

Walidacja elementów systemów sterowania związanych z bezpieczeństwem jako krok do zapewnienia bezpieczeństwa użytkowania maszyn

mgr inż. Tomasz Strawiński

Zakład Techniki Bezpieczeństwa CIOP - PIB

Walidacja

Walidacja elementów systemów sterowania maszyn związanych z bezpieczeństwem (ESSZB) jest zespołem działań, które w systematyczny sposób pozwolą zebrać dowody na spełnienie założeń bezpieczeństwa i upewnić wprowadzających maszynę na rynek, że spełniono w tym zakresie wymagania zasadnicze.

Walidacja jest obecnie jedyną polecaną metodą potwierdzania wymaganych właściwości ESSZB i dotyczy nawet najprostszych maszyn.

Wynika to z faktu, że podstawowe funkcje sterowania maszyn, jakimi są uruchamianie i zatrzymywanie normalne, zostały uznane za funkcje bezpieczeństwa.

Normy zawierające wymagania dotyczące walidacji ESSZB

PN-EN ISO 13849-2:2005 Bezpieczeństwo maszyn -- Elementy systemów sterowania związane z bezpieczeństwem -- Część 2: Walidacja (cały arkusz normy)

PN-EN 62061:2005 Bezpieczeństwo maszyn -- Bezpieczeństwo funkcjonalne elektrycznych, elektronicznych i programowalnych elektronicznych systemów sterowania związanych z bezpieczeństwem (oryg.) (rozdział 8)

Seria norm PN-EN 61508 Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych systemów związanych z bezpieczeństwem (części 1-7) (walidacja całkowita bezpieczeństwa, walidacja układów E/E/EP, walidacja oprogramowania odpowiednio w częściach 1, 2 i 3)

Walidacja – podstawowe wymagania

W ramach walidacji należy wykonać analizy i badania funkcji bezpieczeństwa przewidzianych do realizacji w ESSZB projektowanym według racjonalnych przesłanek i zgodnie z normami.

Zakres analiz i badań powinien obejmować właściwości charakterystyczne funkcji bezpieczeństwa oraz ich osiągnięte właściwości związane z bezpieczeństwem funkcjonalnym (kategoria, PL, SIL).

Walidacja powinna być prowadzona zgodnie z planem z zastosowaniem ogólnego schematu działań.

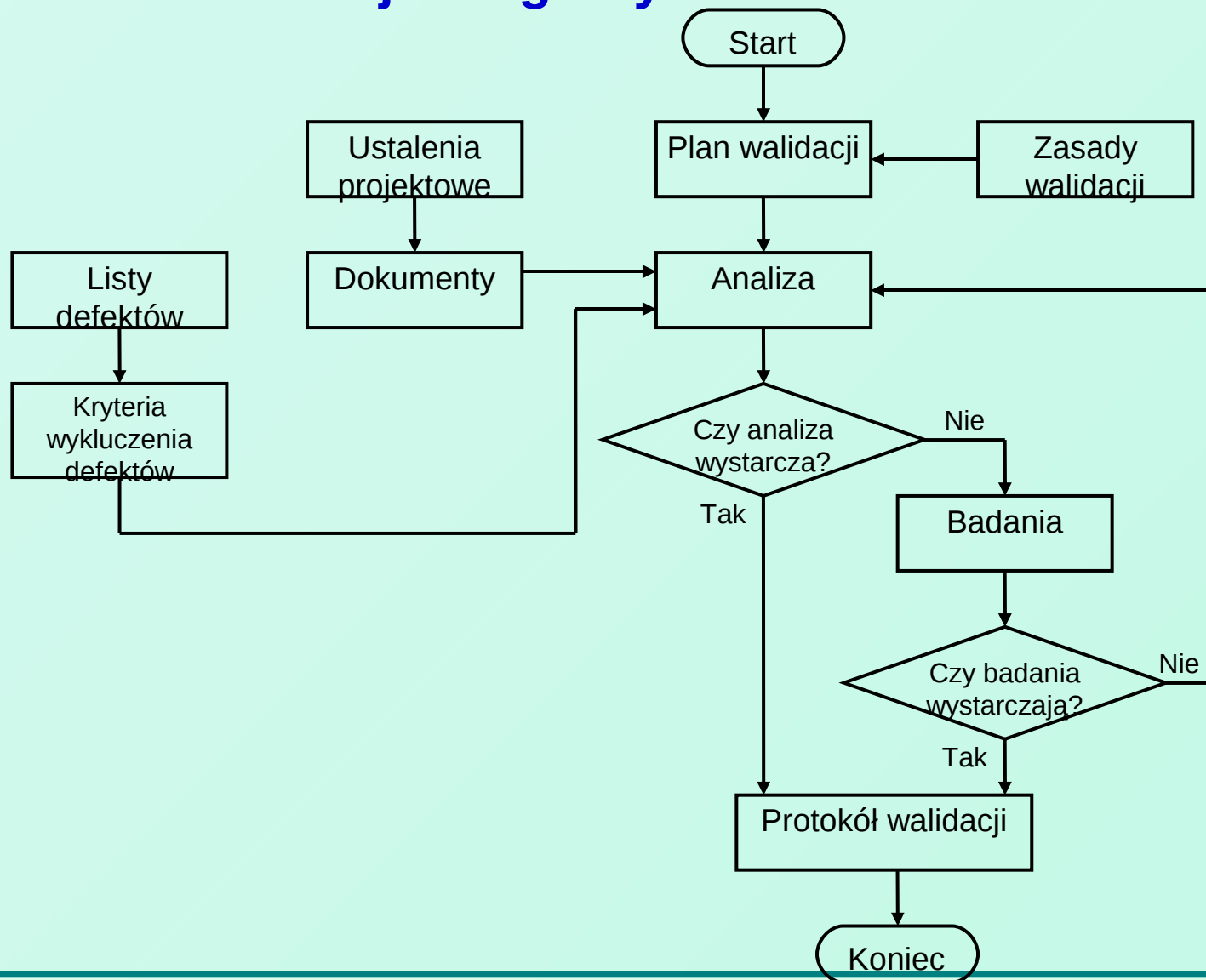
Walidację należy rozpocząć najwcześniej, jak to jest tylko możliwe, i równoległe z procesem projektowania, tak aby problemy mogły być rozwiązane wcześniej, gdy stosunkowo łatwo można je skorygować.

Analizy dla potrzeb walidacji należy prowadzić w oparciu o dokumentację zgromadzoną w procesie projektowania.

W przypadku systemów dużych ze względu na rozmiar, złożoność lub zintegrowanie systemu sterowania (z maszyną) można prowadzić walidację części ESSZB oddzielnie przed połączeniem, a następnie walidację skutków połączenia tych części między sobą i pozostałą częścią maszyny.

Proces walidacji powinien obejmować przeanalizowanie zachowania się ESSZB przy wszystkich defektach, które należy rozważyć. Podstawą do analizy powinny być odpowiednie, wynikające z doświadczenia, wykazy defektów podstawowych i szczególnych.

Walidacja – ogólny schemat działań



Plan walidacji - wymagania

W planie walidacji należy zidentyfikować i sformułować wymagania dotyczące przeprowadzenia procesu walidacji określonych funkcji bezpieczeństwa oraz ich kategorii. Należy w nim także zidentyfikować środki, których należy użyć w procesie walidacji wyszczególnionych funkcji bezpieczeństwa i ich właściwości w zakresie bezpieczeństwa funkcjonalnego (kategorii). We właściwych przypadkach należy w nim także określić:

- identyfikację dokumentów zawierających warunki techniczne, warunki pracy oraz środowiskowe,
- podstawowe zasady bezpieczeństwa,
- wypróbowane zasady bezpieczeństwa,
- wypróbowane elementy,
- założenia dotyczące defektów i wykluczenia defektów, które należy rozpatrzyć,
- analizy i badania, które należy zastosować.

Metodyka prowadzenia projektowania i walidacji ESSZB maszyn (1)

- Projekt ESSZB maszyny składa się z pewnej liczby projektów umownie określonych funkcji bezpieczeństwa.
- Projekt umownie określonej funkcji bezpieczeństwa obejmuje jedną lub więcej rzeczywistych funkcji bezpieczeństwa realizowanych w jednym połączonym procesie projektowania i następnie walidacji.
- W przypadku dużych złożonych systemów umownie określona funkcja bezpieczeństwa może określać rzeczywistą funkcję bezpieczeństwa, do której realizacji wykorzystano podzespoły i wyniki uzyskane w procesie projektowania i walidacji innych umownych funkcji bezpieczeństwa (w ramach których powstały użyte podzespoły).
- Proces projektowania umownie określonej funkcji bezpieczeństwa należy podzielić na etapy.
- Liczba etapów projektowania i zakres prac projektowych wchodzących do etapu jest dowolny (powinno to wynikać z przyjętych zasad realizacji projektów i być dostosowane do właściwości i wymagań związanych z realizowanym układem).

Metodyka prowadzenia projektowania i walidacji ESSZB maszyn (2)

- Liczba i rodzaj etapów projektowania może być dynamicznie dostosowywana do wymagań kształtujących się podczas realizacji projektu.
- Z każdym etapem projektowania związana jest walidacja wyników uzyskanych w danym etapie (faza projektowania i faza walidacji).
- Plan walidacji umownej funkcji bezpieczeństwa jest listą etapów projektowania (i jednocześnie planem realizacji projektu). Plan walidacji ESSZB maszyny jest listą etapów projektowania wszystkich umownie określonych funkcji bezpieczeństwa.
- Faza projektowania etapu (w sensie metodyki projektowania i walidacji ESSZB) polega na sporządzeniu lub zgromadzeniu dokumentacji wymaganej i odpowiedniej dla danego etapu, zarejestrowaniu jej i zaznaczeniu jako gotowej do wykorzystania podczas walidacji.
- Po zakończeniu fazy projektowania etapu (gotowość dokumentacji) może rozpocząć się jej walidacja. W ramach fazy walidacji powinna powstać dokumentacja (raport) przedstawiająca jej wyniki, zostać zarejestrowana powinien zostać podany wynik ogólny walidacji etapu (pozytywny, negatywny).

Metodyka prowadzenia projektowania i walidacji ESSZB maszyn (3)

- Projektowanie umownie określonej funkcji bezpieczeństwa kończy się w momencie zakończenia wszystkich faz projektowania w etapach (gotowość dokumentacji) i uzyskania dla tych etapów pozytywnego wyniku walidacji.
- Projektowanie ESSZB maszyny kończy się momencie zakończenia projektowania wszystkich umownie określonych funkcji bezpieczeństwa.
- Za realizację faz projektowania ESSZB maszyny odpowiada koordynator projektu ESSZB, który może powierzyć zadanie projektowania umownie określonej funkcji bezpieczeństwa wyznaczonemu projektantowi (może on reprezentować zespół projektowy).
- Za realizację faz walidacji ESSZB maszyny odpowiada koordynator walidacji, który może powierzyć zadanie walidacji umownie określonej funkcji bezpieczeństwa wyznaczonej osobie.

Narzędzia programowe do prowadzenia i dokumentowania walidacji ESSZB

- Zastosowanie przedstawionej metodyki prowadzenia projektowania i walidacji ESSZB;
- Wprowadzenie pomocniczych baz danych dotyczących wypróbowanych elementów stosowanych w projektach ESSZB, defektów związanych z wykorzystanymi elementami, zasad bezpieczeństwa, które mogą być uwzględnione w projekcie oraz osób uczestniczących w procesach projektowania i walidacji;
- Możliwość sporządzania różnych dokumentów i raportów

Sugerowane etapy projektowania i walidacji

- Ocena ryzyka i określenie wymagań dotyczących realizacji funkcji bezpieczeństwa;
- Określenie warunków technicznych, środowiskowych i wpływu materiałów przetwarzanych;
- Projektowanie funkcji bezpieczeństwa (schematy blokowe, ideowe, montażowe układów, opis funkcjonalny, wykresy sekwencji czasowych sygnałów);
- Opracowanie oprogramowania funkcji bezpieczeństwa;
- Opracowanie opisu funkcji bezpieczeństwa dla użytkownika i procedury sprawdzeń funkcji bezpieczeństwa;
- Sporządzenie listy wypróbowanych elementów zastosowanych w projekcie funkcji bezpieczeństwa;
- Określenie zasad bezpieczeństwa uwzględnionych w projekcie funkcji bezpieczeństwa;
- Wyznaczenia osiągniętego PL lub SIL;
- Badania laboratoryjne i testy funkcjonalne;
- Testy oprogramowania;
- (ewentualne dodatkowe etapy projektowania i walidacji);
- Końcowa walidacja funkcji bezpieczeństwa;