prof. dr inż. Tadeusz Missala
Przemysłowy Instytut Automatyki i Pomiarów, Warszawa

WALIDACJA ZŁOŻONYCH SYSTEMÓW AUTOMATYKI I ROBOTYKI

Walidacja systemu, to znaczy wykazanie, że system spełnia wymagania wynikające z warunków jego zastosowania jest istotnym krokiem przy dopuszczeniu systemu do eksploatacji. Przedstawiono metodykę oceny złożonego systemu zawartą w normach międzynarodowych oraz wymagania wynikające z problemów ergonomicznych, bezpieczeństwa i zabezpieczenia, w tym przed atakami terrorystycznymi.

VALIDATION OF COMPLEX AUTOMATIC AND ROBOTIC SYSTEMS

System validation, i.e. proof the system comply the requirements resulting of the conditions of its application, is the important step by the system commissioning. The evaluation methodology done in the International Standards is presented, as well as the requirements resulting from system ergonomic, safety and security, including protection against the terrorist attacks.

1. WPROWADZENIE

Walidacja jest zdefiniowana [2] następująco:

Walidacja – potwierdzenie, przez przedstawienie dowodu obiektywnego, że zostały spełnione wymagania dotyczące konkretnego zamierzonego użycia lub zastosowania.

W pracy [1] autor przedstawił zagadnienie walidacji urządzeń i systemów automatyki, jednakże stan wiedzy i opracowań zmienił się znacznie od tego czasu. Doszły zagadnienia wynikające z transmisji w informatycznych sieciach przemysłowych, zwiększyło się znaczenie zagadnień ergonomicznych, pojawiły się zagadnienia ataków na systemy sieciowe: hakerskich (dla sportu) i terrorystycznych. Ujawniły się problemy z awariami w sieciach rozległych, gdy utraci się odpowiedniość danych na krańcach sieci. W niniejszym referacie podjęto próbę przedstawienia tych zagadnień na tle ogólnej metodyki oceny systemów [5]. Ponadto zostały wprowadzone wymagania dotyczące badań akceptacyjnych [6, 7, 8], które też wymagają omówienia.

2. METODYKA OGÓLNA

Danymi referencyjnymi procesu walidacji są zadania, które ma wykonywać oceniany system. Zadania te, w ogólności są określone jako *misja systemu*.

W przypadku walidacji systemu obejmującego obiekt sterowania, urządzenia sterowania obiektem i ewentualnie systemy związane z bezpieczeństwem [6], wskazana jest metodyka oceny podana w PN-EN 61069 [5]. Zamieszczono tam następujące wymagania dotyczące planowania oceny:

2.1. Analiza misji systemu i zestawienie wymagań systemowych:

Działanie w tym zakresie obejmuje:

- określenie granic systemu;

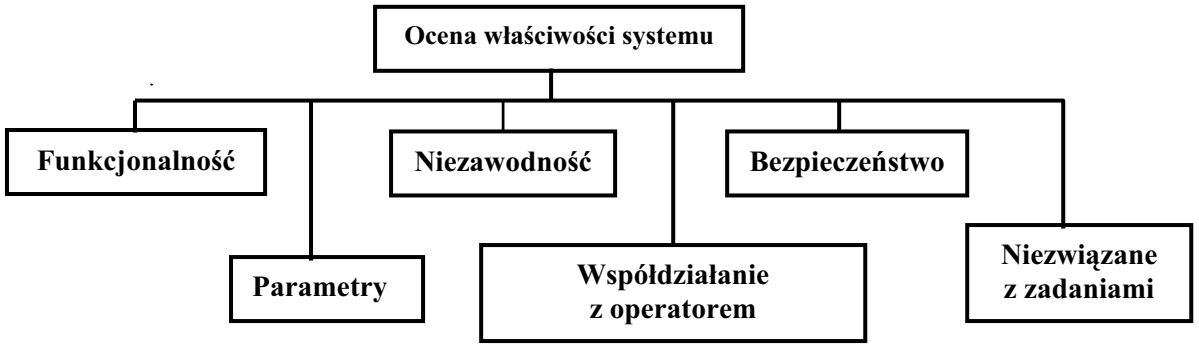
- zdefiniowanie misji systemu biorąc pod uwagę system wraz z całym jego kontekstem obejmującym personel, proces sterowany i/ lub zabezpieczany, wszystkie powiązane z nim systemy zewnętrzne oraz środowisko, w którym będzie pracować;
- zdefiniowanie misji przez opisanie jej faz: początkowa konfiguracja i przekazanie do eksploatacji; konfiguracja lub układ do konkretnego przebiegu produkcji, przejście z jednego przebiegu produkcji na inny, wyłączenie awaryjne lub przejście do bezpiecznego stanu postojowego, wyłączenie normalne, unowocześnienie i zmiany w systemie, wycofanie systemu z eksploatacji;
- przedstawienie misji przez zadania, które system wykonuje w poszczególnych fazach: monitorowanie i zobrazowanie wartości mierzonych, uaktywnianie określonej fazy procesu zgodnie z poleceniami wprowadzanymi ręcznie lub automatycznie, automatyczne sterowanie procesem, sterowanie uzależnieniami między zmiennymi procesu itp.;
- przypisanie zadaniom względnej ważności;
- określenie czynników wpływających;
- zidentyfikowanie dokumentu zawierającego wymagania systemowe;
- zidentyfikowanie specyfikacji systemu

2.2. Sprawy szczegółowe:

- ustalenie ważności poszczególnych zadań i wielkości wpływających na wypełnianie misji systemu;
- określenie zakresu oceny: funkcjonalności, parametrów, niezawodności, współdziałania z operatorem, bezpieczeństwa i właściwości niewiążących się z zadaniami;
- ocena dostępności narzędzi do wykonania poszczególnych fragmentów oceny;
- oszacowanie kosztów i czasu wykonania oceny.
- sporządzenie sprawozdania z oceny

2.3. Prezentacja metodyki [5a, b]

Metodykę procesu oceny przedstawiono na rys. 1.



Rys. 1 – Prezentacja składowych metodyki oceny

Przy rozpatrywaniu każdego składnika oceny należy analizować i uwzględniać wpływ czynników zewnętrznych, w tym oddziaływanie człowieka. Błędy i pomyłki ludzkie są ważnym źródłem defektów i awarii systemów sterowania i procesów sterowanych

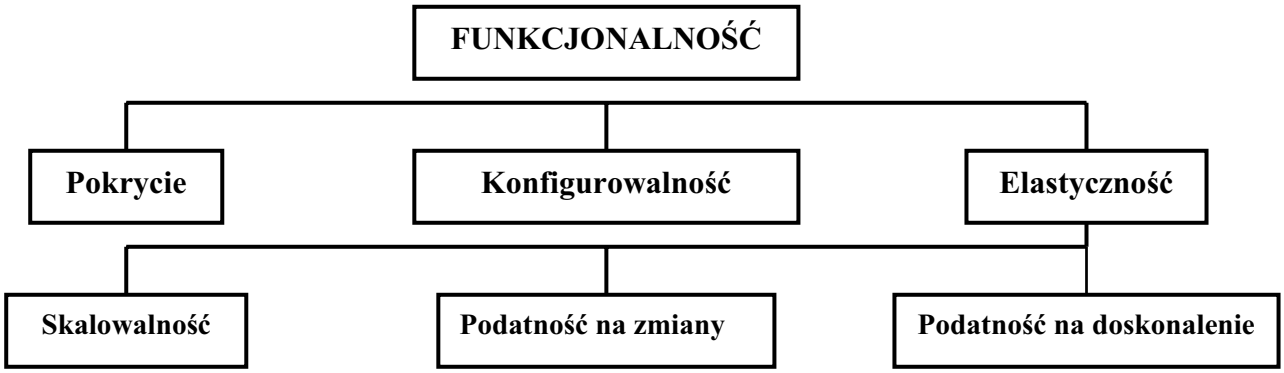
Tablica 1 – czynniki wpływające zestawienie

CZYNNIKI WPŁYWAJĄCE						
Zadanie	**Człowiek**	**Proces**	**Zasilanie**	**Środowisko**	**Serwis**	**Systemy zewnętrzne**
• Rodzaj - ciągłe - wsadowe - dyskretne	• Rozkazy - uprawnione - nieuprawnione - błędne	• Wejście/wyjście • Zaburzenia el. - sygnał wspólny - sygnał różnicowy	• Napięcie • Częstotliwość • Krótkie przerwy • Zapady • Stany przejściowe • Harmoniczne • Zaburzenia RF • Izolacja	• Temperatura • Czas - pełzanie - starzenie • Wilgotność • Deszcz • Substancje korozyjne • Mgła solna • Ciśnienie • Zamocowanie • Zaburzenia EM - RF promieniowane - RF przewodzone - nanosekundowe - udary • Zanieczyszczenia • Pleśnie • Narażenia mech. - udary - wibracje - przyspieszenia	• Dokumentacja • Pomoc techniczna • Serwis techniczny	• Rozkazy - uprawnione - nieuprawnione - błędne - atakujące
• Przedmiot - jednoparametrowe - wieloparametrowe	• Zadanie - zrozumiałe - niezrozumiałe					
• Rodzaj pracy - włączanie - wyłączanie - normalny - awaryjny	• Szkolenie - adekwatne - niewystarczające					
• Nadzorowanie - ciągłe - okresowe - bez nadzoru	• Obecność - ciągła - okresowa					

W tablicy 1 zestawiono czynniki wpływające na działanie systemu złożonego, które należy uwzględniać przy analizie i ocenie takiego systemu.

3. OCENA FUNKCJONALNOŚCI [5c]

Funkcjonalnością jest zakres, w jakim system zapewnia i ułatwia łączenie funkcji w celu wykonania zadań wynikających z misji systemu. Na rys. 2 przedstawiono składniki, które należy uwzględnić przy ocenie funkcjonalności.



Rys. 2 – Składowe funkcjonalności

Pokrycie jest scharakteryzowane przez:

- zakres zapewnianych funkcji;
- sposób w jaki funkcje współdziałają w celu wykonania zadań;
- liczbę dostępnych powtórzeń każdej funkcji.

Pokrycie wyraża się liczbowo przez współczynnik pokrycia.

Konfigurowalność jest to zakres, w jakim system ułatwia wybór, nastawianie i przygotowanie jego modułów do wykonywania zadań wynikających z misji systemu. Metody konfigurowania dzielą się na sprzętowe (np. za pomocą przewodów, zworników, łączników nastawnych lub wstawianie modułów sprzętowych) oraz programowe (np. przez nastawianie parametrów, opcji, wstawianie modułów oprogramowania).

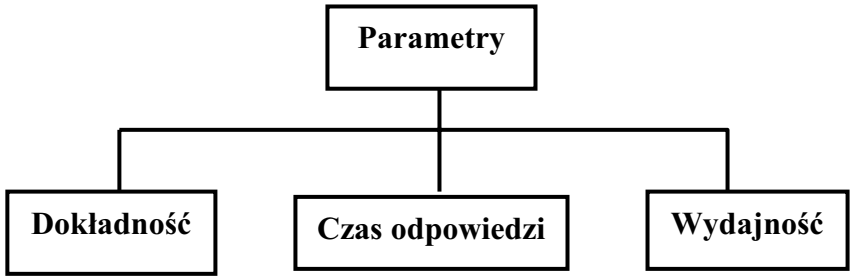
Elastyczność jest to zakres, w jakim system może być adaptowany. Wskazane na rysunku składowe elastyczności to:

- skalowalność, to jest zakres w jakim jest możliwa zmiana rozmiaru systemu, tak przez dodanie jak i usunięcie modułów;
- podatność na zmiany, jest możliwością zmiany zakresu wykonywanych zadań;
- podatność na doskonalenie jest możliwością udoskonalania pewnych właściwości systemu bez naruszania możliwości jego pracy (np. przez wprowadzenie modułów sprzętowych kompatybilnych z systemem, lecz o większej wydajności)

4. OCENA PARAMETRÓW SYSTEMU [5d]

Przez parametry systemu (ang. „performance” to po polsku właściwie „osiągi”- termin rzadko używany) należy tu rozumieć dokładność i szybkość, z jakimi system wykonuje swoje zadania w warunkach, do jakich jest przeznaczony. Tak rozumiane parametry mogą być ocenione tylko przez swoje składowe – podział na składowe zilustrowano na rys. 3. Aby móc

przeprowadzić ocenę, należy przeanalizować system pod kątem widzenia przetwarzania informacji.



Rys. 3 – Cechy składowe parametrów

Dokładność przetwarzania informacji jest scharakteryzowana przez: zgodność (z charakterem odtwarzanej wielkości), histerezę, strefę martwą, błąd powtarzalności, błąd odtwarzalności, rozdzielczość) i może być wyrażona ilościowo.

Na czas odpowiedzi przy przetwarzaniu informacji składają się szeregowo: czas zbierania informacji, czas obróbki informacji i czas uaktywniania wyjść, przy czym czas wynikowy nie musi być prostą sumą czasów składowych – niektóre przetwarzania mogą być współbieżne.

Wydajność systemu jest określona przez jego projekt i może zostać zmieniona tylko przez modyfikacje systemu. Nie można zmierzyć jej bezpośrednio, a tylko wyznaczyć przez pomiar zapasu wydajności jaki system ma przy każdym przetwarzaniu informacji.

Zapas wydajności systemu przy konkretnym przetwarzaniu informacji jest różnicą między największą liczbą tego konkretnego przetwarzania informacji (obciążenie 100 %) i liczbą odniesienia tego samego przetwarzania informacji zdefiniowaną w dokumencie wymagań systemowych (SRD) (obciążenie bazowe), którą system może wykonać w określonym przedziale czasu i w określonych warunkach odniesienia. Wartość żadnej z właściwości systemu nie powinna ulec degradacji, podczas pomiaru zapasu wydajności konkretnego przetwarzania informacji.
W przypadku systemów mogących realizować pewną liczbę różnych przetwarzań informacji, zapas wydajności nie może być wyrażony jedną wartością, a tylko w postaci tablicy wartości wyliczonych z największych ilości każdego przetwarzania informacji, które może być wykonane przez system w określonym okresie czasu, gdy liczby innych przetwarzań informacji są utrzymywane jako wartości stałe, równe wymaganym w SRD i gdy wartość żadnej właściwości systemu nie uległa degradacji.

Ocenę zapasu wydajności systemu można otrzymać obliczając, w odniesieniu do każdego z przetwarzań informacji, współczynnik obciążenia:

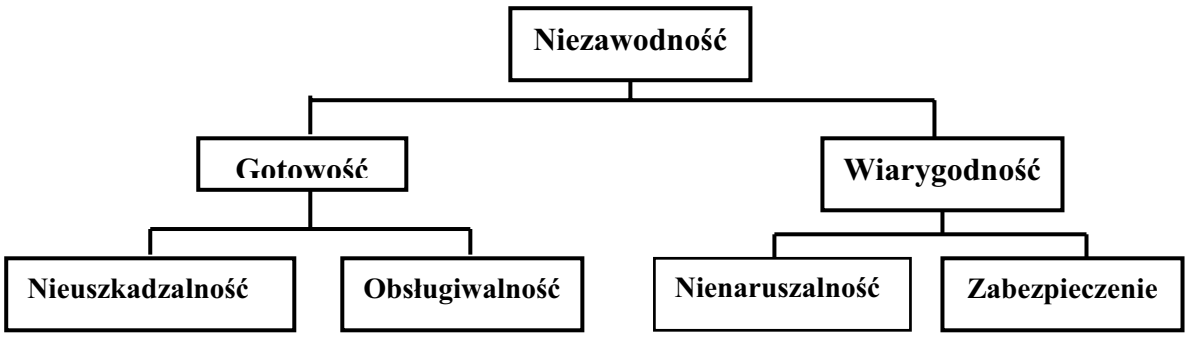
$$\textit{Współczynnik obciążenia} = \frac{\textit{Liczba przetworzeń informacji wg SRD/jedn. czasu}}{\textit{Maks. liczba przetworzeń informacji wg pomiaru/jedn. czasu}}$$

W odniesieniu do każdej wartości, zaleca się podanie precyzyjnej i szczegółowej informacji o warunkach, w jakich zostały one zmierzone.

5. OCENA NIEZAWODNOŚCI SYSTEMU [5e]

Niezawodność systemu jest zakresem, w jakim można polegać, że w danych warunkach, danej chwili lub w danym przedziale czasu, system wykona jedynie i prawidłowo określone zadanie pod warunkiem, że są dostarczone wymagane środki zewnętrzne. Aby system był niezawodny jest konieczne, iżby był gotowy do poprawnego wykonania swoich funkcji. W tym sensie niezawodność nie może być oceniona bezpośrednio, a tylko przez ocenę jej składowych.

Podział na składowe zilustrowano na rys. 4.



Rys. 4 – Cechy składowe niezawodności

Gotowością sytemu jest jego zdolność do utrzymywania się w stanie umożliwiającym wypełnianie wymaganych funkcji w warunkach, chwili lub przedziale czasu wynikających z misji systemu, przy założeniu, że są dostarczone wymagane środki zewnętrzne.

Gotowość systemu zależy od gotowości poszczególnych części systemu i od sposobu, w jaki te części współpracują przy wypełnianiu zadań systemu. Gotowość systemu przypisana każdemu zadaniu może być wyrażona ilościowo na dwa sposoby:

Do predykcji gotowości systemu, jego gotowość może być obliczona jako:

$$gotowość = \frac{średni\ czas\ do\ uszkodzenia}{(średni\ czas\ do\ uszkodzenia + średni\ czas\ naprawy)}$$

gdzie

- „gotowość" jest gotowością systemu przypisaną danemu zadaniu;
- „średni czas do uszkodzenia" jest średnią z czasów od naprawienia systemu do stanu wykonywania danego(ch) zadania(ń) do chwili, gdy system ponownie się uszkodzi;
- „średni czas naprawy" jest średnim z całkowitych czasów wymaganych do przywrócenia wykonywania danego zadania od chwili, gdy system przestał wykonywać to zadanie.

W przypadku systemu pracującego, gotowość może być obliczona jako:

$$gotowość = \frac{całkowity\ czas\ w\ którym\ system\ był\ zdolny\ do\ wykonania\ zadania}{całkowity\ czas\ w\ którym\ spodziewano\ się,\ że\ system\ wykona\ zadanie}$$

Cechami składowymi gotowości są:

– nieuszkadzalność, czyli zdolność do wypełnienia wymaganych funkcji w danych warunkach i w wymaganym przedziale czasu;
– obsługiwalność, czyli zdolność systemu do utrzymania lub odtwarzania w danych warunkach eksploatacji stanu, w którym może wypełniać wymagane funkcje przy założeniu, że obsługa jest wykonywana zgodnie z ustalonymi procedurami.

Wiarygodnością systemu jest zakres w jakim on jest zdolny do rozpoznania, zasygnalizowania i wytrzymania niepoprawnych wejść i nieuprawnionego dostępu. Ona zależy od zaimplementowanych mechanizmów nienaruszalności i zabezpieczenia.

Nienaruszalność jest pewnością dostarczaną przez system, że zadanie będzie wykonane prawidłowo; ona wiąże się z cechą bezpieczeństwa sytemu i będzie omówiona przy prezentacji oceny bezpieczeństwa.

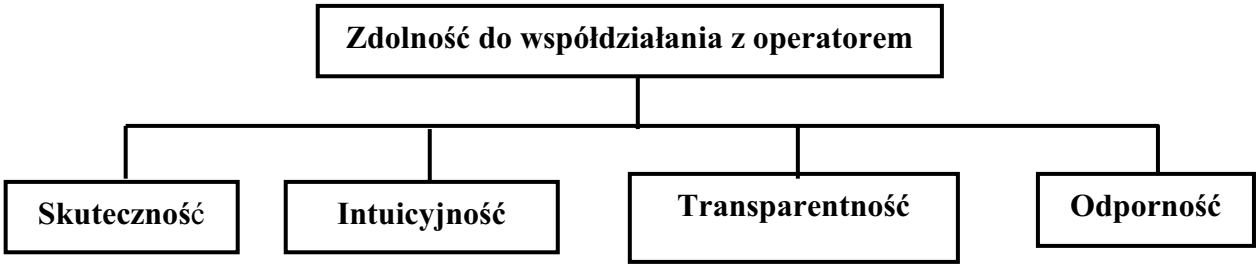
Zabezpieczenie jest pewnością dostarczana przez system, że każde niepoprawne wejście lub każdy nieuprawniony dostęp jest niemożliwy. Podstawą analizy i oceny są: model groźba-ryzyko i cykl życia zabezpieczenia. Przy walidacji jest wymagane sprawdzenie i wykazanie [10], że na przestrzeni całego cyklu życia zabezpieczenia są konsekwentnie przestrzegane zasady polityki zabezpieczenia w zakresie zarządzania dostępnością, nienaruszalnością, dostępem logicznym, dostępem fizycznym, dostępem zewnętrznym i podziałem pamięci.

Dokładna ocena nienaruszalności zabezpieczenia od działań zewnętrznych i przed niezrównoważeniem danych w sieci jest szczególnie ważną w przypadku systemów wykorzystujących zewnętrzne łącza informacyjne, np. Internet. W tym zakresie są prowadzone intensywne prace badawcze i normalizacyjne.

6. OCENA WSPÓŁDZIAŁANIA SYSTEMU Z OPERATOREM [5f]

Współdziałaniem systemu z operatorem jest to zakres w jakim środki operatorskie udostępniane przez system są skuteczne, intuicyjne, transparentne i odporne. Ta cecha systemu wiąże się ściśle z ergonomicznością i bezpieczeństwem systemu; środki operatorskie niedogodne dla operatora są nieergonomiczne i mogą prowadzić do powstawania zagrożeń.

Na rys. 5 zilustrowano cechy składowe do współdziałania systemu z operatorem.



Rys. 5 – Cechy składowe zdolności do współdziałania z operatorem

Skuteczność we współpracy z operatorem jest wtedy, gdy system pozwala operatorowi wykonać jego zadanie(a) w akceptowalnym przedziale czasu, z minimalnym wysiłkiem umysłowym i fizycznym, przy minimalnym ryzyku popełnienia błędu.

Zakres, w jakim jest to spełnione, stanowi miarę skuteczności systemu we współpracy z operatorem.

Skuteczność we współpracy z operatorem zależy między innymi od:

- ergonomiczności zaprojektowania urządzeń (klawiatura, mysz, wejście głosowe, przyciski specjalizowane, ekrany, wskaźniki itd.) zastosowanych jako środki operatorskie wspomagania interfejsu człowiek-maszyna;
- rozmieszczenia przestrzennego, liczby zastosowanych urządzeń i ich wzajemnego usytuowania na stacji operatorskiej;
- konfiguracji stacji operatorskiej;
- metody i procedur, które należy użyć do uzyskania informacji, wydania rozkazów itd.

Skuteczność we współpracy z operatorem nie może być wyrażona ilościowo jako jedna liczba. Jednakże może być wyrażona przez opis jakościowy zawierający pewne element ilościowe, na przykład:

- współczynnik pokrycia otrzymany przez porównanie środków operatorskich udostępnianych przez system z konkretnymi wymaganiami podanymi w dokumencie wymagań systemowych i w odpowiednich normach z wymaganiami ergonomicznymi;
- czas wymagany do wydania rozkazu i do otrzymania informacji.

Intuicyjność systemu we współpracy z operatorem wyraża się stopniem w jakim środki operatorskie odpowiadają powszechnej praktyce pracy.

Intuicyjność zależy od następujących czynników:

- zakresu, w jakim się postępuje się według ogólnych standardowych procedur, reguł i metod przy posługiwaniu się elementami „działania";'
- konwencji, według których postępuje się przy prezentowaniu informacji operatorowi, na przykład barwa czerwona do warunków awaryjnych itd.;
- konwencji, według których się postępuje przy wydawaniu rozkazów, na przykład obracanie pokrętła zgodnie z ruchem wskazówek zegara, aby zwiększyć wartość itd.

Transparentność oznacza, że środki operatorskie udostępniane przez system, umożliwiające operatorowi wydawanie rozkazów i prezentujące mu informacje, dają operatorowi rzeczywisty ogląd działań (i ich sekwencji), które należy wykonywać, aby wypełnić zadanie, które ma być zrealizowane. Zakres, w jakim te środki są udostępniane jest miarą transparentności systemu we współpracy z operatorem.

Transparentność zależy od następujących czynników:

- zasad logicznych, według których przedstawia się strukturę funkcjonalną i przestrzenną procesów i zadań, które ma wykonać operator,
- sposobu, w jaki użyto etykiet i nazw do zidentyfikowania środków operatorskich i konsekwentności ich użycia;
- konsekwentności w zastosowaniu barw, nazw, sygnalizatorów akustycznych itd. we wszystkich zadaniach i na wszystkich poziomach informacji;
- sposobu, realistycznego symulowana dynamiki zadań tak, aby dać operatorowi „rzeczywiste" wyczucie wykonywanych zadań, itd.

Informacje prezentowane przez system powinny być jasne, treściwe, jednoznaczne i niesprzeczne

Odporność oznacza, że środki operatorskie udostępniane przez system, umożliwiające operatorowi wydawanie rozkazów, poprawnie interpretują każde z działań operatora i poprawnie odpowiadają na nie, jeśli ono jest jednoznaczne a jeśli nie jest to żądają informacji dodatkowych do usunięcia niejednoznaczności. Stopień, w jakim jest to zrealizowane jest miarą odporności systemu we współpracy z operatorem.

Odporność zależy od następujących czynników:

– zakresu, w jakim odchylenie od ogólnych reguł standardowych jest dopuszczalne i jest interpretowane;
– zakresu, w jakim system jest zdolny do wykrycia i zgłoszenia odchyleń i powiązania tych odchyleń z żądaniami o dalsze informacje, itd.

7. OCENA BEZPIECZEŃSTWA SYSTEMU [5g]

7.1. Uwagi podstawowe

Właściwość bezpieczeństwa systemu we wszystkich aspektach (mechanicznym, elektrycznym itd.) zależy od bezpieczeństwa jego projektu jako takiego oraz jego niezawodności Ocena bezpieczeństwa systemu powinna obejmować wszystkie działania wiążące się z systemem podczas faz jego cyklu życia: instalowania, eksploatacji, wyłączenia z pracy i likwidacji. Ocena powinna ponadto obejmować wszystkie aspekty środowiskowe. W odniesieniu do każdej fazy należy rozpatrzyć, co najmniej następujące środki i działania:

- procedury eksploatacji, obsługiwania i wyłączenia z pracy;
- umieszczone oznakowania i napisy ostrzegawcze;
- likwidację opakowań, produktów odpadowych z urządzeń, wymienianych elementów składowych i materiałów czyszczących.

Przy ocenie bezpieczeństwa systemu należy rozpatrzyć następujące aspekty:

- rodzaje zagrożeń;
- odbiorców skutków zagrożeń;
- drogi rozprzestrzeniania zagrożeń;
- środki zmniejszenia ryzyka.

Metodyka oceny bezpieczeństwa funkcjonalnego zawarta w [9] wskazuje na obowiązek przeprowadzenia analizy zagrożeń i ryzyka przy której jest konieczność rozpatrzenia:

- zagrożeń: mechanicznych, elektrycznych, chemicznych, biologicznych, EMC, wprowadzanych przez światło i promieniotwórczość;
- odbiorców zagrożeń: człowieka, przyrodę i urządzenia;
- drogi rozprzestrzeniania się zagrożeń: bezpośrednie, pośrednie, dynamiczne i bezdotykowe.
- środków zmniejszenia ryzyka: zmniejszenie źródła urazu, przerwanie drogi rozprzestrzeniania się i ograniczenie prawdopodobieństwa, że odbiorca znajdzie się w strefie zagrożenia.

7.2. Sprawdzenie bezpieczeństwa użytkowania

System E/E/PES związany z bezpieczeństwem musi być przede wszystkim bezpieczny w użytkowaniu, które jest określane jako zakres , w którym system nie stwarza zagrożeń, pomimo działania na niego czynników zakłócających jego pracę. Badanie bezpieczeństwa użytkowania urządzeń i ocena bezpieczeństwa systemu jako całości należy wykonać ogólnie znanymi metodami. Wśród badań należy przykładowo wymienić:

- sprawdzenie zabezpieczenia przed dotykiem części czynnych;
- sprawdzenie wytrzymałości elektrycznej izolacji;
- sprawdzenie wytrzymałości obudów;
- sprawdzenie stopnia ochrony zapewnianego przez obudowy.
- sprawdzenie wprowadzenia urządzeń ochronnych wynikających z oceny zagrożeń i ryzyka.

8. OCENA WŁAŚCIWOŚCI NIE WIĄŻĄCYCH SIĘ Z ZADANIEM:

Składają się na nie cechy:

- wspomaganie systemu, określane jako zakres i jakość: serwisu technicznego, serwisu eksploatacyjnego u klienta, dokumentacji i szkolenia personelu;
- kompatybilność systemu, określana jako zgodność z przepisami prawnymi, normami i normami de facto (ogólnie uznanymi specyfikacjami technicznymi);
- właściwości fizyczne systemu, np. ciężar, gabaryty, konieczna przestrzeń serwisowa, generowanie wibracji i zaburzeń elektromagnetycznych, pobór mocy, wydzielanie ciepła, w odniesieniu do rzeczywistych warunków pracy.

9. BADANIA AKCEPTACYJNE [6, 7, 8]

9.1. Wprowadzenie

Badania akceptacyjne są ważnym elementem potwierdzania zgodności wykonania ze specyfikacją wymagań bezpieczeństwa. One są jednym z etapów odbioru komisyjnego systemów elektrycznych, pomiarowych i sterowania w przemyśle; punkty węzłowe odbioru są przedmiotem normy międzynarodowej IEC 62337:2007 [6]. Stanowią zatem element procesu weryfikacji i walidacji systemu złożonego. Metodyka przeprowadzania Fabrycznych Badań Akceptacyjnych (FAT) jest przedmiotem normy międzynarodowej [7]. Uzupełnieniem FAT są Badania Akceptacyjne Obiektowe (SAT) i Badania Integracyjne Obiektowe (SIT). Poniżej przedstawiono zasadnicze tezy metodyki ich przeprowadzania. Wszystkie te badania są badaniami typu konstruktorskiego i poprzedzają komisyjne uruchomienie i odbiór systemu. Kolejnym badaniem wykonywanym przed odbiorem komisyjnym jest sprawdzanie obwodów elektrycznych i sygnałowych [8]. W dalszym ciągu przedstawiono główne tezy metodyki prowadzenia tych badań.

9.2. Fabryczne badania akceptacyjne

Badania te są wykonywane przez wytwórcę, na terenie jego fabryki, na systemie zmontowanym i w pełni oprogramowanym. Minimalny zakres badania jest następujący:

A. Sprawdzenie dokumentacji wytwórcy, w tym raportów z badań wewnętrznych;
B. Sprawdzenie kompletności sprzętu i oprogramowania;
C. Kontrola mechaniczna;
D. Kontrola uzwojeń i zacisków;
E. Uruchomienie;
F. Sprawdzenie ogólnych funkcji systemu, w tym redundancji i diagnostyki sprzętu;
G. Sprawdzenie zgodności wizualizacji funkcjonalności z dokumentami opracowanymi przez Użytkownika i Wytwórcę, w tym złożonych i rodzajów pracy;
H. Badanie interfejsu podsystemów;
I. Przygotowanie dokumentów do SAT.

Badania są wykonywane metodą list kontrolnych. Dokumentacja z badań obejmuje: plany badania funkcji, zbiór list kontrolnych, dokumenty z badań sprzętu i oprogramowania, kopie wyświetlanych okien wiązanych z pomiarami.

9.3. Obiektowe badania akceptacyjne (SAT)

Badania są wykonywane na obiekcie, po całkowitym zainstalowaniu systemu u klienta. Minimalny zakres badań obejmuje:
A. Sprawdzenie dokumentacji wytwórcy;
B. Sprawdzenie kompletności sprzętu i oprogramowania;
C. Kontrolę mechaniczną;
D. Sprawdzenie uruchamiania i diagnostyki;
E. Załadowanie oprogramowania.

Badania są wykonywane metodą list kontrolnych. Dokumentacja z badań ma zawartość jak podano powyżej.

9.4. Obiektowe badania integracyjne (SIT)

Badania wykonuje się na obiekcie, po wykonaniu SAT. Minimalny zakres badań obejmuje:
A. Sprawdzenie dokumentacji wytwórcy;
B. Kontrolę mechaniczną;
C. Sprawdzenie diagnostyki;
D. Załadowanie oprogramowania.

Badania są wykonywane metodą list kontrolnych. Dokumentacja z badań ma zawartość jak podano powyżej.

9.5. Sprawdzanie obwodów elektrycznych i sygnałowych [8]

Badanie jest częścią działań poprzedzających odbiór komisyjny systemu. Jego zadaniem jest upewnienie się, że są dostępne wszystkie dokumenty dotyczące wykonania instalacji elektrycznej i sygnałowej, zostało dostarczone całe wyposażenie i wszystkie przyrządy, instalacja została wykonana zgodnie z dokumentami technicznymi i przepisami miejscowymi oraz funkcjonalność obwodów jest poprawna.

Wykonanie badania obejmuje:

A. Sprawdzenie dokumentacji: sprawdzenie kompletności i spójności dokumentacji obwodu, sprawdzenie dokumentów związanych z instalowaniem, sprawdzenie raportu z FAT.

B. Inspekcja wizualna – oględziny obwodu pod względem: poprawności zainstalowania oraz poprawności oznakowania i zaetykietowania.

C. Sprawdzenie poprawności funkcjonowania: sprzętu - wszystkich składników i podzespołów oraz oprogramowania.

D. W przypadku sprawdzania instalacji i obwodów związanych z bezpieczeństwem należy sporządzić uzupełniający plan sprawdzenia, procedury dodatkowe i dodatkowe formularze raportów zawierające czynności wynikające z cyklu życia bezpieczeństwa systemu.

E. Udokumentowanie sprawdzenia i jego wyników przez sporządzenie znormalizowanych raportów.

10. PODSUMOWANIE

Przedstawiono metodykę i wymagania dotyczące walidacji złożonego systemu automatyki i/lub robotyki, przy czym uwzględniono najnowsze opracowania międzynarodowe w tym zakresie.

Opracowanie zostało sfinansowane w ramach zadania 4.R.08 „Modele i procedury zgodności bezpieczeństwa funkcjonalnego systemów zabezpieczeniowych w sektorze przemysłu procesowego" Programu Wieloletniego „Poprawa bezpieczeństwa i warunków pracy" koordynowanego przez CIOP-PIB.

LITERATURA

[1] Missala T.: *Walidacja bezpieczeństwa urządzeń i instalacji automatyki*. Prace XIV Krajowej Konferencji Automatyki, t. I. ss. 515 – 522, Zielona Góra, czerwiec 2002 r.

[2] Missala T.: *Zagadnienia wybrane bezpieczeństwa sieciowych instalacji automatyki*. Materiały Konferencji Automation'2000, s. 94 - 101, Warszawa 2000 r.

[3] Missala T.: *Bezpieczeństwo funkcjonalne komunikacji w sieciach przemysłowych –stan normalizacji.* Materiały Konferencji Automation'2007, PAR nr 2/2007 + dyskietka, Warszawa 2007 r.

[4] PN-EN ISO 9000:2001. Systemy zarządzania jakością – Podstawy i terminologia.

[5] PN-EN 61069, Pomiary i sterowanie procesami przemysłowymi – Określenie właściwości systemu w celu jego oceny

a. PN-EN 61069-1:2002, Postanowienia ogólne i metodologia

b. PN-EN 61069-2:2002, Metodologia oceny

c. PN-EN 61069-3:2002, Ocena funkcjonalności systemu

d. PN-EN 61069-4:2004, Ocena parametrów systemu

e. PN-EN 61069-5:2004, Ocena niezawodności systemu

f. PN-EN 61069-6:2004, Ocena współdziałania systemu z operatorem

g. PN-EN 61069-7:2004, Ocena bezpieczeństwa systemu

h. PN-EN 61069-8:2004, Ocena niewiążących się z zadaniem właściwości systemu PN-EN 62337:2007, Odbiór komisyjny systemów elektrycznych, pomiarowych i sterowania w przemyśle procesowym – Określone fazy i punkty końcowe (*oryg*.)

[6] PN-EN 62381:2007, Czynności podczas fabrycznego testu akceptacyjnego (FAT), obiektowego testu akceptacyjnego (SOT) i obiektowego testu integracyjnego (SIT) systemów automatyzacji w przemyśle procesowym (*oryg.*).

[7] PN-EN 62382:2007, Sprawdzanie obwodów elektrycznych i przyrządowych (*oryg*.).

[8] PN-EN 61508 (IEC 61508): Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem:

a. PN-EN 61508-1:2004 Część 1: Wymagania ogólne

b. PN-EN 61508-2:2005 Część 2: Wymagania dotyczące elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem

c. PN-EN 61508-3:2004 Część 3: Wymagania dotyczące oprogramowania

d. PN-EN 61508-4:2004 Część 4: Definicje i skrótowce

e. PN-EN 61508-5:2005 Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa

f. PN-EN 61508-6:2007 Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3 PN-EN 61508-7:2003 Część 7: Przegląd technik i miar *(oryg.)*

[9] IEC 65/402/NP, Security for industrial-process measurement and control – Network and system security