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

JAKOŚĆ A BEZPIECZEŃSTWO – RELACJE WZAJEMNE

Wprowadzona w nowej PN-EN ISO 9000:2000 (idt. ISO 9000: 2000) definicja jakości wymaga bardziej wnikliwego spojrzenia na to pojęcie, niż wynikało to z definicji podanej w PN ISO 8402: 1996. Przedstawiono propozycję nowego podejścia do zagadnienia jakości; w szczególności przeanalizowano bezpieczeństwo jako składową jakości i wskazano, że aktualne przepisy normatywne i techniczne stawiają bezpieczeństwo na pozycji uprzywilejowanej w tym względzie.

QUALITY VERSUS SAFETY - INTERRELATIONS

The definition of quality introduced in a new ISO 9000 :2000 needs a more detailed look on this idea then such a look resulting from the old definition done in ISO 8402: 1994. The proposal of a new approach to the problem of quality; the particular attention is paid on the problems of safety as a component of the quality. It is indicated, the actual normative and technical regulations place the safety on the privileged position.

1. WSTĘP

W PN-EN ISO 9000: 2001 (idt. ISO 9000: 2000) podano następujące definicje:
Jakość – stopień, w jakim zbiór inherentnych właściwości spełnia wymagania:

- "inherentny" jako przeciwny do "przypisany", oznacza istniejący sam w sobie, szczególnie jako stała właściwość.

Właściwość – cecha wyróżniająca:

- Właściwość może być inherentna lub przypisana;
- Właściwość może być jakościowa lub ilościowa;
- Są różne klasy właściwości, takie jak: fizyczne (mechaniczne, elektryczne, chemiczne lub biologiczne), dotyczące zmysłów (odnoszące się do zapachu, dotyku, smaku, wzroku, słuchu), behawioralne (np. uprzejmość, uczciwość, prawdomówność), czasowe (np. punktualność, niezawodność, dostępność), ergonomiczne (np. właściwości fizjologiczne lub odnoszące się do bezpieczeństwa człowieka), funkcjonalne.

Wymaganie – potrzeba lub oczekiwanie, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe;

- "Przyjęte zwyczajowo" oznacza, że istnieje zwyczaj lub powszechna praktyka organizacji, jej klientów i innych stron zainteresowanych, że rozpatrywana potrzeba lub oczekiwanie jest przyjęte.

Jeżeli porównać je z definicją występującą w poprzedniej, dziś unieważnionej PN ISO 8402: 1996:

Jakość – ogół właściwości obiektu wiążących się z jego zdolnością do zaspokojenia potrzeb stwierdzonych i oczekiwanych,

to widać wyraźnie, że nowa definicja ma bardziej adresowany kontekst.

Współczesne urządzenia techniczne są coraz bardziej skomplikowane, a świadczone usługi są coraz trudniejsze do skontrolowania przez klienta. Powstała więc konieczność odwołania się, przy formułowaniu pojęcia jakości, do zbioru wymagań, w tym do wymagań formalnych, a zwłaszcza obowiązkowych.

W szczególności dotyczy to sektora pomiarów, automatyki i robotyki; urządzenia i systemy tego sektora sterują rozmaitymi instalacjami technologicznymi stwarzającymi niejednokrotnie, w przypadku powstania awarii, poważne zagrożenia dla personelu, jak też narażające środowisko naturalne i sam proces sterowany oraz finanse firmy. Wnikliwa analiza pojęcia jakości produkcji i usług jest tu więc na miejscu.

Wśród wymagań formułowanych w odniesieniu do urządzeń i systemów szczególną pozycję zajmuje bezpieczeństwo. Człowiek ma prawo do życia w bezpiecznym otoczeniu, używać bezpiecznych urządzeń i korzystać z możliwie czystego środowiska naturalnego – to przeświadczenie stało się dewizą działań w ostatnich dziesięcioleciach.

A co to jest urządzenie bezpieczne ? To takie urządzenie, które:

- nie wprowadza zagrożeń, gdy pracuje normalnie,
- gdy się uszkodzi to nie spowoduje zagrożenia ani dla ludzi ani w środowisku;
- gdy zostanie niewłaściwie użyte to też nie spowoduje zagrożenia.

Systemy sterowania mają istotne znaczenie z punktu widzenia zapewnienia bezpieczeństwa; są stosowane m.in. do:

- zapobiegania powstawaniu zagrożeń, np. przez wprowadzanie blokad uniemożliwiających niebezpieczne sekwencje zdarzeń;
- ograniczania prawdopodobnej ostrości urazów, szkód zdrowia, szkód w środowisku, szkód w procesie związanych z sytuacją zagrażającą, np. ograniczanie prędkości, włączanie wentylacji awaryjnej, ograniczanie ciśnienia, włączanie alarmów ostrzegawczych lub nakazujących ewakuację;
- zapobieganie narażania na zagrożenie, np. przez blokowanie wejścia osób nieuprawnionych do stref niebezpiecznych;
- wprowadzanie dodatkowych środków ochronnych, np. zatrzymanie awaryjne połączone z procedurą zatrzymania bezpiecznego;
- redukowanie ryzyka w warunkach uszkodzeń, np. automatyczne monitorowanie, ochrona przeciążeniowa.

Systemy automatyki same przeto powinny być bezpieczne.

2. ELEMENTY SKŁADOWE POJĘCIA JAKOŚCI - WPROWADZENIE

Za składowe pojęcia jakości można uznać te właściwości analizowanego obiektu (urządzenia, systemu, organizacji itp.), którym sformułowano wymagania, bądź bezpośrednio, bądź też przez określenie misji. Można przyjąć pogrupowanie właściwości np. takie jak podano w [3]:

- funkcjonalne;
- niezawodnościowe;
- określające osiągi (parametry) urządzenia;
- wiążące się z obsługą przez człowieka;
- wiążące się z bezpieczeństwem.

Powiązanie wymienionych grup właściwości, charakteryzujących jakość z bezpieczeństwem jest przedmiotem obecnych rozważań.

3. WŁAŚCIWOŚCI FUNKCJONALNE

Podstawowym warunkiem należytej jakości obiektu jest zrealizowanie przewidzianej dlań funkcjonalności. Prawidłowe wykonywanie wszystkich wymaganych funkcji nie tylko jest elementem jakości obiektu, lecz także elementem jego bezpiecznej pracy – obiekt, który nie w pełni realizuje wymagane funkcje jest *obiektem niebezpiecznym*.

Funkcjonalność daje się przedstawić jako wynik trzech cech składowych [4]:

- pokrycia;
- konfigurowalności;
- elastyczności.

Obiekt jest zdolny do wykonania wymaganych zadań, jeżeli funkcje przezeń zapewniane umożliwiają realizację tych zadań. Zakres w jakim to ma miejsce jest "pokryciem". W szczególności, gdy jednym z zadań obiektu jest redukcja ryzyka [2], to obiekt nazywa się "wiążącym się z bezpieczeństwem", a funkcje ograniczające ryzyko – "funkcjami wiążącymi się z bezpieczeństwem".

Przykładami funkcji wiążących się z bezpieczeństwem są:

- uruchomienie procesu z zachowaniem należytych środków bezpieczeństwa;
- wyłączenie procesu z zachowaniem należytych środków bezpieczeństwa;
- wyłączenie awaryjne połączone z procedurą bezpiecznego zatrzymania;
- uniemożliwienie nieoczekiwanego uruchomienia;
- funkcje uruchamiania, zatrzymywania i rewersu napędów;
- funkcje sterowania ruchem;
- funkcje ochrony człowieka.

Do funkcji wiążących się z bezpieczeństwem definiuje się pojęcie nienaruszalności bezpieczeństwa. Jest to prawdopodobieństwo, że obiekt wiążący się z bezpieczeństwem

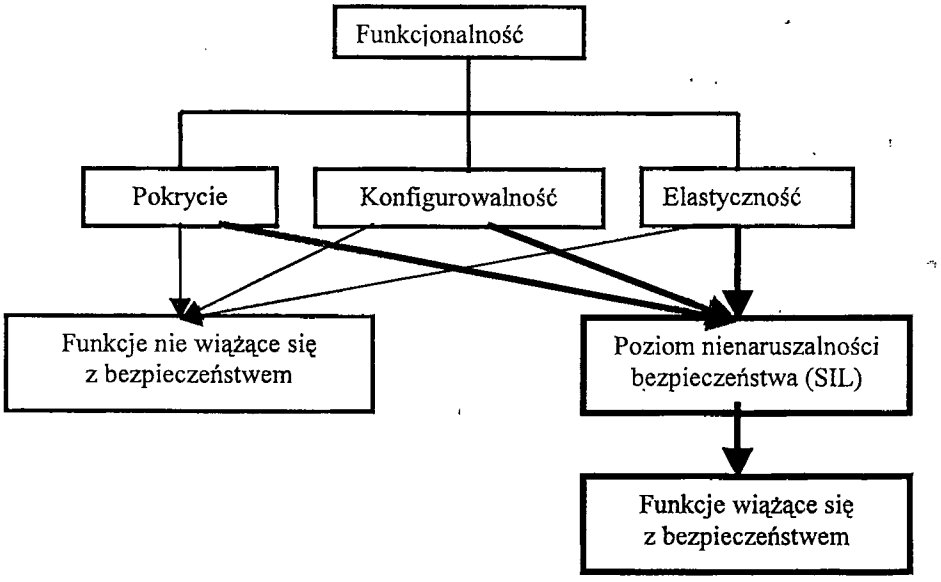
będzie wypełniał prawidłowo wymagane funkcje bezpieczeństwa, we wszystkich ustalonych warunkach i w ustalonym okresie czasu [9].

Nienaruszalność bezpieczeństwa wymagana w odniesieniu do obiektów wiążących się z bezpieczeństwem i zewnętrznych urządzeń do redukcji ryzyka musi mieć taki poziom, aby zapewnić że:

- częstość uszkodzeń systemów wiążących się z bezpieczeństwem jest wystarczająco niska, aby zapobiec przekroczeniu przez prawdopodobieństwo wystąpienia zdarzeń zagrażających wartości wymaganej do uzyskania ryzyka tolerowalnego. i/lub
- systemy wiążące się z bezpieczeństwem ograniczają konsekwencje uszkodzenia do rozmiarów wymaganych do uzyskania ryzyka tolerowalnego.

Możliwości realizowania funkcji wymaganych aktualnie i takich, których potrzeba może się pojawić, zależą nie tylko od istniejącego lecz także od potencjalnego pokrycia; to ostatnie zaś jest funkcją możliwości zmiany konfiguracji obiektu i jego adaptacji do wykonywania nowych lub rozszerzonych zadań. Te cechy, zwane konfigurowalnością i elastycznością obiektu, odnoszą się również do funkcji wiążących się z bezpieczeństwem.

Wzajemne relacje zilustrowano na rysunku 1.



Rysunek 1 – Relacje funkcjonalności i funkcji wiążących się z bezpieczeństwem

4. WŁAŚCIWOŚCI NIEZAWODNOŚCIOWE

Obiekt jest niezawodny wówczas gdy [6]:

- jest w każdej chwili gotowy do wypełniania swoich funkcji;
- swoje funkcje wykonuje poprawnie, niezależnie od wpływu otoczenia (innych obiektów, środowiska, człowieka).

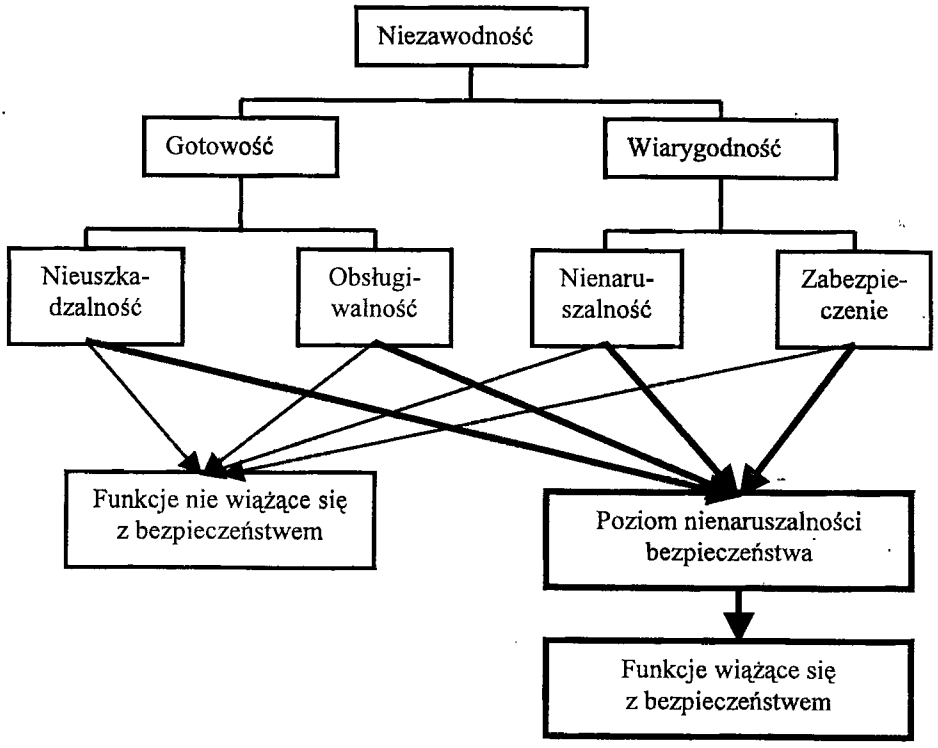
Gotowość do wypełniania swoich funkcji zależy od nieuszkadzalności obiektu oraz od czasu koniecznego do jego naprawy (zwanego obsługiwalnością). Poprawność wykonania funkcji, to jest wiarygodność obiektu, zależy od jego nienaruszalności i zabezpieczenia.

Przyjęto tutaj definicje:

- niezawodność – zakres w jakim można polegać, że obiekt wykona jedynie i prawidłowo zadanie w danych warunkach, w danej chwili lub w danym przedziale czasu, przy założeniu, że są dostarczone wymagane środki zewnętrzne (np. zasilania);
- nieuszkadzalność – zdolność obiektu do wypełnienia wymaganych funkcji w danych warunkach i w dany przedziale czasu;
- obsługiwalność – zdolność obiektu do utrzymywania lub odtwarzania w dant\ych warunkach eksploatacji stanu, w którym może on wypełniać wymagane funkcje przy założeniu, że obsługa jest przeprowadzana w ustalonych warunkach z zachowaniem ustalonych procedur i środków;
- gotowość – zdolność obiektu do utrzymywania się w stanie umożliwiającym wypełnianie wymaganych funkcji w danych warunkach, w danej chwili lub danym przedziale czasu, przy założeniu, że są dostarczane wymagane środki zewnętrzne;
- nienaruszalność – pewność dostarczana przez obiekt, że zadanie będzie wykonane prawidłowo;
- zabezpieczenie – pewność dostarczana przez obiekt, że każde niepoprawne wejście lub każdy nieuprawniony dostęp są zabronione;
- wiarygodność – zakres w jakim obiekt jest zdolny do rozpoznania i zasygnalizowania stanu systemu i w jakim wytrzymuje niepoprawne wejścia i nieuprawniony dostęp.

Powyżej podane cechy niezawodności obiektu dotyczą nie tylko realizacji podstawowych funkcji, lecz także funkcji wiążących się z bezpieczeństwem. W tym ostatnim przypadku wymagania są wyrażone przez "poziom nienaruszalności bezpieczeństwa" i są one szczególnie wysokie [1, 9]. Wzajemne relacje zilustrowano na rysunku 2.

O poziomie nienaruszalności bezpieczeństwa funkcji wiążących się z bezpieczeństwem decydują wszystkie cechy składowe niezawodności.



Rysunek 2 – Relacje niezawodności i bezpieczeństwa

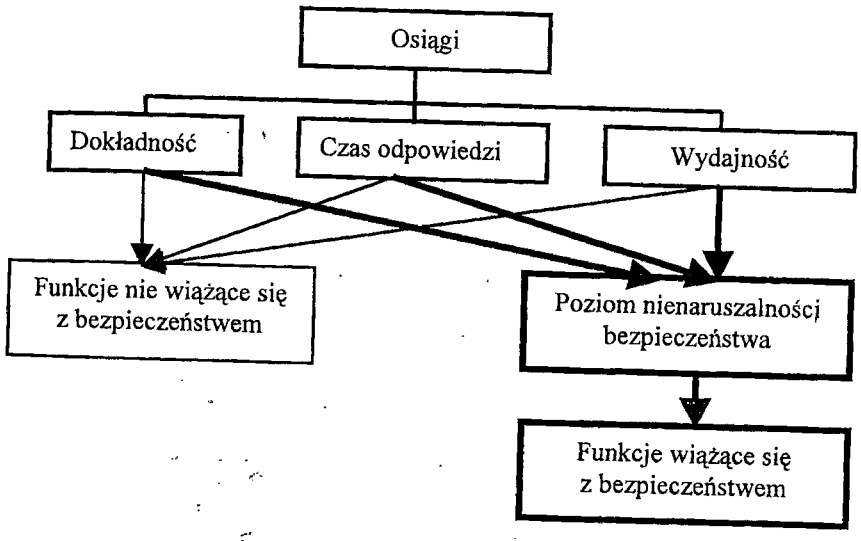
5. OSIĄGI OBIEKTU

Jako osiągi obiektu przyjęto wg [5]:

- dokładność to jest stopień zgodności między wyspecyfikowanym przetwarzaniem informacji i realizowanym przez system w określonych warunkach;
- czas odpowiedzi to jest okres czasu między zainicjowaniem przetwarzania informacji a chwilą, gdy wynikająca z tego odpowiedź stanie się dostępna w określonych warunkach;
- wydajność to jest największa liczba przetworzeń informacji, którą obiekt jest zdolny wykonać w określonym okresie czasu, bez wpływania na jakąkolwiek swoją właściwość.
- Przetwarzanie informacji jest to zmiana lub przeniesienie informacji wchodzącej do obiektu na jego granicy na informację wyjściową z obiektu na jego granicy.

Obiekt może być uznany za właściwej jakości, gdy wykonuje wymagane odeń zadania dokładnie, pewnie i w czasie oraz liczbie podanych w jego specyfikacji technicznej.

Osiągi te nie tylko są istotnymi właściwościami wiążącymi się z możliwościami spełnienia wymagań aplikacyjnych, a więc z jakością, lecz także wszelkie niedokładności w realizacji zadań mogą prowadzić np. do awarii procesu sterowanego, a więc mają wpływ na bezpieczną pracę obiektu, a w przypadku gdy realizuje on funkcje wiążące się z bezpieczeństwem, będą wpływać bezpośrednio na niezawodność realizacji tych funkcji, a więc na poziom nienaruszalności bezpieczeństwa (SIL).
Powiązania te przedstawiono na rysunku 3.



Rysunek 3 – Relacje osiągów i bezpieczeństwa

6. WSPÓŁDZIAŁANIE Z OPERATOREM

Jako cechy współdziałania obiektu z operatorem przyjęto [7]:

- Skuteczność, to jest zakres w jakim środki operatorskie, udostępniane przez obiekt, minimalizują czas i wysiłek operatora przy stosowaniu obiektu;
- Intuicyjność, to jest zakres w jakim środki operatorskie, udostępniane przez obiekt, są natychmiast rozumiane przez operatora;
- Transparentność, to jest zakres w jakim środki operatorskie, udostępniane przez obiekt, wirtualnie wprowadzają operatora w bezpośredni kontakt z wykonywanym zadaniem;
- Odporność, to jest zakres w jakim obiekt poprawnie interpretuje działania operatora i odpowiada na nie i pomija wszystkie niejednoznaczności.

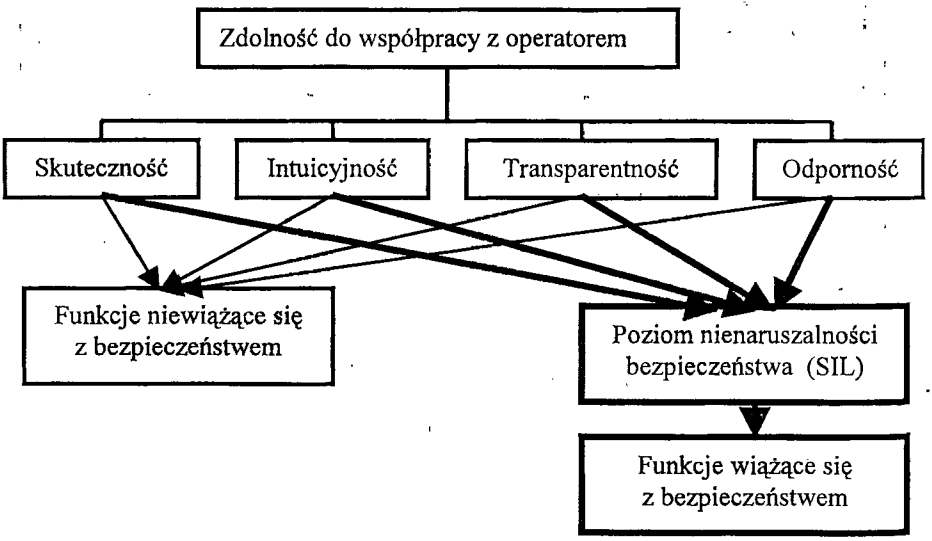
Obiekt jest skuteczny we współpracy z operatorem, jeżeli umożliwia operatorowi wykonanie jego zadania w akceptowalnym przedziale czasu, przy minimalnym prawdopodobieństwie popełnienia błędu.

Obiekt charakteryzuje się intuicyjnością we współpracy z operatorem, jeżeli udostępniane środki operatorskie nie są w sprzeczności z poziomem wykształcenia i ogólną kulturą przewidywanych operatorów.

Obiekt jest transparentny we współpracy z operatorem, jeżeli udostępniane środki operatorskie dają operatorowi rzeczywisty ogląd działań, które należy wykonać, aby zrealizować wymagane zadanie.

Obiekt uważa się za odporny we współpracy z operatorem, jeżeli poprawnie interpretuje i poprawnie odpowiada na każde jednoznaczne działanie operatora, a żada dodatkowych informacji wyjaśniających, gdy nie jest ono jednoznaczne.

Te cechy nie tylko są właściwościami niezbędnymi do spełnienia wymagań aplikacyjnych, a więc nierozerwalnie powiązanymi z jakością, lecz także istotnie wpływającymi na bezpieczeństwo procesu sterowanego i obsługującego go personelu, a w przypadku gdy obiekt realizuje funkcje wiążące się z bezpieczeństwem, będą wpływać bezpośrednio na niezawodność realizacji tych funkcji, a więc na poziom nienaruszalności bezpieczeństwa (SIL). Powiązania te przedstawiono na rysunku 4.



Rysunek 4 – Relacje zdolności do współpracy z operatorem i bezpieczeństwa

7. BEZPIECZEŃSTWO

Jedną z właściwości obiektu świadczących o jego jakości jest bezpieczeństwo.

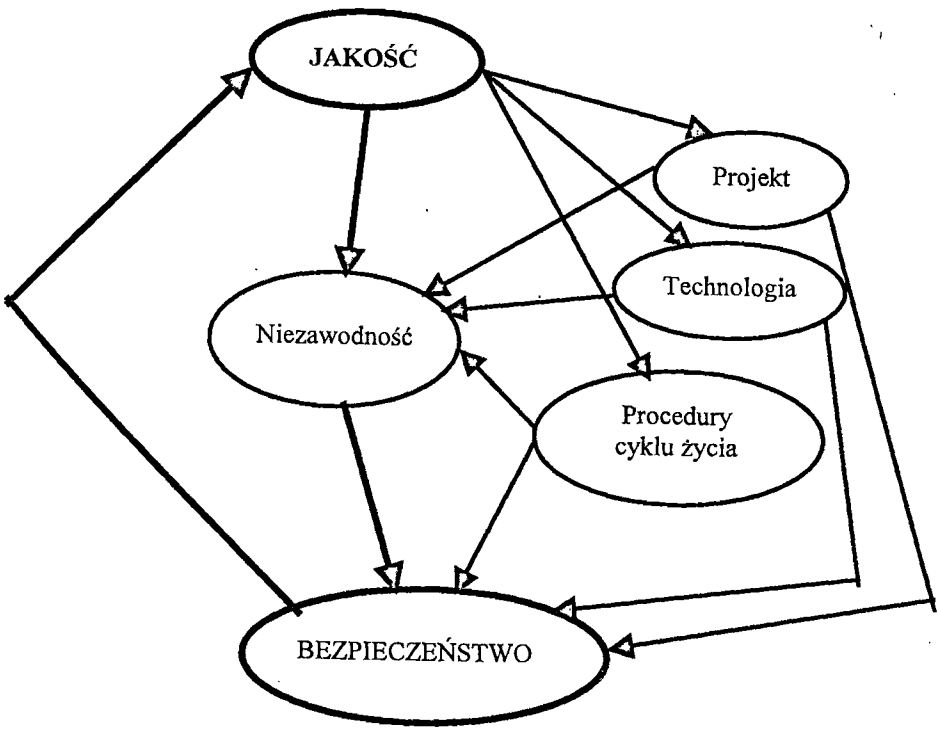
Obiekt jest bezpieczny, jeżeli sam, jako wyodrębniona całość fizyczna, nie wprowadza zagrożeń.

Tak pojęte bezpieczeństwo obiektu, rozpatrywane we wszystkich aspektach (elektrycznym, mechanicznym, chemicznym, cieplnym itd.) zależy od poprzednio przeanalizowanych jego właściwości, będących atrybutami jakości obiektu.

Ten zbiór właściwości można rozpatrzyć jako złożony z:

- Inherentnych właściwości projektu – tu można wskazać: pokrycie, konfigurowalność, elastyczność, osiągi, ogół właściwości związanych ze współpracą z operatorem, zastosowanie środków zwiększających niezawodność (np. redundancje, unikanie defektów wspólnej przyczyny, głosowanie 2 z 3), projektowe ograniczenie wpływu zewnętrznych czynników zakłócających pracę obiektu (np. ekranowanie, odpowiednie projektowanie płyt drukowanych, stosowanie odpowiednich obudów i złączy);
- Inherentnych właściwości technologii i wykonania, np. czystość, adekwatne procedury sprawdzania, zabezpieczanie przed działaniem czynników uszkadzających (np. elektryczności statycznej).
- Inherentnych właściwości realizacji cyklu życia obiektu: procedur użytkowania, obsługiwania i likwidacji, oznakowania bezpieczeństwa itd.

Te relacje przedstawiono na rysunku 5.



Rysunek 5 – Relacje jakości i bezpieczeństwa

8. PODSUMOWANIE

Przeanalizowano zbiór właściwości obiektu składających się na jego jakość, w świetle PN-EN ISO 9001:2001. Zwrócono uwagę na nierozerwalną zależność jakości obiektu i jego bezpieczeństwa i na dwukierunkowe sprzężenie zwrotne między tymi atrybutami obiektu.

LITERATURA

1. Missala T.: *Bezpieczeństwo funkcjonalne urządzeń automatyki i robotyki.* Pomiary Automatyka Robotyka, 1997 r., z. 3.,ss 5-8 oraz Materiały Konferencji Automation'97, t. 1, ss 113-126, PIAP, 1997 r.
2. Missala T.: *Ocena ryzyka w systemie zautomatyzowanym – propozycja postępowania.* Materiały Konferencji Automation'2001, ss. 299-308, PIAP, 2001 r..
3. PN-EN 61069-1:2001 – *Pomiary i sterowanie procesami przemysłowymi- Wyznaczanie właściwości systemu w celu jego oceny – Część 1: Postanowienia ogólne i metodologia.*
4. PN-EN 61069-3:2001 – *Pomiary i sterowanie procesami przemysłowymi- Wyznaczanie właściwości systemu w celu jego oceny – Część 3: Ocena funkcjonalności systemu.*
5. PN-EN 61069-4:2002 – *Pomiary i sterowanie procesami przemysłowymi- Wyznaczanie właściwości systemu w celu jego oceny – Część 4: Ocena parametrów systemu.*
6. PN-EN 61069-5:2002 – *Pomiary i sterowanie procesami przemysłowymi- Wyznaczanie właściwości systemu w celu jego oceny – Część 5: Ocena niezawodności systemu.*
7. PN-EN 61069-6:2002 (U) – *Pomiary i sterowanie procesami przemysłowymi- Wyznaczanie właściwości systemu w celu jego oceny – Część 6:Ocena współdziałania systemu z operatorem*
8. PN-EN 61069-7:2002 (U) – *Pomiary i sterowanie procesami przemysłowymi- Wyznaczanie właściwości systemu w celu jego oceny – Część 7: Ocena bezpieczeństwa systemu.*
9. PN-EN 61508-1:2002 (U). - *Functional safety: safety related systems - Part 1: General requirements (Bezpieczeństwo funkcjonalne - Systemy wiążące się z bezpieczeństwem - Wymagania ogólne);*