prof. dr inż. Tadeusz Missala
Przemysłowy Instytut Automatyki
i Pomiarów, Warszawa
e-mail: tmissala@sg.piap.waw.pl

ZAGADNIENIA WYBRANE BEZPIECZEŃSTWA SIECIOWYCH INSTALACJI AUTOMATYKI

Współczesne układy automatyki szeroko korzystają z sieci komputerowych umożliwiających realizowanie struktur zdecentralizowanych. W śród funkcji realizowanych przez te układy jest wiele funkcji wiążących się z bezpieczeństwem, toteż struktury sieciowe powinny spełniać wymagania odpowiednich dyrektyw i norm. Analiza zagrożeń i ryzyka w instalacjach zautomatyzowanych prowadzi wielokrotnie do wniosku, że koniecznym jest wprowadzenie struktur przyrządowych o określonym poziomie nienaruszalności bezpieczeństwa. Zagadnienia zapewnienia takiego poziomu w układach sieciowych jest przedmiotem referatu.

CHOOSEN SAFETY PROBLEMS CONCERNING THE NETWORK AUTOMATION SYSTEMS

Automation systems of today used widely the computer networks to realise the distributed architectures. These systems execute many safety-related functions, and this is the reason, the networks shall comply the requirements of relevant UE Directives and standards. Hazard and risk analysis concerning the automated installations, in many cases leads to the conclusion, it is necessary to introduce the control instruments, performing a defined System Integrity Level. The problems, how to achieve such a level, are the object of the paper.

1. WSTĘP

We współczesnych instalacjach automatyki coraz częściej są stosowane rozwiązania sieciowe, tj. łączenie urządzeń obiektowych między sobą i z urządzeniami sterowania i nadzoru wyższego poziomu, oraz tych ostatnich między sobą, za pomocą sieci komputerowych, których istotnym elementem jest wielodostępna, szeregowa magistrala przesyłu danych. Stosowane tu urządzenia i układy realizują liczne funkcje, np. start, restart, zatrzymanie pracy obiektu, sterowanie ruchami i ich prędkością, które są zaliczane do funkcji wiążących się z bezpieczeństwem. W rachubę wchodzi tu bezpieczeństwo ludzi, bezpieczeństwo środowiska, a niekiedy też bezpieczeństwo ekonomiczne.

Samo zastosowanie sieci komputerowej wprowadza dodatkowy element zagrożenia, jakim jest narażenie obiektu na powstanie stanu niebezpiecznego wynikające z przekłamania w przekazywaniu sygnałów sterujących lub niezareagowanie systemu na stan nienormalny lub awaryjny jako wynik przekłamaniu w przekazywaniu sygnałów pomiarowych i/lub sygnałów informujących o stanie alarmowym.

Większość przypadków powstawania zagrożeń może być eliminowana w drodze postępowania wg procedur przewidzianych do uzyskania bezpieczeństwa funkcjonalnego [2,5 do 8].

Tak sformułowane zadanie instalacji sieciowej implikuje jednak rozważenie bezpieczeństwa jej pracy w zależności od zastosowania i postępowanie nie tylko według zacytowanych wyżej procedur ogólnych, lecz także wymagań i wskazówek zawartych w :

- zakresie zastosowania do maszyn - w PN-EN 954-1 [9] - prowadzących do określenia wymaganej i osiąganej kategorii bezpieczeństwa; przykład analizy spełnienia przez sieć wymagań dotyczących określonej kategorii bezpieczeństwa jest przedstawiony w [1];
- w zakresie zastosowania w przemysłach procesowych - w IEC 61511-3 [10] - prowadzących do określenia wymaganego poziomu nienaruszalności przyrządowej funkcji bezpieczeństwa.

To ostatnie postępowanie jest, zdaniem autora, szczególnie ważne, gdyż umożliwia, przy najmniejszej możliwej wysokości nakładów, zredukowanie do minimum groźby wypadków wynikających z niedostatecznej nienaruszalności bezpieczeństwa instalacji.

2. SFORMUŁOWANIE PROBLEMU

Bezpieczeństwo instalacji sieciowych obejmuje następujące ważniejsze zagadnienia:
- bezpieczeństwo gromadzenia i archiwizowania danych dotyczących przebiegu procesu;
- zapewnienie bezpiecznej pracy urządzeń i instalacji sterowanych i/lub nadzorowanych lub tylko monitorowanych, przy uwzględnieniu zakłócającego oddziaływania środowiska (narażenia klimatyczne, mechaniczne, elektromagnetyczne, chemiczne itp.);
- prawidłowe i natychmiastowe reagowanie na sygnały informujące o stanach zagrażających lub mogących prowadzić do zagrożeń;
- nie powodowanie stanów zagrażających lub mogących prowadzić do zagrożeń wskutek uszkodzenia lub braku reakcji ze strony sieci komputerowej.

Podstawowym zadaniem jest więc bezpieczeństwo wymiany i przechowywania informacji.

Powstaje pytanie o jakim bezpieczeństwie należy tu mówić:
- czy tylko o bezpieczeństwie użytkowania;
- czy zagadnienie ma szersze odniesienie ?

Oczywistym jest, że potocznie rozumiane bezpieczeństwo użytkowania ma jedynie ograniczone zastosowanie do rozważanego problemu, dotyczy bowiem niezagrażania człowiekowi przez urządzenie, w tym przypadku przez urządzenia wchodzące w skład instalacji sieciowej.

Zasadniczą sprawa jest, aby instalacja sieciowa była wystarczająco niezawodna, innymi słowy by miała wystarczająco wysoki poziom nienaruszalności bezpieczeństwa [2,5]. Jak wysoki to ma być poziom, to zależy od sterowanego obiektu.

Ze względu na skomplikowanie sprzętowe i programowe instalacji sieciowej, podstawowym odniesieniem do dalszych rozważań będzie bezpieczeństwo funkcjonalne.

2. ANALIZA ZAGROŻEŃ I RYZYKA.

Przy analizie zagrożeń i ryzyka ważne są następujące pojęcia:
- Zagrożenie (hazard) - możliwość doznania urazu lub nadwyrężenia zdrowia [5].
- Ryzyko (risk) - kombinacja prawdopodobieństwa wystąpienia i stopnia możliwego urazu lub nadwyrężenia zdrowia w sytuacji zagrożenia [5].

Podstawowa metodyka bazująca na grafie ryzyka jest podana w [8] i przedstawiona w [2]

W [10] rozpatruje się rozwinięcie tej metodyki przez wprowadzenie grafu kalibrowanego (opatrzonego liczbowym wyrażeniem prawdopodobieństwa wystąpienia zagrożenia) oraz uwzględnienia zagrożenia środowiska i istotnych strat ekonomicznych.

Analizę zagrożeń i ryzyka, w przypadku instalacji sieciowej, należy przeprowadzić w dwu aspektach:

- poziomu nienaruszalności bezpieczeństwa wymaganego przez obiekt;
- poziomu nienaruszalności bezpieczeństwa oferowanego przez sieć komputerową.

Przeprowadzona w [10] analiza prostego przypadku procesu produkcyjnego wskazuje, że przy dostatecznie wysokich, ale całkowicie uzasadnionych wymaganiach dotyczących bezpieczeństwa pracy obiektu, niedostatecznym zabezpieczeniem może być nie tylko normalny układ sterowania z funkcjami bezpieczeństwa, lecz także podwojenie tego układu w strukturze hierarchicznej. Konieczne jest wprowadzenie nowej jakości w postaci układu o poziomie nienaruszalności bezpieczeństwa SIL> 1.

3. WYMAGANIA DOTYCZĄCE SPRZĘTU [6]

3.1. Poziom nienaruszalności bezpieczeństwa

W kontekście nienaruszalności bezpieczeństwa sprzętu, najwyższy poziom nienaruszalności, jaki może być osiągnięty w odniesieniu do funkcji bezpieczeństwa, jest ograniczony przez odporność sprzętu na uszkodzenia i wyrażaną w procentach podatność na uszkodzenia podsystemów realizujących funkcje wiążące się z bezpieczeństwem. Ten najwyższy osiągalny poziom nienaruszalności bezpieczeństwa, wynikający z właściwości sprzętu, został przedstawiony w tablicach 1 i 2 w odniesieniu do podsystemów typu a i B.

Podsystem jest typu A, jeżeli w odniesieniu do realizowanych funkcji bezpieczeństwa wykazuje następujące właściwości:

- sposoby uszkodzeń wszystkich części składowych decydujących o realizacji funkcji bezpieczeństwa są dobrze określone;
- zachowanie się podsystemu w warunkach uszkodzenia jest całkowicie zdeterminowane;
- jest dostatecznie dużo danych z doświadczeń na obiektach aby wykazać, że jest zachowana wymagana relacja między wykrywanymi i niewykrywanymi niebezpiecznymi uszkodzeniami.

Podsystem jest typu B jeżeli w odniesieniu do realizowanych funkcji bezpieczeństwa wykazuje następujące właściwości:

- sposób powstania uszkodzenia co najmniej jednej części składowej decydującej o realizacji funkcji bezpieczeństwa nie jest dobrze określony;
- zachowanie się podsystemu w warunkach uszkodzenia nie może być całkowicie zdeterminowane;
- nie ma dostatecznie dużo danych z doświadczeń na obiektach aby wykazać, że jest zachowana wymagana relacja między wykrywanymi i niewykrywanymi niebezpiecznymi uszkodzeniami.

W tablicach przyjęto, że odporność sprzętu na uszkodzenia na poziomie N oznacza, iż N+1 uszkodzenie może spowodować utratę realizacji funkcji bezpieczeństwa.

Tablica 1 - Nienaruszalność bezpieczeństwa sprzętu : ograniczenia wynikające z architektury w przypadku podsystemów typu A

Podatność na uszkodzenia	Odporność sprzętu na uszkodzenia		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60% do < 90 %	SIL 2	SIL 3	SIL 4
90 % do < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

UWAGA - SIL oznacza poziom nienaruszalności bezpieczeństwa wg [5].

Tablica 2 - Nienaruszalność bezpieczeństwa sprzętu : ograniczenia wynikające z architektury w przypadku podsystemów typu B

Podatność na uszkodzenia	Odporność sprzętu na uszkodzenia		
	0	1	2
< 60 %	nie dopuszczalne	SIL 1	SIL 2
60% do < 90 %	SIL 1	SIL 2	SIL 3
90 % do < 99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

3.2. Unikanie błędów systematycznych

Niezależnie od błędów przypadkowych sprzętu, na osiągany poziom nienaruszalności bezpieczeństwa istotny wpływ ma zapobieganie powstawaniu błędów systematycznych. W tej mierze norma [6] podaje liczne zalecenia odnoszące się do wszystkich faz cyklu trwałości [2,5]; przykładowo w tablicy 3 przytoczono zalecenia dotyczące fazy specyfikowania wymagań bezpieczeństwa.

Przy formułowaniu wymagań wprowadzono następujące oznaczenia:

- HR : technika jest wysoce zalecana w odniesieniu do tego poziomu nienaruszalności bezpieczeństwa. Jeśli ta technika nie została użyta, to należy przedstawić dokładne uzasadnienie tej decyzji;
- R : technika jest zalecana w odniesieniu do tego poziomu nienaruszalności bezpieczeństwa. Wymaga się użycia co najmniej jednej techniki z wymienionych w grupie, zaznaczonej na szaro:
- - : nie ma zaleceń ani przeciwwskazań do zastosowania tej techniki;
- NR : technika jest całkowicie niezalecana w odniesieniu do tego poziomu nienaruszalności bezpieczeństwa. Jeżeli zostanie użyta, to należy przedstawić dokładne uzasadnienie tej decyzji;
- Obowiązkowa : użycie tej techniki jest wymagane odnośnie wszystkich poziomów nienaruszalności bezpieczeństwa i powinna ona być użyta tak dalece jak to możliwe (to jest zapewnić wysoką skuteczność);
- Niska : technika, jeżeli jest użyta, to powinna zostać zastosowana w stopniu koniecznym do uzyskania niewielkiej skuteczności w zapobieganiu błędom systematycznym;

- Średnia : technika, jeżeli jest użyta, to powinna zostać zastosowana w stopniu koniecznym do uzyskania średniej skuteczności w zapobieganiu błędom systematycznym;
- Wysoka : technika powinna zostać zastosowana w stopniu koniecznym do uzyskania wysokiej skuteczności w zapobieganiu błędom systematycznym;

Jeśli stosowanie techniki nie jest obowiązkowe, to, w zasadzie, może ona być zastąpiona inną techniką lub pomiarem (indywidualnie lub w kombinacji); jest to wskazane szarym polem i uwagami w odpowiednich tablicach.

4. WYMAGANIA DOTYCZĄCE OPROGRAMOWANIA [7]

4.1. System zarządzania jakością oprogramowania

Przy planowaniu funkcjonalnym oprogramowania należy zdefiniować strategię pozyskiwania, rozwoju, integracji, weryfikacji, walidacji i modyfikacji oprogramowana, w takim zakresie jak jest to wymagane ze względu na poziom nienaruszalności bezpieczeństwa systemów E/E/PE wiążących się z bezpieczeństwem.

Zarządzanie konfiguracją oprogramowania powinno zapewnić:

a) administracyjne i techniczne sterowanie, w ciągu całego cyklu trwałości oprogramowania, w celu zarządzania zmianami oprogramowania i które zapewni, że będą spełniane przyjęte wymagania dotyczące utrzymania bezpieczeństwa oprogramowania;
b) pewność, że wykonano wszystkie konieczne czynności do wykazania, że został osiągnięty wymagany poziom nienaruszalności bezpieczeństwa oprogramowania;
c) utrzymanie dokładne i z jednoznaczną identyfikacją wszystkich elementów konfiguracji koniecznych do utrzymania poziomu nienaruszalności bezpieczeństwa systemu E/E/PE, wiążącego się z bezpieczeństwem; te elementy konfiguracji obejmują co najmniej: analizę i wymagania bezpieczeństwa, specyfikację oprogramowania i dokumentację jego projektowania, moduły kodu źródłowego, plany i wyniki testowania , istniejące poprzednio składniki i zbiory oprogramowania wprowadzone do projektowanego systemu , wszystkie narzędzia i środowiska projektowe użyte do tworzenia i badania lub wykonywania jakichkolwiek czynności dotyczących oprogramowania systemu;
d) stosowanie procedur wprowadzania zmian, w celu: zapobiegania nieautoryzowanym modyfikacjom; zapewnienia dokumentowania zmian, oceny wpływu proponowanych modyfikacji i ich aprobaty lub odrzucenia; ustalania modułów bazowych konfiguracji w odpowiednich miejscach opracowywania oprogramowania i dokumentowania częściowego badania integracji, potwierdzającego zrealizowanie tych modułów; zagwarantowanie, że wykorzystano wszystkie moduły bazowe oprogramowania;
e) dokumentowanie następujących informacji w celu umożliwienia następnie przeprowadzenia auditu: status konfiguracji, status wydania, uzasadnienie i zatwierdzenie wszystkich modyfikacji i szczegóły dotyczące modyfikacji;
f) formalne udokumentowanie wydania oprogramowania wiążącego się z bezpieczeństwem - kopie wzorcowe oprogramowania i wszystkich dokumentów towarzyszących powinny być zachowane, aby umożliwić utrzymanie i modyfikowanie w ciągu całego czasu użytkowania wydanego oprogramowania.

4.2. Zarządzanie cyklem trwałości bezpieczeństwa

a) cykl trwałości bezpieczeństwa oprogramowania powinien być zaprojektowany w trakcie planowania bezpieczeństwa wg wymagań IEC 61508-1[2,6];

b) procedury zapewnienia jakości i bezpieczeństwa należy zintegrować z czynnościami wynikającymi z cyklu trwałości bezpieczeństwa;
c) każda faza cyklu trwałości bezpieczeństwa oprogramowania powinna zostać podzielona na czynności elementarne o przedmiocie, wejściach i wyjściach wynikających z danej fazy cyklu;
d) do realizacji każdej fazy cyklu trwałości należy zastosować odpowiednie techniki i miary;
e) wyniki wszystkich czynności realizowanych w ramach cyklu trwałości bezpieczeństwa należy dokumentować;
f) jeśli przy realizacji jakiejkolwiek fazy cyklu trwałości bezpieczeństwa okaże się konieczną zmiana dotycząca wcześniejszej fazy cyklu trwałości, to należy powtórzyć wykonanie tej poprzedniej fazy i wszystkich faz po niej następujących.

Tablica 3 - Zalecenia dotyczące unikania błędów podczas specyfikowania wymagań bezpieczeństwa

Technika/pomiar	Patrz IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
Zarządzanie projektem	B.1.1	HR niska	HR niska	HR średnia	HR wysoka
Dokumentacja	B.1.2	HR niska	HR niska	HR średnia	HR wysoka
Oddzielanie układów E/E/PE wiążących się z bezpieczeństwem od układów nie wiążących się z bezpieczeństwem	B.1.3	HR niska	HR niska	HR średnia	HR wysoka
Specyfikacja usystematyzowana	B.2.1	HR niska	HR niska	HR średnia	HR wysoka
Przegląd specyfikacji	B.2.6	- niska	HR niska	HR średnia	HR wysoka
Metody semi-formalne	B.2.3 oraz tabl. B.7 z IEC 61508-3	R niska	R niska	HR średnia	HR wysoka
Lista kontrolna	B.2.5	R niska	R niska	R średnia	R wysoka
Narzędzia wspomagane komputerowo	B.2.4	- niska	R niska	R średnia	R wysoka
Metody formalne	B.2.2	- niska	- niska	R średnia	R wysoka

UWAGI : 1. Techniki oznaczone przez R w grupie zaznaczonej na szaro są wzajemnie zamienne, lecz co najmniej jedna powinna być użyta.

2. Przy weryfikacji tej fazy cyklu trwałości powinna być zastosowana co najmniej jedna technika wymieniona w grupie zaznaczonej na szaro.

3. E/E/PE oznacza: elektryczne/elektroniczne/programowalne elektroniczne.

4.3. Wymagania dotyczące specyfikacji wymagań bezpieczeństwa

a) specyfikacja wymagań dotyczących bezpieczeństwa oprogramowania powinna wynikać z wymagań bezpieczeństwa systemu E/E/PE wiążącego się z bezpieczeństwem i z wymagań dotyczących zarządzania cyklem bezpieczeństwa (p.4.2); te informacje należy udostępnić opracowującemu oprogramowanie;
b) Specyfikacja wymagań bezpieczeństwa powinna być wystarczająco szczegółowa, aby pozwolić na zaprojektowanie oprogramowania i jego implementację umożliwiające osiągnięcie wymaganego poziomu nienaruszalności bezpieczeństwa oraz przeprowadzenie oceny bezpieczeństwa funkcjonalnego;
c) opracowujący oprogramowanie powinien przeprowadzić przegląd danych wynikających z powyżej podanych czynności, aby się upewnić, że wymagania są należycie sformułowane; w szczególności powinien on rozważyć następujące sprawy:
   - funkcje bezpieczeństwa;
   - konfigurację lub architekturę systemu;
   - wymagania dotyczące nienaruszalności bezpieczeństwa sprzętu (elektroniczne urządzenia programowalne, czujniki i elementy wykonawcze);
   - wymagania dotyczące nienaruszalności bezpieczeństwa oprogramowania;
   - właściwości odnoszące się do zakresu i czasu odpowiedzi;
   - wyposażenie i interfejs operatora;
d) opracowujący oprogramowanie powinien ustalić procedury do rozwiązywania jakichkolwiek różnic dotyczących wyznaczenia poziomu nienaruszalności bezpieczeństwa oprogramowania;
e) wymagania odnoszące się do bezpieczeństwa oprogramowania powinny być tak wyrażone i sformułowane, aby były:
   - jasne, precyzyjne, jednoznaczne, weryfikowalne, testowalne, utrzymywalne i wykonalne, proporcjonalnie do poziomu nienaruszalności bezpieczeństwa;
   - dające się odnieść wstecz do specyfikacji wymagań bezpieczeństwa systemu E/E/PE wiążącego się z bezpieczeństwem;
   - wolne od terminologii i opisów wieloznacznych i/lub niezrozumiałych dla tego, kto będzie użytkował ten dokument w dowolnym miejscu cyklu trwałości bezpieczeństwa oprogramowania;
f) specyfikacja wymagań bezpieczeństwa oprogramowania powinna wymieniać i dokumentować jakiekolwiek więzy między sprzętem i oprogramowaniem, wiążące się z bezpieczeństwem lub z jego dotyczące;
g) ze względu na zasięg wymagany przez opis systemu E/E/PE, specyfikacja wymagań bezpieczeństwa oprogramowania powinna rozpatrywać następujące zagadnienia:
   - samo nadzorowanie oprogramowania;
   - monitorowanie elektronicznego sprzętu programowalnego, czujników i elementów wykonawczych;
   - okresowe testowanie funkcji bezpieczeństwa w czasie pracy systemu;
   - umożliwienie testowania funkcji bezpieczeństwa w czasie pracy systemu;
h) jeśli system E/E/PE wiążący się z bezpieczeństwem ma wykonywać funkcje inne niż funkcje bezpieczeństwa, to wymagania dotyczące bezpieczeństwa oprogramowania powinny wyraźnie identyfikować te funkcje;
i) specyfikacja bezpieczeństwa oprogramowania ma wyrażać wymagane właściwości bezpieczeństwa **produktu**, a nie projektu; w związku z tym powinny być wyspecyfikowane właściwości, jak podano w p. j,k, o ile mają zastosowanie;
j) funkcje bezpieczeństwa oprogramowania:

- funkcje umożliwiające osiągnięcie lub utrzymanie stanu bezpiecznego przez obiekt sterowany;
- funkcje dotyczące wykrywania, sygnalizowania i zarządzania uszkodzeniami w elektronicznym sprzęcie programowalnym
- funkcje dotyczące wykrywania, sygnalizowania i zarządzania uszkodzeniami czujników i elementów wykonawczych;
- funkcje dotyczące wykrywania, sygnalizowania i zarządzania uszkodzeniami w samym oprogramowaniu (samo monitorowanie oprogramowania);
- funkcje dotyczące okresowego testowania on-line funkcji bezpieczeństwa;
- funkcje dotyczące okresowego testowania off-line funkcji bezpieczeństwa;
- funkcje umożliwiające bezpieczne modyfikowanie elektronicznego systemu programowalnego;
- interfejsy do funkcji nie wiążących się z bezpieczeństwem;
- właściwości odnoszące się do zakresu i czasu odpowiedzi;
- interfejsy między oprogramowaniem i elektronicznym systemem programowalnym (te interfejsy obejmują narzędzia programowe pracujące tak on-line jak i off-line).

k) poziom nienaruszalności bezpieczeństwa każdej z funkcji wymienionych w j).

Spełnienie wymagań podlega walidacji. Metody walidacji przez badanie implementacji omówiono w [4].

LITERATURA

1. Meyer-Gräfe K. : *Interbus Safety.* AMD&C Automation - Motion, Drives & Control, 1999 r.,z. 12, ss. 34-36
2. Missala T.: *Bezpieczeństwo funkcjonalne urządzeń automatyki i robotyki.* Pomiary Automatyka Robot\yka, 1997 r., z. 3.,ss 5-8 oraz Materiały Konferencji Automation'97, t. 1, ss 113-126, PIAP, 1997 r.
3. Missala T.: *Bezpieczeństwo funkcjonalne w procesie projektowania urządzeń mechatroniki.* Materiały III Konferencji Naukowo-Technicznej MECHATRONIKA'97. Warszawa 20-22 listopada 1997 r. Politechnika Warszawska. Prace Naukowe. Konferencje. z. 14, ss. 541-546.
4. Missala T.: *Ocena a priori i a posteriori bezpieczeństwa robota.* Prace Naukowe Instytutu Cybernetyki Stosowanej Politechniki Wrocławskiej, Nr 99. Prace VI Krajowej Konferencji Robotyki , t. 2. s.133-148, Wrocław wrzesień 1998 r.
5. IEC 1508-1: 1999. - *Functional safety: safety related systems - Part 1: General requirements.*
6 IEC 1508-2: 2000. - *Functional safety: safety related systems - Part 2: Requirements for electrical/electronic/ programmable electronic systems.*
7. IEC 1508-3: 1999. - *Functional safety: safety related systems - Part 3: Software requirements.*
8. IEC 1508-5: 1999 - *Functional safety: safety related systems - Part 5: Guidelines on the application of Part 1.*
9. EN 954-1: 1996 - *Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (Wersja polska prPN-EN 954-1 - Maszyny - Bezpieczeństwo - Elementy systemu sterowania związane z bezpieczeństwem - Ogólne zasady projektowania).*
10. IEC 61511-3 (draft - 65A/291/CD) - *Functional safety instrumented systems for the process industry sector. Part 3: Guidelines on the application of hazard and risk analysis.*