Komputerowe wspomaganie walidacji systemów sterowania maszynami

Computer support of machinery control system validation

MAREK DŹWIAREK
JAKUB TERCZYŃSKI *

Materiały z XX SKWPWiE, Jurata 2016 r.
DOI: 10.17814/mechanik.2016.7.126

Właściwe przeprowadzenie walidacji poziomu zapewnienia bezpieczeństwa (PL) uzyskiwanego przez systemy sterowania maszynami jest podstawowym warunkiem potwierdzającym, że defekty tych systemów nie doprowadzą do utraty funkcji bezpieczeństwa. W artykule przedstawiono program komputerowy usprawniający prowadzenie i dokumentowanie walidacji systemów realizujących funkcje bezpieczeństwa w maszynach.
SŁOWA KLUCZOWE: bezpieczeństwo maszyn, funkcje bezpieczeństwa, poziomy zapewnienia bezpieczeństwa, walidacja

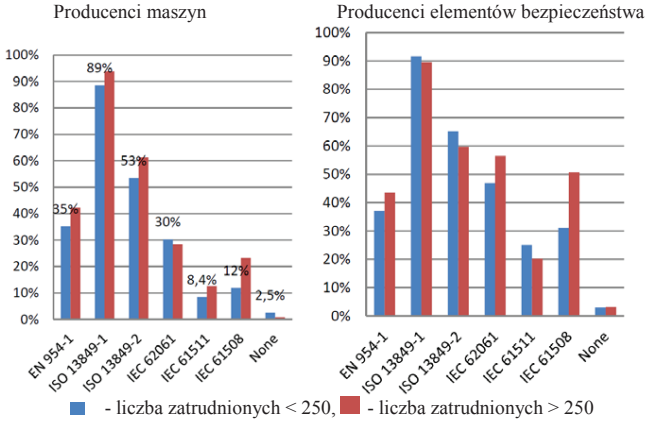
The proper validation of a performance level (PL) achieved by machinery control system is prerequisite for ensuring that the failure appearing in those systems would not cause the loss of safety functions. The paper presents software developed for making more efficient all the operations involved into conducting validation and documentation processes of the systems providing safety functions in machinery.
KEYWORDS: safety of machinery, safety functions, performance level, validation

Według *Rocznika Statystycznego Przemysłu* w 2005 r. w Polsce działało 4288 przedsiębiorstw produkujących maszyny. W 2012 r. były to 4992 przedsiębiorstwa. Natomiast naprawą konserwacją i instalowaniem maszyn zajmowało się odpowiednio 23 423 w 2005 r. i 24 239 w 2012 r. Wszystkie te działania mają wpływ na bezpieczeństwo operatorów maszyn. Według sprawozdania z działalności PIP w 2013 roku w Polsce miało miejsce 57 wypadków śmiertelnych spowodowanych utratą kontroli nad maszyną, co stanowi 15,1% wszystkich wypadków śmiertelnych zbadanych przez PIP. Dane te wskazują, jak istotne jest projektowanie, a następnie instalowanie maszyn z uwzględnieniem właściwego zastosowania środków ochronnych. W celu upewnienia się, że działania te są prowadzone właściwie, należy przeprowadzić walidację zastosowanych środków bezpieczeństwa. W przypadku nowych maszyn dyrektywa maszynowa 2006/42/WE nakłada na producenta obowiązek przeprowadzenia oceny zgodności oraz jej udokumentowania. Wśród tych środków ochronnych szczególną rolę odgrywają elementy systemów sterowania realizujące funkcje bezpieczeństwa. Właściwe przeprowadzenie walidacji poziomu zapewnienia bezpieczeństwa uzyskiwanego dzięki zastosowaniu tych systemów jest podstawowym warunkiem potwierdzającym, że defekty tych systemów nie doprowadzą do utraty funkcji bezpieczeństwa, a w konsekwencji nie spowodują groźnych w skutkach wypadków [1].

Dotychczasowy stan wiedzy

Możliwość ciągłej kontroli pracy maszyn jest także wykorzystywana do zapobiegania sytuacjom niebezpiecznym, a więc do realizacji funkcji bezpieczeństwa przez systemy sterowania.

Ponieważ nieprawidłowe działanie systemu sterowania jest skutkiem defektu, przypadkowego lub systematycznego, więc istotną właściwością systemów realizujących funkcję bezpieczeństwa jest odporność na defekty. Znalazło to także odzwierciedlenie w wymaganiach zasadniczych dyrektywy maszynowej. Wymagania dotyczące odporności systemów sterowania maszynami na defekty zostały uszczegółowione w normach: PN EN-ISO 13849-1 i EN 62061 [2].



Rys. 1. Stosowanie norm dotyczących systemów sterowania maszynami

W przypadku obu tych norm wymaga się, aby w celu potwierdzenia spełnienia wszystkich wymagań przeprowadzić walidację elementów systemu sterowania realizujących funkcje bezpieczeństwa. Według ankiety przeprowadzonej przez ISO TC 199/WG1 „Merging of ISO 13849-1 and IEC 62061" prawie 90% producentów maszyn i dostawców elementów bezpieczeństwa stosuje w praktyce normę ISO 13849-1, a 60% normę ISO 13849-2, jak to pokazano na rys. 1. Wyniki tej ankiety wskazują, że główne zapotrzebowanie dotyczy wspomagania realizacji wymagań norm z serii ISO 13849. Znalazło to odzwierciedlenie w opracowaniach dotyczących projektowania związanych z bezpieczeństwem systemów elementów sterowania maszynami. Aktualnie najpowszechniej używany jest przewodnik opracowany w IFA. Narzędziem wspomagającym projektowanie tych systemów jest oprogramowanie SISTEMA. Umożliwia ono wyznaczenie uzyskanego poziomu zapewnienia bezpieczeństwa PL na podstawie parametrów niezawodnościowych, wyznaczonych w procesie walidacji. Natomiast nie obejmuje szeregu działań związanych z walidacją systemu [2]. Podobne rozwiązanie zastosowano w narzędziach wspomagających ocenę ryzyka przy projektowaniu maszyn PRO-M. Także program Safexpert zawiera moduły dotyczące wymagań odnoszących się do systemu sterowania maszyną.

Praktyczne badania dostępnych narzędzi wspomagających ocenę systemu sterowania według normy ISO 13849-1 przedstawiono w [2]. Wnioski uzyskane przez autorów artykułu potwierdzają, że różne dostępne narzędzia programistyczne dedykowane do oceny systemów sterowania maszynami umożliwiają przede wszystkim wyznaczenie osiąganego PL, ale nie zawierają narzędzi wspomagających walidację parametrów niezbędnych do prowadzenia obliczeń.

* Dr hab. inż. Marek Dźwiarek (madzw@cip.pl), prof. CIOP-PIB; mgr inż. Jakub Terczyński (jater@ciop.pl) – CIOP – PIB

Metodyka badań

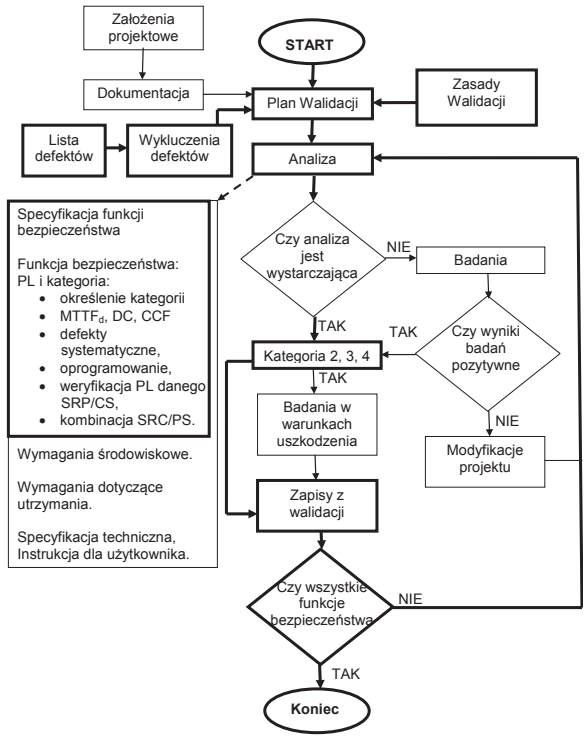
Podstawą do sformułowania założeń programu było opracowanie procedur prowadzenia walidacji poziomu zapewnienia bezpieczeństwa PL przez systemy sterowania maszynami. Konieczne było przeanalizowanie analizy wymagań dotyczących poszczególnych poziomów zapewnienia bezpieczeństwa przez systemy sterowania maszynami i określenie, jak poszczególne wymagania należy potwierdzić w procesie walidacji. Uwzględnione przy tym zostały systemy wykonane w różnych technikach: elektromechaniczne, elektroniczne, pneumatyczne, hydrauliczne.

Walidacja powinna wykazać, że SRP/CS spełnia wymagania ISO 13849-1, a w szczególności:

- określone w procesie projektowania wymagania dotyczące realizowanych przez te elementy funkcji bezpieczeństwa,
- wymagania dotyczące określonego poziomu zapewnienia bezpieczeństwa,
- wymagania dotyczące określonej kategorii zgodnie z PN-EN ISO 13849-1,
- środki zastosowane w celu zapobiegania defektom systematycznym,
- wymagania dotyczące oprogramowania, jeśli dotyczy,
- zdolność SRP/CS do realizacji funkcji bezpieczeństwa w określonych warunkach środowiskowych,
- ergonomiczność zaprojektowanego interfejsu operatora, tak aby operator nie był nakłaniany do niebezpiecznych działań, np. obchodzenia SRP/CS.

Podstawowe wymagania dotyczące prowadzenia walidacji SRP/CS podane są w PN EN ISO 13849-2. Ogólny proces walidacji SRP/CS według tej normy pokazany jest na rys. 2. Na rysunku tym pogrubiono obszary dotyczące walidacji poziomu zapewnienia bezpieczeństwa PL poprzez analizę, a więc te, które powinny być uwzględniane w opracowywanym programie. Są to działania dotyczące:

- planu walidacji w części dotyczącej analizy poziomu zapewnienia bezpieczeństwa,
- tworzenia list defektów wraz z ich wkluczeniami,
- formułowania specyfikacji funkcji bezpieczeństwa,
- określania i walidacji kategorii funkcji bezpieczeństwa,
- wyznaczania wskaźników PL: MTTFd, CD, CCF,



Rys. 2. Walidacja PL w ogólnym procesie walidacji SRP/CS

- sprawdzania środków zapobiegania defektom systematycznym, w tym w oprogramowaniu,
- weryfikacji osiągniętego PL,
- wyznaczania PL w przypadku kombinacji SRP/CS realizujących jedną funkcję bezpieczeństwa.

Opracowana metodyka przedstawiona została w formie graficznych procedur, które stanowiły założenia do programu.

Następnie opracowany został program komputerowy. Program ten opracowano zgodnie z tzw. zwinnymi metodami wytwarzania oprogramowania – *agile software development*. Proces realizacji oprogramowania ukierunkowany był na:

- bezpośrednią i regularną współpracę zespołu programistów z ekspertami merytorycznymi,
- szybkie reagowanie na zmiany wymagań na każdym etapie tworzenia oprogramowania,

Działania te miały na celu dostarczanie działającego oprogramowania możliwie jak najwyższej jakości. Poszczególne moduły programu w miarę powstawania były poddawane testom sprawdzającym, że działają zgodnie z założeniami.

Struktura programu

Opracowana aplikacja przystosowana jest do obsługi przez przeglądarkę internetową. Jednak ze względu na charakter wprowadzanych danych aplikacja dostarczana będzie użytkownikom jako pakiet instalacyjny. Możliwe jest także wykorzystanie technologii chmury do przechowywania danych.

Program ma formę hierarchicznej bazy danych. Baza składa się z 21 tabel, które połączone są między sobą relacyjnie w przypadku, kiedy dane zasoby przyporządkowane są zasobom z innej tabeli. Do napisanych funkcji stworzono interfejs użytkownika w oparciu o język HTML oraz framework styli CSS Bootstrap.

Działanie programu i jego testowanie

Testowanie programu miało na celu sprawdzenie, czy wszystkie zawiera on wszystkie niezbędne elementy zawarte w założeniach opracowanych w poprzednim etapie. Testowanie obejmowało sprawdzenie wszystkich modułów programu. Przeprowadzono je z wykorzystaniem pięciu różnych systemów sterowania kategorii B, 1, 2, 3 i 4.

W efekcie testowania końcowego potwierdzono poprawność funkcjonowania programu. Wykazano także, że umożliwia on zrealizowanie wszystkich procedur postępowania w procesie walidacji według normy systemów sterowania maszynami. Szczególnie istotne jest, że program prowadzi użytkownika wykonującego walidację krok po kroku. Ten sposób postępowania pozwala uniknąć pominięć i omyłek. Jednocześnie zastosowanie programu pokazuje, jak wykonać wszystkie kroki walidacji skutecznie i w stosunkowo prosty sposób.

* * *

Publikacja opracowana na podstawie wyników III etapu programu wieloletniego „Poprawa bezpieczeństwa i warunków pracy”, finansowanego w latach 2014÷2016 w zakresie zadań służb państwowych przez Ministerstwo Rodziny, Pracy i Polityki Społecznej. Koordynator programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

LITERATURA

1. Dźwiarek M. “An analysis of Accident Caused by Improper Functioning of Machine Control Systems”. *International Journal of Occupational Safety and Ergonomics*. 2004; 10(2), pp. 129÷136.
2. Jocelyn S., Baudoin J., Chinniah Y., Charpentier P. “Feasibility study and uncertainties in the validation of anexisting safety-related control circuit with the ISO 13849-1:2006 design standard”. *Reliability Engineering and System Safety*. 2014; 121: pp. 104÷112.