonalnie urządzeniami zewnętrznymi;
- działanie ścian ogniowych wprowadza opóźnienia w ruchu sieciowym z danym węzłem. Może to mieć wpływ na działanie tego węzła oraz, z racji zwiększenia czasów odpowiedzi (ang. *timeout*), na działanie całego systemu.

3. Niezawodność działania

Według współczesnych wymogów utrzymania ruchu kwestie związane z działaniem systemu powinny być traktowane szerzej niż tylko jako zadania regulacji i przekazywania danych. Szczególnie dotyczy to zadań komunikacyjnych w systemach rozproszonych, gdyż to ze strony sieci pojawiają się obecnie największe niebezpieczeństwa.

Zagrożenia poprawnego funkcjonowania systemu i kontrola bezpieczeństwa z tym związana wiążą się z teorią niezawodności systemów (ang. *dependability*). Występują w niej ogólne zagrożenia klasyfikowane jako:

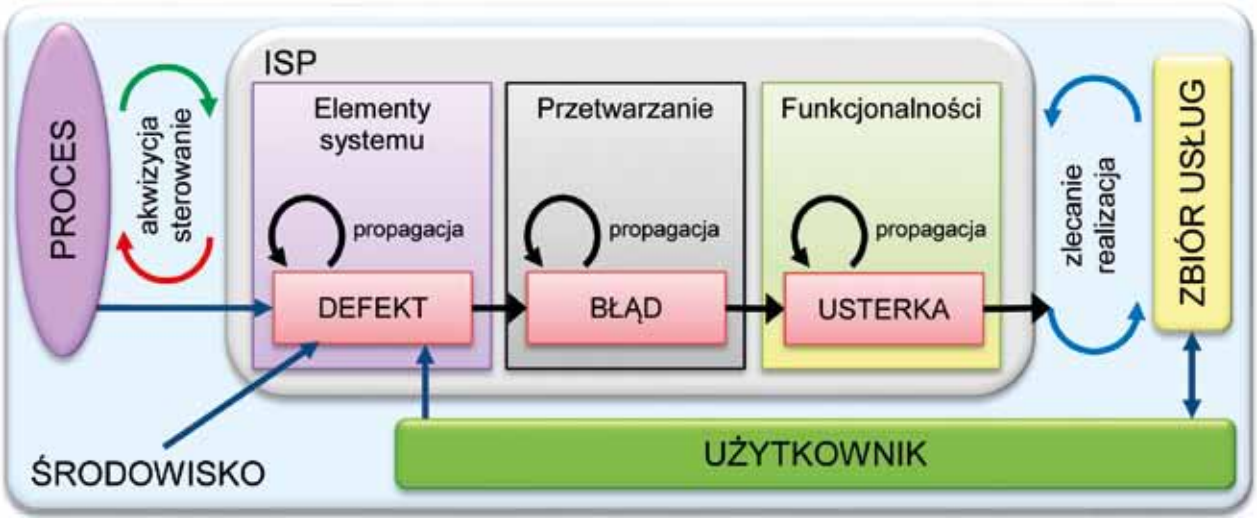
- defekt (ang. *fault*) – występuje jako efekt zaburzeń lub upadków działania komponentów systemu i wynika z wad sprzętu lub oprogramowania bądź też z błędów lub negatywnych działań użytkownika i/lub środowiska, w którym system pracuje;
- błąd (ang. *error*) – generowany jest jako efekt wystąpienia defektu i dotyczy procesu przetwarzania w węzłach systemu;
- usterka (ang. *failure*) – powodowana jest przez błędy i uniemożliwia poprawne wykonanie usług.

Wszystkie zagrożenia mogą ulegać propagacji w zakresie swojego oddziaływania. Zostało to zobrazowane na rys. 1.

Zagrożenia te mogą wpływać na bezpieczeństwo integralności zasobów (ang. *security*), bezpieczeństwo funkcjonalne (ang. *functional safety*) oraz dostępność systemu (ang. *availability*) [1]. Zostały one opisane w kolejnych podrozdziałach.

3.1. Zagrożenia dostępu

Bezpieczeństwo dostępu do zasobów systemu było przez wiele lat ignorowane jako niedotyczące ISP. Wynikało to głównie ze szczególnych cech tych systemów i priorytetów bezpieczeństwa, różniących się od tradycyjnych, biurowych systemów komputerowych. ISP, z racji swojego fizycznego umiejscowienia i odizolowania, a zatem istnienia fizycznych utrudnień dostępu, były postrzegane jako systemy, do zasobów których nie ma realnej możliwości włamania. Ponadto nie rozpatrywano tego typu systemów jako atrakcyjnych dla hackerów lub innych osób znajdujących zysk lub radość z włamania do systemów komputerowych. W praktyce takie założenie było cały czas w pewnym stopniu błędne, gdyż nawet w odizolowaniu systemy te były narażone na bezpośrednie ataki wirusów i robaków pochodzących z umyślnych lub nieumyślnych infekcji lokalnych, z nośników przenośnych. Tego rodzaju infekcje nie wpływały z reguły na działanie systemów opartych o sieci przemysłowe i PLC, gdyż nie istniało złośliwe oprogramowanie infekujące takie zasoby. W praktyce były one jednak w stanie utrudniać pracę współpracujących z nimi systemów nadrzędnych działających w oparciu o komputery klasy PC i sieć Ethernet. Rozwój dostępu zdalnego, w tym sieci Internet, sieci komórkowych, sieci bezprzewodowych itp., poszerzył ten problem [8, 15]. In-



Rys. 1. Zagrożenia i ich oddziaływania

tegracja z sieciami publicznymi, prowadzona lepiej lub gorzej, spowodowała otwarcie ISP na ataki, które do tej pory były domeną sieci ogólnodostępnych (np. DoS, DDoS, File Inclusion, SQL Injection, MIM, XSS itp.). Ponadto poza typowymi i wyrafinowanymi atakami sfery biurowej, systemy ISP zostały wystawione na ataki, których motywacją są działania związane ze szpiegostwem gospodarczym, nieuczciwą konkurencją czy wręcz sabotażem i terroryzmem. W efekcie ostatnimi laty można zaobserwować, że wirusy, robaki i inne formy szkodliwego oprogramowania coraz bardziej mogą dotknąć zakresu działania systemów automatyki [16–25]. I chociaż zaawansowane techniki ochrony zasobów dla systemów domowych, biurowych i biznesowych rozwijały się i stale się rozwijają, to dla ISP rozwoju takiego nie ma, a wręcz istnieje brak dedykowanych technik ochrony dla tego typu systemów. Przykładami ostatnich ataków na systemy przemysłowe mogą być:

- Ataki na PLC. Najbardziej znany medialnie atak ostatnich lat dokonany został przez program robaka o nazwie Stuxnet [16]. Jest to rodzaj rootkita atakującego wybrane typy PLC i narzędzi deweloperskich, rozpowszechnianego właśnie przez przenośne nośniki pamięci i sieć. Złośliwe oddziaływanie polega na zmianie sterowania przekształtnikami częstotliwości sterującymi napędami np. pomp. Dokładna skala ataków nie jest znana, ale mówi się o tysiącach zakładów na całym świecie o różnym znaczeniu, od prostej produkcji po instalacje krytyczne (np. wirówki frakcjonujące stosowane przy wzbogacaniu uranu w elektrowniach) [25].
- Uzyskanie nieuprawnionego dostępu do systemu sterowania ruchem kolejowym. Zaburzony został system sterowania sygnalizacja świetlną, co skutkowało opóźnieniami pociągów [19].
- Uzyskanie nieuprawnionego dostępu do obiektów stacji pomp wody. Akcje wielokrotnego włączania i wyłączania pompy spowodowały jej awarie [20, 21].
- Włamanie do systemu elektrociepłowni oraz routerów brzegowych [22].
- Wielokrotne włamania do systemów metropolitalnych odpowiedzialnych za kontrolę urządzeń infrastruktur miejskich [23].

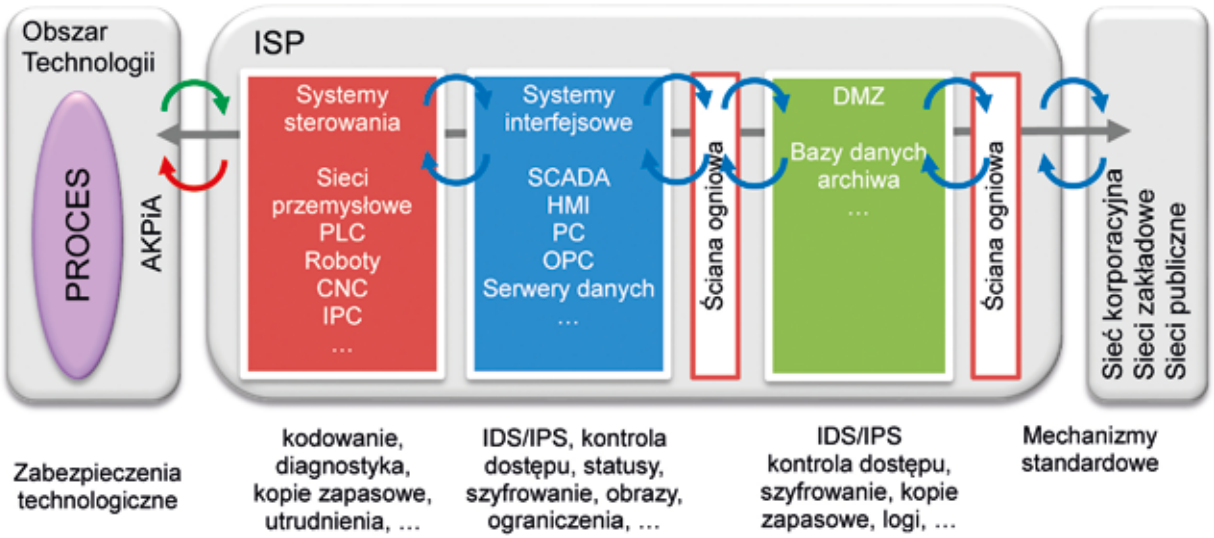
Planowo prowadzone audyty bezpieczeństwa prowadzą również do wykrycia poważnych luk. Przykładem może być przepompownia wody [24]. Dostęp uzyskano przez łącze bezprzewodowe bluetooth i hasło 0000. Do dalszego poszukiwania zagrożeń można użyć internetowego serwisu Shodan (www.shodanhq.com). Wielu ekspertów bezpieczeństwa IT uważa go za wyszukiwarkę dla hakerów. Serwis pozwala odnaleźć w sieci konkretne elementy systemów podatnych na ataki, w tym systemy ISP np. SCADA.

Dlatego zagadnienia ochrony bezpieczeństwa zasobów i ich integralności w rozumieniu ochrony informacji przed nieuprawnionym ujawnieniem, transferem, modyfikacją lub zniszczeniem – niezależnie od tego, czy przypadkowym czy celowym – należy obecnie brać pod uwagę przy projektowaniu ISP. Istnieją trzy podstawowe wymagania bezpieczeństwa zasobów [26, 27]:

- dostępność (ang. *availability*) – zdolność do poprawnej realizacji zadań na rzecz innych zasobów;
- integralność (ang. *integrity*) – zdolność do zachowania poprawności i kompletności danych;
- poufność (ang. *confidentiality*) – gwarancji, że informacje nie będą udostępniane lub ujawniane nieuprawnionym osobom, podmiotom lub procesom.

Priorytety tych wymagań są różne od wymagań w systemach biurowych. Dla ISP najważniejszym wymaganiem jest dostępność [1]. Wynika to z ochrony procesu, gdyż bez dostępności zasobów prowadzenie procesu jest niemożliwe. Na drugim miejscu jest integralność danych. Poprawna realizacja zadań regulacji jest możliwa tylko z użyciem poprawnych i kompletnych danych, zarówno w wymiarze ich wartości, jak i orientacji w czasie. Brak ochrony poufności nie uniemożliwia działania ISP, choć w wyniku takiego braku może dojść do zachwiania lub zaniku integralności, a nawet dostępności zasobów.

Zagrożenia tego typu nie są tylko problemem sieci, a proste rozdzielanie sieci zaporami ogniowymi (ang. *firewall*) nie jest wystarczające i nie umożliwia zachowania specyficznej obsługi informacji w ISP. Należy brać pod uwagę wszelkie środki zapobiegające dostępowi nieuprawnionych ludzi lub oprogramowania do systemu krytycznego. Istnieją mechanizmy obronne niezwiązane z funkcjonalnością samego systemu i pracujące niejako obok. Mogą one zmniejszyć zagrożenia od nieuprawnionego dostępu do zasobów. Dzielą się one na trzy kategorie [1]:



Rys. 2. Umiejscowienie środków ochrony dostępu do zasobów

- mechanizmy prewencji – są to podstawowe mechanizmy obrony, których celem jest uniemożliwienie skutecznego oddziaływania zagrożenia;
- mechanizmy detekcji – są to programy śledzące zachowanie ruchu sieciowego oraz aktywności węzłów i reagujące w sytuacjach, gdy odbiegają od przyjętego wzorca. Celem takich systemów jest wykrycie dokonanego już ataku;
- mechanizmy reakcji i przywracania – są to zadania w systemie, które mają za cel minimalizowanie szkód w przypadku wykrytego ataku oraz przywrócenie systemu do poprawnego działania, gdy w wyniku ataku pojawiły się jakieś defekty.

W przypadku komputerowych sieci przemysłowych stosuje się mechanizmy prewencji i detekcji. Najczęściej bezpieczeństwo zapewniają:

- Utrudniony fizyczny dostęp do switchów, hubów, routerów, access-pointów i innych aktywnych elementów infrastruktury. Elementy te powinny być zlokalizowane w miejscach umożliwiających dostęp tylko osobom uprawnionym. Z racji pracy na terenie zakładów przemysłowych jest to łatwe do zapewnienia względem osób spoza zakładu. Jednak zawsze pracowników należy również traktować jako potencjalne źródło zagrożenia.
- Działanie mechanizmów autoryzacji w węzłach interfejsowych. Dla człowieka i innych urządzeń uniemożliwienie nieuprawnionego dostępu do węzłów, uniemożliwienie wprowadzenia niepożądanego ruchu.
- Pokrycie zasięgiem sieci bezprzewodowych powinno być minimalnie niezbędne.
- Sieci bezprzewodowe powinny mieć załączone zabezpieczenia w standardzie WPA2 z szyfrowaniem AES/TKIP lub innym dającym porównywalny lub wyższy poziom bezpieczeństwa transmisji, jak również powinno się wykorzystywać złożone hasła dostępu.
- Montaż uniemożliwiający uzyskanie dostępu do medium i łączówek.
- Obsługa transmisji sieciowych tylko z określonych adresów.
- Detekcja i odrzucanie ruchu obcego przez wykorzystanie ścian ogniowych lub podobnych rozwiązań.

W przypadku węzłów systemu, czyli różnego rodzaju komputerów (PLC, ICS, DCS itp.), stosuje się wszystkie rodzaje mechanizmów dodatkowych. W tym wypunktowane poniżej i zilustrowane na rys. 2.

Utrudnienia lub ograniczenia w dostępie fizycznym do szafy, urządzeń i ich interfejsów (pamięć, urządzenia HID, sieci PAN itp.) oraz w uruchamianiu dodatkowych funkcji i kodu.

Sprzęt i oprogramowanie kodujące, konwertujące, szyfrujące i dokonujące identyfikacji, autoryzacji i uwierzytelniania. Ponadto wszelkie mechanizmy diagnostyczne sprzętu, jak wykrywanie awarii, zmian konfiguracji, sum kontrolnych, przeciwdziałania wykonywaniu kodu itp.

Systemy klasy IDS (ang. *Intruder Detection System*). Są to systemy analizujące transakcje sieciowe węzła i sieci w czasie rzeczywistym pod kątem adresów i zawartości użytecznej. W ISP aktywności sieciowe są mało zmienne, dlatego działanie takich systemów może być bardzo przydatne i skuteczne. W praktyce nie ma specjalizowanych systemów tej klasy dedykowanych dla ISP, a te istniejące są uniwersalne i nie są dostosowane do specyfiki węzłów ISP.

Systemy IPS (ang. *Intrusion Prevention System*). Działają tak jak IDS z tym, że dodatkowo posiadają funkcjonalności blokowania ataków w czasie rzeczywistym.

Strefy DMZ (ang. *Demilitary Zone*). Jest to wydzielony obszar sieci znajdujący się pomiędzy siecią zewnętrzną a wewnętrzną strefą chronioną. W przypadku ataku infekcji ulegają zasoby w strefie DMZ, a atak jest powstrzymany do obszaru tej strefy. Stosuje się głównie do zabezpieczania krytycznych obszarów wymiany danych. Dla ochrony pojedynczych węzłów ISP jest to mechanizm mało praktyczny. W DMZ nie powinny znajdować się systemy oddziałujące bezpośrednio z procesem, a jedynie te ich zasoby, które są wykorzystywane przez systemy współpracujące.

Przywracanie obrazów węzłów. Proste i skuteczne działania reakcji przeważnie dokonywane ręcznie przez administratorów lub utrzymanie ruchu. Istotne jest, aby nie tylko móc przywrócić komputer do działania, ale i mieć odpowiedni obraz do przywrócenia. Należy zatem dbać o cykliczne tworzenie takich obrazów. Dotyczy to zarówno kopii programów, konfiguracji, całej pamięci (w tym dysków), jak i backupów baz danych.

Ściany ogniowe, poza standardową funkcjonalnością filtracji pakietów, powinny mieć funkcjonalności umożliwiające wprowadzanie i wyprowadzanie informacji bez zakłócania obiegu danych w sieciach przemysłowych [28].

Tabela 1. Miary SIL względem PFD i konsekwencji

SIL	PFD (THR)	Konsekwencje
1	$10^{-6} \leq PFD < 10^{-5}$	niewielkie urazy i uszkodzenia
2	$10^{-7} \leq PFD < 10^{-6}$	poważne urazy, jednostkowa śmiertelność
3	$10^{-8} \leq PFD < 10^{-7}$	niejednostkowe zagrożenie życia
4	$10^{-9} \leq PFD < 10^{-8}$	liczna śmiertelność

Tabela 2. Szacowanie SIL na podstawie macierzy ryzyka

	Klasa prawdopodobieństwa		
Klasa konsekwencji	okazjonalne	prawdopodobne	częste
katastrofalne	3	3	4
krytyczne	2	3	3
marginalne	1	2	3
nieznaczne	brak	1	2

Przy działaniach prewencyjnych ważne jest, aby ustalić kwestie kluczowe funkcjonowania zabezpieczeń [1] dotyczące:
- polityki bezpieczeństwa firmy;
- listy zagrożeń realnych i mało prawdopodobnych;
- ustaleń procedur kontrolnych weryfikujących działanie polityki bezpieczeństwa;
- ustaleń procedur testowych systemu weryfikujących, że wprowadzone mechanizmy nie wpływają negatywnie na działania ISP.

Czasami bezpieczeństwo uzyskuje się przez ukrycie detali implementacyjnych systemu (ang. *security through obscurity*). Nie jest to jednak technika zalecana, gdyż bazuje tylko na potencjalnej niewiedzy atakujących i jest w sprzeczności z zasadą Kerckhoffsa [29].

3.2. Zagrożenia funkcjonalne

Bezpieczeństwo funkcjonalne (BF) jest to stan układu wolny od niedopuszczalnego ryzyka wystąpienia uszczerbku na zdrowiu ludzi, bezpośrednio lub pośrednio w wyniku uszkodzenia mienia lub środowiska [3].

Różnice w podejściach do tematu bezpieczeństwa funkcjonalnego wynikają z przyjętego punktu widzenia na umiejscowienie mechanizmów zapewniania poprawności działania. Teoria niezawodności, w zakresie zagrożeń funkcjonalnych, charakteryzuje usługi zapewniania bezpieczeństwa dostarczane przez system. Teoria bezpieczeństwa funkcjonalnego dotyczy natomiast wszelkich środków dodanych do systemu celem zapewnienia bezpieczeństwa jego działania. Istnieją zatem rozwiązania zwiększające bezpieczeństwo użytkowania układu, które są wbudowane w system i jego elementy, oraz niezależne systemy bezpieczeństwa działające niejako obok ISP [7]. Cel działania w obu przypadkach jest podobny, a funkcjonalności związane z bezpieczeństwem nie są związane z funkcjonalnościami ISP.

Standardy BF (IEC 61508) obejmują analizę zagrożeń (ang. *hazard*) i ryzyka (ang. *risk*) [30] oraz wymagania względem zabezpieczeń. Analiza zagrożeń dotyczy określania potencjalnych źródeł szkodliwego oddziaływania na człowieka, mienie lub środowisko, a także określania awarii (wypadków, ang. *accident*), czyli niepożądanych zdarzeń zachodzących w konsekwencji wystąpienia nieprzewidzianych zagrożeń. Analiza

ryzyka dotyczy natomiast określania miary niebezpieczeństw płynących z wystąpienia awarii [31]. Formułuje się ją na podstawie częstości (lub prawdopodobieństwa) wystąpień oraz ich konsekwencji (dotkliwości, ang. *severity*) oddziaływania na otoczenie. Typowymi klasami częstości wystąpienia są: częste, prawdopodobne, okazjonalne, mało prawdopodobne, nieprawdopodobne oraz jednostkowe. Typowymi klasami konsekwencji są: katastrofalne, krytyczne, marginalne oraz nieznaczne.

Działanie systemów BF (ang. *safety-related systems*) ma na celu zapewnienie określonego poziomu bezpieczeństwa układu przez zmniejszanie ryzyka. Wymagania względem bezpieczeństwa układu wynikają z analizy ryzyka i są określane przez prawdopodobieństwo wystąpienia awarii (PFD – ang. *Probability of Failure on Demand*) lub akceptowalny poziom zagrożeń (THR – ang. *Tolerable Hazard Rate*). Najczęściej jednak określa się je czterostopniową miarą jakościową SIL (ang. *Safety-Integity Level*), określającą w czterech przedziałach prawdopodobieństwo wystąpienia usterki lub prawdopodobną liczbę zadziałań układu do wystąpienia pierwszej usterki. Miara SIL i prawdopodobieństwa usterki zostały przedstawione w tabeli 1.

Systemy bezpieczeństwa muszą być implementowane, gdy ryzyko związane z zagrożeniami jest niedopuszczalne. Istnieją techniki szacowania poziomu SIL do istniejącego ryzyka. Do najpopularniejszych należy metoda bazująca na konsekwencjach oraz na macierzy ryzyka [31]. Zilustrowane one zostały w tabeli 1 oraz tabeli 2.

W ogólnej masie większość aplikacji przemysłowych nie stanowi systemów krytycznych względem bezpieczeństwa funkcjonalnego. Jednak gdy z analizy ryzyka wynika konieczność stosowania środków zabezpieczających, nigdy nie należy ignorować takich zagrożeń.

3.3. Dostępność

ISP w zastosowaniach krytycznych muszą charakteryzować się wysoką dostępnością, czyli zdolnością systemu do wykonania wymaganej funkcji w danych warunkach i w danym momencie czasu lub w określonym przedziale czasu, przy założeniu, że dostępne są wymagane do działania zasoby i dane zewnętrzne. Miarę dostępności zdefiniowano w następnym rozdziale.

W ISP zarówno dostępność komputerów, jak i dostępność sieci jest kluczowym zagadnieniem. Jednym ze sposobów zwiększenia dostępności jest wykorzystanie redundancji środków transmisji w sieci, elementów węzłów systemu lub całych węzłów. Przez dodanie nadmiarowości sprzętu i oprogramowania system staje się bardziej odporny na usterki. Oznacza to, że w przypadku wystąpienia błędów w systemie system nie zawodzi względem realizacji wymaganej funkcji, gdyż jest w stanie wyeliminować zdiagnozowane defekty. W przypadku awarii danego zasobu, system przełącza się na kolejny dostępny. Najistotniejszym parametrem pracy układów redundantnych, dla zapewnienia dostępności systemu, jest czas przełączania (ang. *switchover*) przy zachowaniu spójności stanu. Jeżeli czas ten jest mniejszy lub równy okresowi akwizycji i aktualizacji informacji na danym elemencie systemu, oraz gdy po przełączeniu stan aktywnego elementu jest taki sam, jak stan elementu uszkodzonego, to mówi się o pracy bezuderzeniowej. Z punktu widzenia procesu zmiana elementu na rezerwowy jest wówczas niezauważalna. W przypadku, gdy czas ten jest większy, może dojść do zaburzenia sterowania (lub regulacji) lub ogólnie do negatywnego oddziaływania takiego przełączania na proces.

Zwielokrotnione elementy systemu mogą pracować w trybie „gorącej rezerwy” (ang. *hot standby*), zimnej rezerwy (ang. *cold standby*) lub rezerwy ciepłej (ang. *warm standby*). W trybie gorącej rezerwy zwielokrotnione środki sprzętowo-programowe stanowią element systemu i są gotowe do przejęcia zadań i udostępnienia usług ze zwłoką wynikającą z cyklu diagnostycznego i synchronizacyjnego. W praktyce jest to działanie bezuderzeniowe. Rezerwa zimna oznacza utrzymywanie zapasu komponentów systemu na wewnętrznych stanach magazynowych utrzymania ruchu. W przypadku awarii istnieje możliwość wymiany uszkodzonego elementu systemu. Jest to tryb zdecydowanie oddziałujący na pracę układu, a wykonanie stosownej procedury w trybie bezuderzeniowym jest w praktyce mało realne. Tryb ciepłej rezerwy oznacza utrzymywanie zwielokrotnionych elementów w trybie gotowości do pracy, aczkolwiek bez integracji z działającym systemem. Oznacza to, że elementy są zabudowane na obiekcie i niejednokrotnie gotowe do pracy, ale przełączenie następuje w wyniku zadziałania czynników zewnętrznych, np. serwisu, utrzymania ruchu itp.

W klasycznym podejściu typu *standby* dane środki sprzętowo-programowe oczekują bezczynnie na awarię środków podstawowych i przejmują ich funkcję, gdy ta awaria wystąpi. Aby to było możliwe, muszą działać specjalne mechanizmy utrzymujące gotowość urządzeń do natychmiastowego uruchomienia. Są one wbudowane w redundowane elementy i działają w czasie rzeczywistym systemu. Mechanizmy te obsługują synchronizację stanu, detekcję awarii oraz wypracowują decyzję, który z elementów jest aktywny w systemie. Istnieje również podejście typu *duplex* bazujące na równoległym (jednoczesnym) działaniu zwielokrotnionych elementów bez określania elementu aktywnego. Wybór elementu, z którego korzystają inne elementy systemu, dokonywany jest przez te elementy.

Redundancja dotyczy także infrastruktury sieci i medium [5]. Zwielokrotnianie całej sieci nie jest zbyt efektywnym sposobem redundancji sieci, choćby ze względów ekonomicznych. Jest jednak stosowane. Do detekcji awarii danej sieci używane są wskaźniki stopy błędów bądź parametry czasowe transmisji. Lepszym, prostszym i tańszym podejściem jest dublowanie medium na bazie architektury dwukierunkowego pierścienia. Umożliwia ona zbudowanie systemu tolerującego awarię medium z przełączeniem bezuderzeniowym [32, 33, 34]. Jeszcze lepszym rozwiązaniem jest sieć typu *mesh*, ale zarządzanie i obsługa przełączania w czasie rzeczywistym jest bardzo trudna do realizacji praktycznej. Przegląd metod redundancji dla Ethernetu czasu rzeczywistego można znaleźć w [35].

3.4. Miary

Do mierzenia niezawodności ISP zostały zdefiniowane miary statystyczne [31, 4] wyrażające się wskaźnikami dotyczącymi:

- rzetelności (ang. *reliability*) – jest to wskaźnik określający prawdopodobieństwo, że system poprawnie wykona usługi w danych warunkach i w danym czasie liczonym od ostatniego czasu, kiedy zostały one poprawnie wykonane. Wskaźnik ten nazywa się powszechnie MTTF (ang. *Mean Time To Failure*);
- konserwacji (ang. *maintainability*) – jest to wskaźnik określający prawdopodobieństwo, że system poprawnie wykona usługi w danych warunkach i w danym czasie, liczonym od czasu wystąpienia awarii. Powszechnie używa się nazwy MTTR (ang. *Mean Time To Repair*);

- dostępności (ang. *availability*) – jest to wskaźnik określający prawdopodobieństwo, że system poprawnie wykona usługi w danych warunkach i w danym czasie. Wskaźnik wyrażany jest zależnością:

$$A = \frac{MTTF}{MTTF + MTTR}$$

3.5. Normalizacja

Podstawowym standardem dla bezpieczeństwa funkcjonalnego związanego z systemami rozproszonymi jest seria norm IEC61508 (ang. *Functional Safety Guide*) [3]. Definiuje ona możliwe struktury sprzętu i oprogramowania oraz proces bezpiecznego projektowania. Normalizację ochrony struktur krytycznych obejmuje standard dotyczący wymagań względem bezpieczeństwa cyfrowego (ang. *cyber security*) IEC 62351, 61334, 62056 oraz EN 13757 [36, 37].

Dla systemów rozproszonych znormalizowaniu podlegają także protokoły sieciowe. Wszystkie proponowane rozwiązania związane z bezpieczeństwem dla sieci przemysłowych są zebrane w części trzeciej normy IEC61784 (ang. *Functional Safety for Fieldbus*) [38]. Dla wszystkich sieci z normy sprecyzowane są potencjalne błędy działania jako źródła możliwych usterek i pokazane jest, jak zdefiniowane rozwiązania bezpieczeństwa zapewniają zachowanie integralności systemu. Typowymi metodami są dodawanie dodatkowych danych w poszczególnych warstwach stosu (np. w postaci preambuł, sum kontrolnych, statusów jakości itp.) i redundancja [39, 5]. Środki programowe są zazwyczaj implementowane na szczycie stosów kanałów komunikacyjnych (zasada *black channel*) [7]. Ustandaryzowane (tzn. niezależne od danej aplikacji) metody redundancji medium są zebrane w normie IEC 62439 (ang. *High Availability Networks*).

4. Podsumowanie

Rozważanie aspektów bezpieczeństwa przy tworzeniu, modyfikacji czy utrzymaniu komputerowo wspomaganych systemów przemysłowych jest niezwykle istotne. Postawy ignorujące zagrożenia w sposób świadomy lub często nieświadomy, a co za tym idzie, pomijanie aplikacji systemów bezpieczeństwa wcześniej czy później prowadzi do przykrych konsekwencji. Przedstawione w artykule podstawowe aspekty bezpieczeństwa, w kontekście elementów składowych systemów oraz teorii ogólnej, powinny nakierować czytelnika na zagadnienia warte dalszych rozważań, a także przybliżyć wiedzę, gdzie i czego należy szukać w temacie współczesnych sposobów zapewniania bezpieczeństwa.

Wysoce wskazane jest aby inżynierowie odpowiedzialni za tworzenie systemów klasy ISP stosowali dobre praktyki wskazane w artykule lub dostępne w innych źródłach np. rekomendacje US ICS-CERT (*United States Industrial Control Systems – Cyber Emergency Response Team*) [40]. Artykuł zawiera fragmenty przygotowywanej książki *Systemy informatyki przemysłowej*.

Literatura

[1] Cheminod M., Durante L., Valenzano A.: *Review of Security Issues in Industrial Networks*, Industrial Informatics, IEEE Transactions on , vol. 9, no. 1, pp. 277, 293, Feb. 2013.

[2] Kirrmann H.: *Fault tolerant computing in industrial automation*, ABB Research Center, Tech. Rep. 2nd Edition, 2005.

[3] IEC, *Functional safety of electrical/electronic/programmable electronic safety-related systems – part 1 to 7*, in International Standard IEC 61508-x, 2nd ed. IEC, June 2010.

[4] Kopetz H.: *Real-Time Systems*, Springer US 2011.

[5] Kwiecień A., Stój J.: *The Cost of Redundancy in Distributed Real-Time Systems in Steady State in Computer Networks*, pp. 106–120, CCIS vol 79, Springer, Berlin – Heidelberg 2010.

[6] Sauter T.: *The three generations of field-level networks - evolution and compatibility issues*, Industrial Electronics, IEEE Transactions on, vol. 57, no. 11, pp. 3585–3595, Nov. 2010.

[7] 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, Feb. 2013.

[8] Gaj P.: *Przemysłowy Ethernet – szybko i wydajnie?,* „Napędy i Sterowanie", 11/2010, s. 78–84.

[9] Felser M.: *Real-time ethernet – industry prospective*, Proceedings of the IEEE, vol. 93, no. 6, pp. 1118–1129, June 2005.

[10] Decotignie J.: *The many faces of industrial ethernet [past and present]*, Industrial Electronics Magazine, IEEE, vol. 3, no. 1, pp. 8–19, March 2009.

[11] Gaj P.: *The Concept of a Multi-Network Approach for a Dynamic Distribution of Application Relationships,* CCIS 160 Springer, Berlin – Heidelberg 2011, ISSN 1865-0929.

[12] Gaj P.: *Pessimistic useful efficiency of epl network cycle*, Computer Networks, ser. Communications in Computer and Information Science, A. Kwiecien, P. Gaj, and P. Stera, Eds. Springer, Berlin – Heidelberg 2010, vol. 79, pp. 297–305.

[13] Gaj P., Kwiecień B.: *Useful efficiency in cyclic transactions of Profinet IO*, Studia Informatica, Gliwice 2010, PL ISSN 0208-7286.

[14] Jasperneite J., Imtiaz J., Schumacher M., Weber K.: *A proposal for a generic real-time Ethernet system*, Industrial Informatics, IEEE Transactions on, vol. 5, no. 2, pp. 75–85, May 2009.

[15] Gaj P.: *Przyjazny monitoring – zdalnie, bezprzewodowo i w Internecie*, „Napędy i Sterowanie", 3/2009, s. 114–116.

[16] Langner R.: *Stuxnet: Dissecting a cyberwarfare weapon*, Security & Privacy, IEEE, vol. 9, no. 3, pp. 49–51, May-June 2011.

[17] Che T., Abu-Nimeh S.: *Lessons from stuxnet*, Computer, IEEE, vol. 44, no. 4, pp. 91–93, April 2011.

[18] Carcano A., Coletta A., Guglielmi M., Masera M., Fovino I., Trombetta A.: *A multidimensional critical state analysis for detecting intrusions in scada systems*, Industrial Informatics, IEEE Transactions on, vol. 7, no. 2, pp. 179–186, May 2011.

[19] Sternstein A.: *Hackers Manipulated railway computers*, InfoSec News, 2012.

[20] Nakashima E.: *Water-pump failure in Illinois wasn't cyberattack after all* November 25, The Washington Post, 2011.

[21] Weiss J.: *Water System Hack – The System Is Broken*, Control Global Digital Edition, 2011.

[22] Xinghu Z.: *Latvenergo RIGAS HES-2 HACKED*, Seclists, 2011.

[23] Hodson H.: *Hackers accessed city infrastructure via SCADA – FBI*, Information Age, 2011.

[24] Johnsrud I., Haugan B., Hegvik G.K., Glomnes L.M., Larsen-Vonstett Ø.: *Could have stopped the water supply from mobile*, VG Nett, 2011.

[25] Kushner D.: *The real story of stuxnet*, Spectrum, IEEE , vol. 50, no. 3, pp. 48, 53, March 2013.

[26] Dzung D., Naedele M., von Hoff T.P., Crevatin M.: *Security for Industrial Control Systems*, Proc. IEEE, vol. 93, no. 6, pp. 1152–1177, 2005.

[27] Parks R.C., Rogers E.: *Vulnerability Assessment for Critical Infrastructure Control Systems*, IEEE Security Privacy, vol. 6, no. 6, pp. 37–43, 2008.

[28] Gaj P., Ober J.: *Firewall++ do zastosowań w systemach przemysłowych*. Studia Informatica col 24, Gliwice 2003.

[29] Anderson R.: *Security Engineering*, Willey, april 2008.

[30] Sato Y.: *Throwing a bridge between risk assessment and functional safety*, in SICE, 2007 Annual Conference, sept. 2007, pp. 2484–2488.

[31] Buja G., Menis R.: *Dependability and Functional Safety: Applications in Industrial Electronics Systems*, Industrial Electronics Magazine, IEEE , vol. 6, no. 3, pp. 4, 12, Sept. 2012.

[32] Kirrmann H., Weber K., Kleineberg O., Weibel H.: *Hsr: Zero recovery time and low-cost redundancy for industrial Ethernet (high availability seamless redundancy, iec 62439-3)*, in Emerging Technologies Factory Automation (ETFA), 2009 IEEE Conference on, sept. 2009, pp. 1–4.

[33] Kirrmann H., Hansson M., Muri P.: *Iec 62439 prp: Bumpless recovery for highly available, hard real-time industrial networks*, in Emerging Technologies and Factory Automation (ETFA), 2007 IEEE Conference on, sept. 2007, pp. 1396–1399.

[34] De Dominicis C., Ferrari P., Flammini A., Rinaldi S., Quarantelli M.: *On the use of ieee 1588 in existing iec 61850-based sass: Current behavior and future challenges*, Instrumentation and Measurement, IEEE Transactions on, vol. 60, no. 9, pp. 3070–3081, sept. 2011.

[35] Wisniewski L., Hameed M., Schriegel S., Jasperneite J.: *A survey of ethernet redundancy methods for real-time Ethernet networks and its possible improvements*, in *Fieldbuses and Networks in Industrial and Embedded Systems*, ser. In: 8th International Conference on Fieldbuses networks in Industrial; Embedded Systems (FET'2009), H. S. H. Juanole, Guy, Ed. IFAC, May 2009, vol. 8, no. Part 1.

[36] Ten C.W., Manimaran G., Liu C.C.: *Cybersecurity for critical infrastructures: Attack and defense modeling*, IEEE Trans. Syst. Man, Cybern. A, vol. 40, no. 4, pp. 853–865, July 2010.

[37] Fries S., Hof H.J., Seewald M.: *Enhancing IEC 62351 to improve security for energy automation in smart grid environments*, in Proc. 5th Int. Conf. Internet Web Applications Services (ICIW), 2010, pp. 135–142.

[38] IEC: *Industrial communication networks – profiles – part 3: Functional safety fieldbuses, several subparts*, in *International Standard IEC 61784-3-x*, 2nd ed. IEC, June 2010.

[39] Kwiecień A., Gaj P.: *Bezpieczeństwo w sieciach przemysłowych*. BISK'02, WPKJS, Gliwice 2002.

[40] US ICS-CERT, *Introduction to Recommended Practices*, dostępne na http://ics-cert.us-cert.gov/practices

dr inż. Piotr Gaj – od roku 1994 pracuje w Instytucie Informatyki wydziału AEI Politechniki Śląskiej, zajmując się rozwiązaniami komunikacyjnymi dla systemów przemysłowych.
Jest organizatorem międzynarodowej konferencji „Computer Networks" (http://sk.polsl.pl), e-mail: piotr.gaj@polsl.pl

artykuł recenzowany