Napęd wyposażony w funkcje bezpieczeństwa zgodnie z IEC EN 61508

Opracowanie i realizacja cech architektury

*Peter Malus, Müllheim; Werner Thomann, Müllheim; Karl-Heinz Kayser, Göppingen *)*

Dokończenie artykułu z zeszytu 2/2015.

Celem przedsięwzięcia jest zintegrowanie funkcji bezpieczeństwa w obecnie produkowanej generacji napędów bez wprowadzania zasadniczych modyfikacji systemowych (na przykład obudowy, wymiarów zewnętrznych) w napędzie już istniejącym.

Redundantne czy wielokanałowe wykonanie elementów składowych, takich jak przekładnia, silnik, układ sterowania silnika (stycznik, tyrystor) wykluczone jest ze względów technicznych oraz z powodów przytoczonych powyżej. Z pierwszych analiz i obliczeń parametrów SFF i PFD wynikało, że wymienione, istniejące elementy pozwalają utrzymać dopuszczalny zakres. Tym samym realizacja funkcji bezpieczeństwa, czyli ich integracja z napędem, okazała się możliwa.

Istniejący sterownik (obwód logiczny) napędu, stanowiący system wieloprocesorowy z oprogramowaniem, nawet w wykonaniu standardowym wyposażony jest w funkcje bezpiecznego zatrzymania lub awaryjnego wyłączenia ESD. Nie spełniają one jednak wymagań SIL 2. Oparta na rozwiązaniach softwarowych integracja funkcji bezpieczeństwa z istniejącym systemem mikroprocesorowym jest teoretycznie możliwa, ale rozdzielenie funkcji bezpieczeństwa i funkcji standardowej wiązałoby się z poważnymi nakładami technicznymi.

Przyłącza umożliwiające komunikację z nadrzędnym systemem sterującym (magistrala obiektowa lub binarne wejścia/wyjścia) również nie spełniają warunków SIL 2 i wymagają modyfikacji.

3.1 Realizacja funkcji bezpieczeństwa

Jak już wspomniano, sterowanie (obwód logiczny) i przyłącza są głównym polem działania dla integracji funkcji bezpieczeństwa – ESD i bezpiecznego zatrzymania w napędzie.

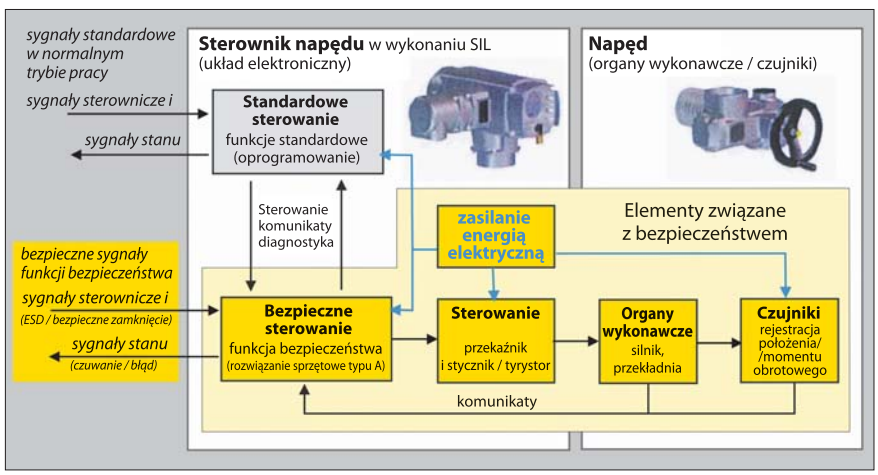
Koncepcje sterowania

Integrację funkcji bezpieczeństwa ze sterownikiem napędu umożliwiają następujące rozwiązania – patrz *ilustr. 6*.

1. Bezpośrednia integracja z dostępnym w wykonaniu standardowym sterownikiem wykorzystującym system wieloprocesorowy (oprogramowanie w bezpiecznym środowisku sprzętowym typu B).
2. Integracja na bazie dodatkowego, bezpiecznego sterownika (jednokanałowego) korzystającego z mikroprocesora (oprogramowanie zainstalowane w dodatkowym bezpiecznym rozwiązaniu sprzętowym typu B).
3. Integracja na bazie dodatkowego, bezpiecznego sterownika (jednokanałowego) korzystającego z mikroprocesora, oprócz tego nadzór (diagnostyka) realizowany przez istniejący sterownik, co oznacza scalenie bezpiecznych algorytmów diagnostycznych z istniejącym sterownikiem (oprogramowanie diagnostyczne w bezpiecznym środowisku diagnostycznym typu B).
4. Integracja na bazie dodatkowego, bezpiecznego sterownika korzystającego z mikroprocesora oraz na bazie istniejącego sterownika. Uzyskuje się w ten sposób dwukanałową implementację pozwalającą na wzajemny nadzór (diagnostykę) (oprogramowanie w bezpiecznym środowisku sprzętowym typu B oraz oprogramowanie w dodatkowym bezpiecznym rozwiązaniu sprzętowym typu B).
5. Integracja na bazie dodatkowego, bezpiecznego obwodu logicznego w postaci układowej, co stanowi rozwiązanie sprzętowe (dodatkowy bezpieczny sprzętowy obwód logiczny typu A).

Ocena koncepcji sterowania

Rozwiązania 1 do 4 korzystają z mikroprocesorów i wymagają stworzenia oprogramowania związanego z bezpieczeństwem. W rozumieniu normy IEC EN 61508 mikroprocesory są złożonymi elementami (typ B), których dotyczą o wiele bardziej restrykcyjne wartości graniczne SFF, co wymusza znacznie większe nakłady na diagnostykę, niż jest to konieczne w wypadku prostych elementów (typ A). Złożone układy typu B oraz wymagające opracowania oprogramowanie bezpieczeństwa niosą ze sobą zwiększone ryzyko wystąpienia uszkodzeń systematycznych (złożoność osprzętu). Natomiast rozwiązanie 5 charakteryzuje się niskim potencjałem uszkodzeń systematycznych (brak oprogramowania, prosty obwód logiczny). Dzięki zastosowaniu elementów o mniejszej złożoności (na przykład układ logiczny typu A) wymagania odnośnie parametru SFF są łagodniejsze, co może się wiązać z mniejszymi wymaganiami diagnostycznymi. Nie oznacza to rezygnacji z rozbudowanych funkcji diagnostycznych w standardowym sterowniku, istniejące algorytmy diagnostyczne nie stanowią tylko przedmiotu formalnej analizy bezpieczeństwa. W rozwiązaniu 5



Ilustracja 7. Budowa kompleksowego systemu bezpiecznego napędu

Objaśnienia – definicje pojęć

Intensywność uszkodzeń λ i prawdopodobieństwo wystąpienia uszkodzenia PF(t)

Intensywność uszkodzeń λ wyraża się w jednostkach [1/h] lub [FIT=10^{-9} 1/h]. Dla λ = *const*. (dotyczy fazy eksploatacji w rozkładzie Weibulla) obowiązuje następująca zależność między prawdopodobieństwem wystąpienia uszkodzenia *PF* [%] (*Probability of Failure*), a intensywnością uszkodzeń λ:

$PF(t) = 1 - e^{-\lambda t}$ lub uproszczona i poddana linearyzacji zależność: $PF(t) = = \lambda \cdot t$ (dla czasu eksploatacji $<< 1/\lambda$)

Intensywność uszkodzeń i prawdopodobieństwo wystąpienia uszkodzenia dla zastosowań związanych z bezpieczeństwem

W przypadku zastosowań związanych z bezpieczeństwem należy ocenić, czy uszkodzenia, na przykład elementu konstrukcyjnego, zagrażają lub nie zagrażają funkcji bezpieczeństwa. Dlatego też intensywność uszkodzeń λ klasyfikuje się jako bezpieczne λ_S (*safe*) i niebezpieczne λ_D (*dangerous*).

Za pomocą diagnostyki i nadzoru można wykryć niebezpieczne uszkodzenie na tyle wcześnie, aby wprowadzić w instalacji bezpieczny stan. Wśród niebezpiecznych uszkodzeń λ_D można wobec tego wyróżnić niebezpieczne wykryte uszkodzenia λ_{DD} (*detected*) oraz niebezpieczne niewykryte uszkodzenia λ_{DU} (*undetected*).

$$\lambda = \lambda_S + \lambda_D = \lambda_S + \lambda_{DD} + \lambda_{DU}$$

Decydujące znaczenie dla oceny systemu związanego z bezpieczeństwem ma w związku z powyższym prawdopodobieństwo wystąpienia niebezpiecznego uszkodzenia PF_D.

$PF_D(t) = 1 - e^{-\lambda_{DU} t}$ dla $\lambda_{DD} \neq 0$ lub $PF_D(t) = 1 - e^{-\lambda_D t}$ przy $\lambda_{DD} = 0$

Uwaga: przedstawiony wzór uwidacznia zależność między λ_{DU}/λ_D a PF_D. Obliczenia przeciętnego prawdopodobieństwa wystąpienia uszkodzenia w rzeczywistych systemach mogą być bardziej złożone. Zwłaszcza wtedy, gdy mamy do czynienia z kompleksowymi, wielokanałowymi systemami i/lub należy uwzględnić cykliczne zabiegi kontrolne lub przedziały czasowe między uruchomieniem funkcji bezpieczeństwa. Właściwymi narzędziami do wyznaczenia przeciętnego prawdopodobieństwa wystąpienia uszkodzenia są analiza drzewa uszkodzeń i uwzględniające stan modele prawdopodobieństwa według Markowa.

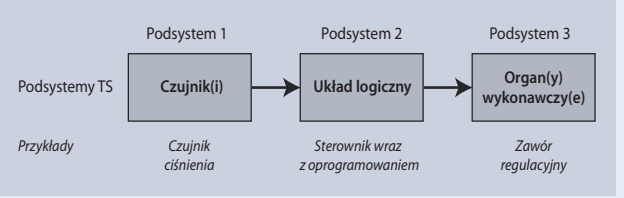
Udział uszkodzeń bezpiecznych SFF i pokrycie diagnostyczne DC

Niskie prawdopodobieństwo wystąpienia uszkodzenia można osiągnąć bez zastosowania technik diagnostycznych, ale w razie wystąpienia niebezpiecznego defektu system ulega wtedy awarii. Dlatego też zdefiniowano w normie dodatkowe parametry. Pokrycie diagnostyczne (*Diagnostic Coverage* – DC) opisuje intensywność wykrytych uszkodzeń niebezpiecznych, a parametr udział uszkodzeń bezpiecznych (*safe failure fraction* – SFF) informuje o stosunku liczby uszkodzeń niegroźnych do ogólnej liczby uszkodzeń.

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \qquad DC = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} = \frac{\lambda_{DD}}{\lambda_D}$$

Architektura odniesienia

Norma IEC EN 61508 określa architekturę referencyjną systemów związanych z bezpieczeństwem składającą się z trzech podsystemów (TS1…TS3), *patrz ilustr. 8*. Podczas analizy konkretnego systemu należy odwzorować go w postaci architektury odniesienia.



***Architektura odniesienia** systemów związanych z bezpieczeństwem [1]*

Wykorzystanie (tryby pracy) systemów związanych z bezpieczeństwem

Wyróżnia się następujące tryby pracy:

- Tryb niskiej intensywności przywołania (low demand lub on demand, na przykład poduszka powietrzna w samochodzie), tzn. funkcja związana z bezpieczeństwem nie jest uruchamiana częściej niż raz w roku i przywołanie nie jest większe niż podwojona częstotliwość kontroli okresowych. Parametr: PFD_D = średnie prawdopodobieństwo wystąpienia uszkodzenia funkcji związanej z bezpieczeństwem w trybie pracy na przywołanie – *probability of failure on demand*.
- Tryb charakteryzujący się wysokim lub stałym przywołaniem (*high demand*, na przykład kurtyny świetlne w ręcznie ładowanej wytłaczarce), tzn. funkcja związana z bezpieczeństwem jest uruchamiana częściej niż raz w roku i zapotrzebowanie jest większe niż podwojona częstotliwość kontroli okresowych. Parametr: PFH_D = średnie prawdopodobieństwo niebezpiecznego uszkodzenia w ciągu godziny – *probability of failure on high demand*.

Sprzętowa realizacja systemów związanych z bezpieczeństwem

Systemy lub podsystemy związane z bezpieczeństwem pod względem realizacji sprzętowej dzieli się na:

- Systemy, podsystemy typu A. Nieskomplikowane systemy, których potencjalne uszkodzenia lub modele występowania uszkodzeń są całkowicie znane. Przykłady: prosty włącznik, przekaźnik, tranzystor, proste układy logiczne.
- Systemy, podsystemy typu B. Systemy o większym stopniu skomplikowania, których potencjalne uszkodzenia, modele występowania uszkodzeń nie są całkowicie znane. Zazwyczaj systemy takie dysponują mikroprocesorem (i oprogramowaniem) i/lub programowalnymi, złożonymi układami logicznymi. Przykład: urządzenie sterujące, inteligentny czujnik.

Cechy architektury systemów związanych z bezpieczeństwem

Z punktu widzenia architektury systemu wyróżnia się systemy nieredundantne (odporność na uszkodzenia sprzętu HFT=0) i redundantne dwukanałowe (HFT=1) i trzy-

kanałowe (HFT=2). HFT=N oznacza, że liczba uszkodzeń N+1 może spowodować utratę funkcji bezpieczeństwa.

Wartość graniczna parametru SFF

W zależności od wymaganego poziomu nienaruszalności bezpieczeństwa (SIL) należy w systemach i podsystemach związanych z bezpieczeństwem przestrzegać wartości granicznych parametru SFF (udział uszkodzeń bezpiecznych), zgodnie z poniższą *tabelą*.

Udział uszkodzeń bezpiecznych SFF	Urządzenie typu A Odporność na defekty sprzętu HFT			Urządzenie typu B Odporność na defekty sprzętu HFT		
	N = 0	N = 1	N = 2	N = 0	N = 1	N = 2
< 60%	SIL 1	SIL 2	SIL 3	niedopuszczalne	SIL 1	SIL 2
60% – < 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% – < 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Wartości graniczne SFF [1]

Jeżeli dla podsystemów TS1 do TS3 (patrz architektura odniesienia) określono wartości SIL z uwzględnieniem parametru SFF, wtedy podsystem o najniższym poziomie SIL określa wartość SIL dla całego systemu.

SIL całego sytemu =
= najniższa wartość SIL dla TS1 do TS3

Wartości graniczne parametrów PFD_D/PFH_D

Dla parametrów PFD_D/PFH_D obowiązują wartości graniczne zestawione w *tabeli 2*.

Poziom nienaruszalności bezpieczeństwa SIL	Praca w trybie niskiej intensywności przywołania. Prawdopodobieństwo wystąpienia uszkodzenia funkcji związanej z bezpieczeństwem w razie przywołania	Praca w trybie ciągłego/wysokiego przywołania Prawdopodobieństwo niebezpiecznego uszkodzenia w ciągu godziny
1	$\geq 10^{-5}$ do $< 10^{-4}$	$\geq 10^{-9}$ do $< 10^{-8}$
2	$\geq 10^{-4}$ do $< 10^{-3}$	$\geq 10^{-8}$ do $< 10^{-7}$
3	$\geq 10^{-3}$ do $< 10^{-2}$	$\geq 10^{-7}$ do $< 10^{-6}$
4	$\geq 10^{-2}$ do $< 10^{-1}$	$\geq 10^{-6}$ do $< 10^{-5}$

Wartości graniczne PFD_D i PFH_D [1]

W celu ustalenia możliwego do osiągnięcia poziomu SIL całego systemu przeciętne prawdopodobieństwa uszkodzeń trzech podsystemów TS1 do TS3 dodaje się, a poziom SIL odczytuje się z tabeli.

$$PFD_{D\ \text{Cały system}} = \sum_{i\,=\,TS1}^{TS3} PFD_{Di} \quad \text{lub}$$

$$PFH_{D\ \text{Cały system}} = \sum_{i\,=\,TS1}^{TS3} PFH_{Di}$$

należy przede wszystkim zapanować nad uszkodzeniami przypadkowymi, co z uwagi na dostępność miarodajnej bazy danych dotyczącej prawdopodobieństwa awarii podzespołów [2] wydaje się proste w realizacji.

Jak już wspomniano, w przypadku dwu- lub wielokanałowej architektury instalacji warunkiem uzyskania poziomu SIL 3 jest unikanie uszkodzeń wywoływanych wspólną przyczyną (CCF). Pod względem CCF rozwiązania od 1 do 4 należy ocenić krytycznie z powodu uszkodzeń systematycznych; natomiast rozwiązanie 5 najlepiej wpisuje się w wielokanałową architekturę instalacji.

Zaleta rozwiązania 1 polega na tym, że implementacja funkcji bezpieczeństwa wymaga niewielkiej modyfikacji istniejącego sprzętowego układu sterującego. Ale, jak wynika z wcześniejszych rozważań, separacja funkcji bezpieczeństwa (software) od rozbudowanej funkcjonalności standardowej (software) wiąże się z pracami rozwojowymi w dużym zakresie. Autorzy wskazują na badania i obserwacje zawarte w publikacjach [3, 4] dotyczących zastosowania w praktyce normy IEC EN 61508. Wynika z nich, że istnieje ryzyko, iż skupienie się wyłącznie na definiowanych przez normę parametrach i wartościach granicznych (SFF i PFD lub PFH) pozostawia na dalszym planie wpływ cech architektury systemu. Zaliczamy do nich bezwzględne rozdzielenie sprzętowe standardowej funkcjonalności od funkcji bezpiecznych oraz zwrot do prostych i łatwych do opanowania rozwiązań technicznych (problematyka uszkodzeń wywoływanych wspólną przyczyną CCF!).

Rozwiązania 2 i 3 spełniają wprawdzie podstawowe wymaganie odnoszące się do rozdzielenia funkcji standardowej i bezpiecznej. Opracowanie oprogramowania istotnego dla bezpieczeństwa i związane z tym zapanowanie nad uszkodzeniami systematycznymi oraz znaczny wysiłek zmierzający do uzyskania dużego pokrycia diagnostycznego (wynikający między innymi z rozleglej diagnostyki sprzętowego rozwiązania wykorzystującego mikroprocesor) wymagają poważnych nakładów technicznych i organizacyjnych na prace rozwojowe. Rozwiązanie 4 jest wykluczone ze względu na koszty oraz wspomniane już problemy dotyczące rozdzielenia funkcji bezpieczeństwa od funkcji standardowych, a także na uszkodzenia wywołane wspólną przyczyną.

W danych warunkach ramowych rozwiązanie 5 wydaje się optymalne.

4. Realizacja, implementacja i doświadczenia

Na *ilustr. 7* przedstawiono kompletną strukturę zrealizowanego, bezpiecznego napędu.

Po dwóch latach poświęconych projektowaniu i realizacji zakończono prace rozwojowe nad bezpiecznym napędem uwzględniające koncepcję 5, z którym zintegrowano odpowiedni system zarządzania bezpieczeństwem funkcjonalnym (functional safety management – FSM). Napęd ze zintegrowanym bezpiecznym sterownikiem przeznaczony jest do poziomu SIL 2, w wykonaniu redundantnym może być stosowany również w zastosowaniach wymagających SIL 3. Zostało to zweryfikowane przez jednostkę certyfikacyjną TÜV Nord i potwierdzone odpowiednim certyfikatem SIL.

W trakcie projektowania wielokrotnie weryfikowano konstrukcję i dostosowywano ją do potrzeb klienta. Uderzające było to, że zainteresowanie klienta nie ograniczało się do zapewnienia parametrów zdefiniowanych w normie i uzyskania pożądanego poziomu SIL. Klient okazywał duże zainteresowanie cechami architektury związanymi z techniczną realizacją funkcji bezpieczeństwa w napędzie. W trakcie prac pozytywnie zweryfikowała się decyzja o wyborze rozwiązania 5.

Z informacji zwrotnych uzyskanych od klienta wynikają następujące korzyści dotyczące zastosowania:

- Użycie oddzielnego, bezpiecznego sprzętowego układu sterowania typu A okazało się korzystne podczas realizacji struktury redundantnej, ze względu na wspomniane problemy z uszkodzeniami CCF.
- Ze szczególnym uznaniem spotkała się specjalna konstrukcja, w której dzięki zastosowania dodatkowego bezpiecznego sprzętowego układu logicznego (modułu SIL) zdołano spełnić najbardziej rygorystyczne wymagania dotyczące niezawodności funkcji bezpieczeństwa.

Zastosowanie dodatkowego modułu SIL pozwoliło scalić z funkcją bezpieczeństwa elektromechaniczne mikrołączniki krańcowe oraz kontrolę momentu obrotowego. W porównywalnych systemach sygnały te zazwyczaj się ignoruje, a napęd w razie wywołania funkcji przesterowywuje armaturę w położenie krańcowe, angażując maksymalny moment obrotowy. W omawianym rozwiązaniu wykorzystano standardowe funkcje do ochrony armatury.

Literatura

[1] DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener/ elektrischer/elektronischer/programmierbarer elektronischer Systeme, Teile 1 bis 7. VDE, Beuth

[2] SN 29500: Ausfallraten Bauelemente – Erwartungswerte, Teile 1 bis 15. Siemens AG

[3] *Arndt, V.*, *Kuschnerus, N.*, *Morr, W.*, *Netter, P.*, *Schroers, B.*: Funktionale Sicherheit – ein wichtiges Thema in der NAMUR. Tagungsband 8. AALE Fachkonferenz 2011, ss. 7-15. Oldenbourg Industrieverlag, 2011

[4] *Netter, P.*: Wie die Sicherheit laufen lernte. Entwicklung der funktionalen Sicherheit in Deutschland. atp edition – Automatisierungstechnische Praxis 52 (1-2), ss. 46-55, 2011

*) Dziękujemy firmie **Auma Polska Sp. z o.o.**, Sosnowiec, za pomoc w przygotowaniu artykułu.

*) Mgr inż. *P. Malus* pracuje w firmie Auma na stanowisku menedżera produktu w zakresie napędów elektrycznych ruchów ustawczych armatury przemysłowej i ochrony przeciwwybuchowej. W ramach projektu rozwojowego był w zespole projektowym odpowiedzialny za zdefiniowanie zasadniczych wymagań wobec „bezpiecznego napędu".

Mgr inż. *W. Thomann* zajmuje się w firmie Auma pracami rozwojowymi w dziale elektronicznym. Odpowiedzialny był za opracowanie dodatkowego sprzętowego układu logicznego (modułu SIL) do bezpiecznego napędu. Ponadto przygotowywał dokumentację zgodnie z planem Functional Safety Menagement.

Prof. dr inż. *K.-H. Kayser* jest wykładowcą w Szkole Wyższej w Esslingen (Niemcy), na wydziale mechatronicznym i elektrotechnicznym, na kierunku technika automatyzacji, w oddziale Göppingen. W ramach urlopu naukowego brał udział w pracach nad bezpiecznym napędem.

Tłumaczenie artykułu z „atpedition – Automatisierungstechnische Praxis", z. 9/2014, ss. 48-56.