Zmniejszenie ryzyka poprzez wprowadzenie funkcjonalnego bezpieczeństwa elementów składowych

*Steffen Preg, Heike Bull-Schmeding; Müllheim *)*

Pytania dotyczące bezpieczeństwa nowoczesnych zakładów przemysłowych stają się coraz bardziej istotne, szczególnie w przypadku instalacji o wysokim potencjale zagrożeń w przemyśle naftowym i gazowym, w przemyśle chemicznym lub w elektrowniach.

Do monitorowania procesów, które stanowią zagrożenie dla ludzi i środowiska, są stosowane dzisiaj coraz bardziej nowoczesne systemy zabezpieczeń, reagujące w przypadku wystąpienia awarii. Takie systemy w sytuacji awaryjnej wyłączają instalację i zatrzymują dopływ substancji niebezpiecznych, zapewniają chłodzenie lub otwarcie zaworów w celu odciążenia systemu.

W celu zmniejszenia ryzyka, jakie może występować w instalacjach, systemy te muszą spełniać swoją funkcję bezpieczeństwa w sytuacjach awaryjnych i nie mogą zawieść. Ale co mogą zrobić operatorzy instalacji i producenci urządzeń, aby zapewnić, że zastosowane systemy będą pracować „bezpiecznie" i spełnią niezbędne wymagania? Jak mogą ocenić ryzyko awarii?

Norma dla bezpieczeństwa funkcjonalnego DIN EN 61508 daje tutaj odpowiedź. Jest to pierwszy dokument, który opisuje metody oceny ryzyka awarii w nowoczesnych systemach sterowanych komputerowo oraz określa środki dla zmniejszenia tego ryzyka.

Co to jest bezpieczeństwo funkcjonalne?

Bezpieczeństwo funkcjonalne według normy DIN EN 61508 odnosi się do systemów, które pełnią funkcje bezpieczeństwa, a ich awaria jest poważnym zagrożeniem dla człowieka i środowiska.

W celu osiągnięcia bezpieczeństwa funkcjonalnego, funkcja bezpieczeństwa musi w razie awarii zadbać o to, że instalacja techniczna zostanie doprowadzona do bezpiecznego stanu lub pozostanie w stanie bezpiecznym. Nie chodzi tutaj o podstawowe zagrożenia dla produktu lub instalacji, jakie na przykład stwarzają obracające się części, lecz o zagrożenia, które mogą wynikać z niezadziałania funkcji bezpieczeństwa w danej instalacji.

Celem bezpieczeństwa funkcjonalnego jest zmniejszenie prawdopodobieństwa awarii i dzięki temu także zmniejszenie ryzyka dla ludzi i środowiska naturalnego do dopuszczalnego poziomu.

Ogólnie rzecz biorąc, bezpieczeństwo funkcjonalne jest ważnym wkładem w bezpieczeństwo całego systemu razem z innymi środkami, takimi jak bezpieczeństwo przeciwpożarowe, bezpieczeństwo elektryczne i zabezpieczenie przed wybuchem.

Historia bezpieczeństwa funkcjonalnego

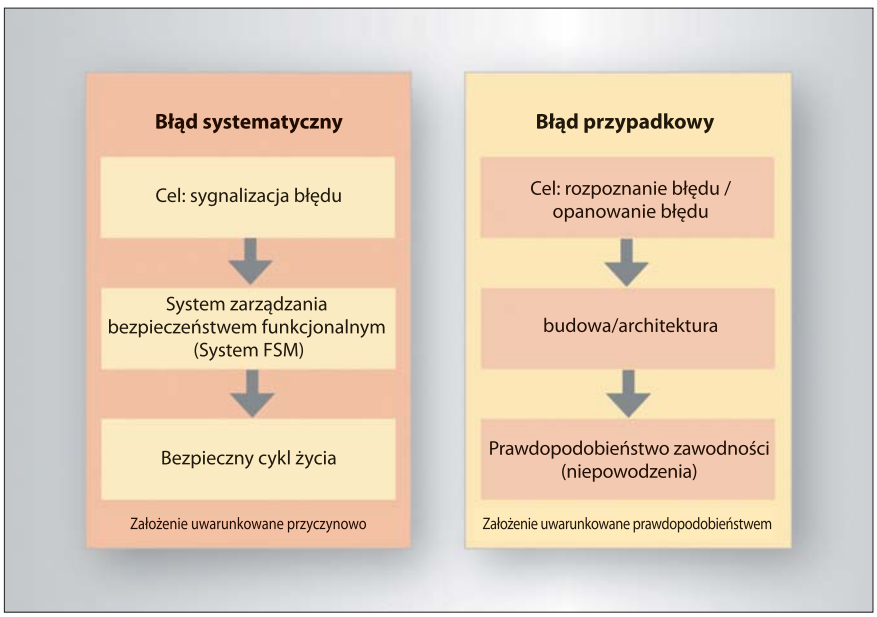
Były wypadki w przemyśle o katastrofalnych skutkach, takie jak wypadek z dioksynami w Seveso w 1976 r. i katastrofa w Bhopalu w Indiach w 1984 roku, które uruchomiły na całym świecie procesy opracowania norm w zakresie bezpieczeństwa instalacji technicznych. Na przykład na poziomie Unii Europejskiej powstała najpierw dyrektywa Seveso I a później Dyrektywa Seveso II 96/82/WE w sprawie opanowywania zagrożeń w razie wypadków z udziałem niebezpiecznych substancji. Przy pomocy tych wytycznych jako najwyższy cel została zapisana ochrona ludzi, środowiska i wartości materialnych.

Ponadto opublikowane zostały szczegółowe przepisy dotyczące instalacji o wysokim potencjale ryzyka.

W celu realizacji tych wytycznych, najpierw pojawiły się krajowe normy dotyczące bezpieczeństwa funkcjonalnego. Od 1998 r. dostępna jest norma IEC 61508, pierwsza obowiązująca norma międzynarodowa. Norma DIN EN 61508 jest odpowiednią normą, obowiązującą od 2002 roku w Niemczech.

Myśl przewodnia bezpieczeństwa funkcjonalnego / norma DIN EN 61508

Norma DIN EN 61508 (lub w sferze międzynarodowej IEC 61508) jest normą obowiązującą na całym świecie odnośnie bezpieczeństwa funkcjonalnego systemów elektrycznych, elektronicznych lub programowalnych systemów



Ilustracja 1. Podział błędów

Tabela 1. Poziomy integralności w zakresie bezpieczeństwa – granice zdarzeń awaryjnych określone dla funkcji bezpieczeństwa, która będzie rozpatrywana w trybie pracy przy niskim współczynniku wymagań

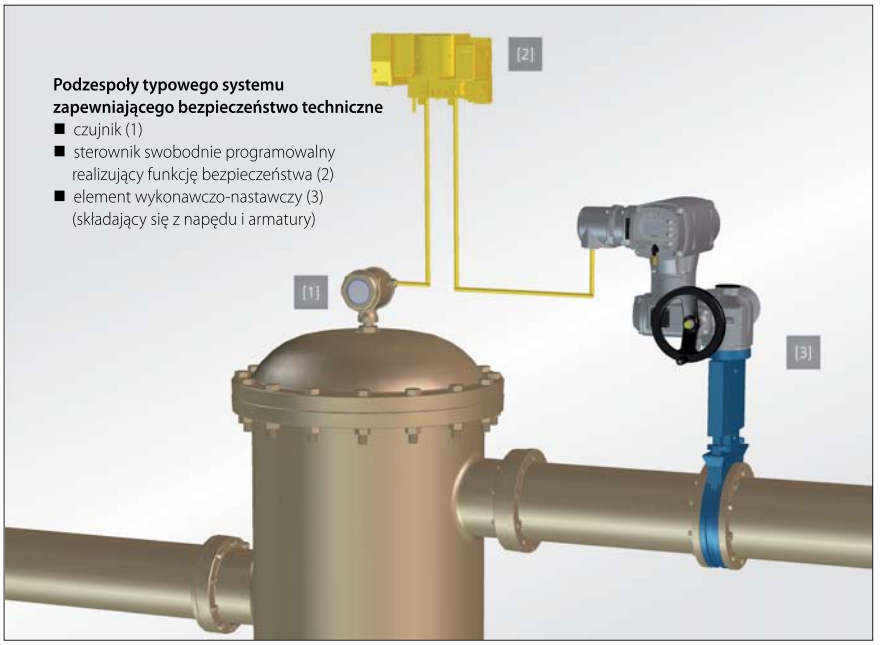
SIL	Średnie prawdopodobieństwo niezadziałania funkcji bezpieczeństwa na żądanie (PFD) (Tryb pracy: niskie wymagania)
SIL 4	10^{-5} do < 10^{-4}
SIL 3	10^{-4} do < 10^{-3}
SIL 2	10^{-3} do < 10^{-2}
SIL 1	10^{-2} do < 10^{-1}

elektronicznych [E / E / PES], realizujących funkcje bezpieczeństwa. Wymagania normy są przenoszone także – tam, gdzie jest to właściwe – na inne, na przykład na mechaniczne podzespoły.

Norma jest skierowana zarówno do projektantów i operatorów instalacji, jak również do producentów urządzeń. Podstawowym założeniem jest przy tym unikanie błędów systematycznych oraz wykrywanie i opanowywanie błędów przypadkowych (*ilustr. 1*).

Co to jest SIL?

SIL jest to pojęcie ściśle związane z bezpieczeństwem funkcjonalnym. SIL oznacza Poziom Integralności w zakresie Bezpieczeństwa (z angielskiego: Safety Integrity Level) i jest miarą zmniejszenia ryzyka związanego z funkcjami bezpieczeństwa.



Ilustracja 2. Bezpieczne otwieranie zaworu bezpieczeństwa

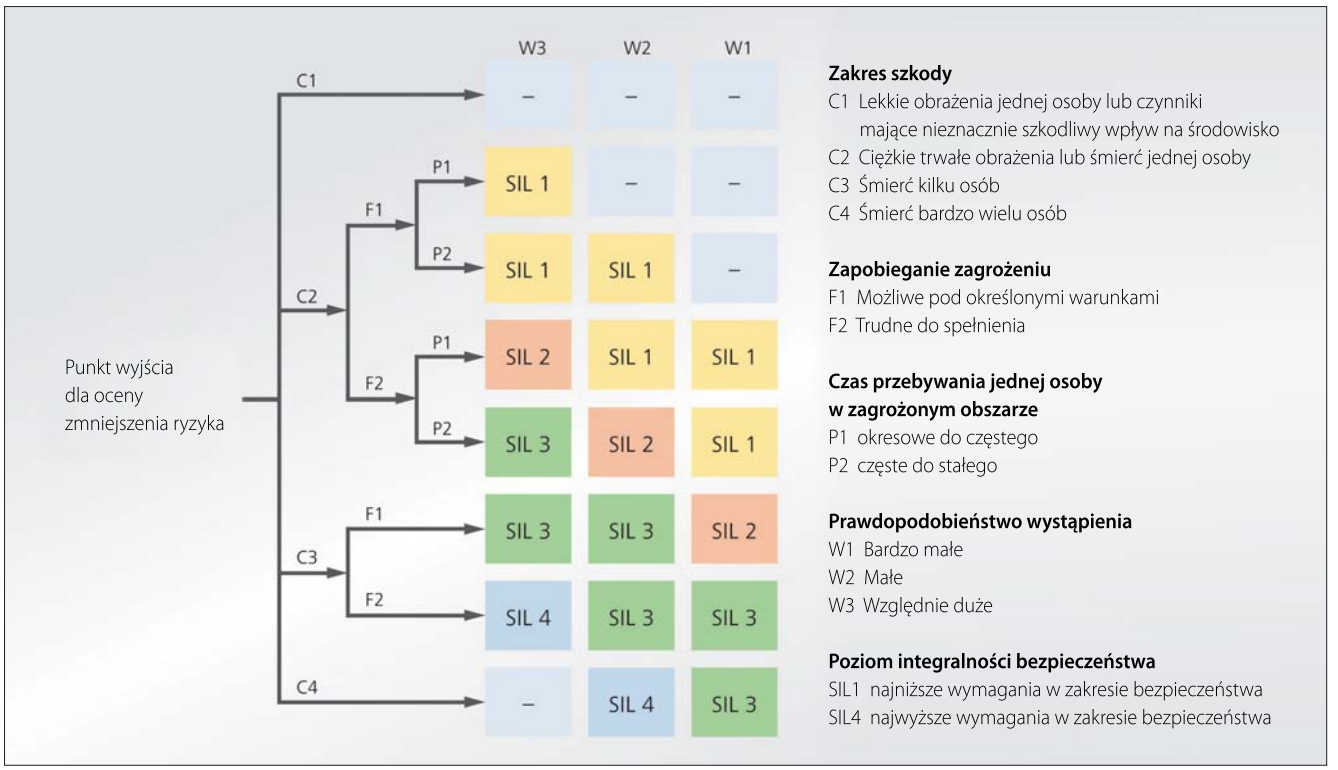
Im większe są zagrożenia pochodzące z procesu lub z instalacji, tym większe są wymagania dotyczące niezawodności funkcji bezpieczeństwa.

Norma DIN EN 61508 definiuje cztery różne poziomy wymagań w zakresie bezpieczeństwa: od SIL 1 do SIL 4. SIL 4 reprezentuje najwyższe wymagania dotyczące bezpieczeństwa, a SIL 1 najniższe. Dla każdego z tych poziomów są określone prawdopodobieństwa awarii (z angielskiego: Probability of a dangerous failure on demand, PFD), których nie może przekroczyć funkcja bezpieczeństwa (*tabela 1*).

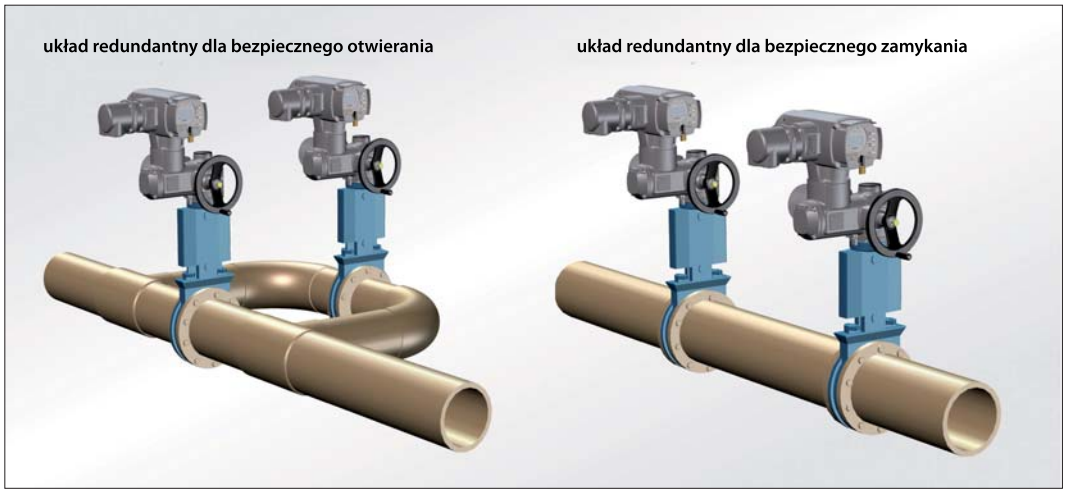
Jaki poziom SIL jest wymagany, można określić na podstawie oceny ryzyka.

Co to jest funkcja bezpieczeństwa?

Funkcje bezpieczeństwa są to środki zabezpieczające, które są aktywowane tylko w przypadku awarii i wówczas zapobiegają, aby nie doszło do powstania



Ilustracja 3. Schemat ryzyka według normy DIN EN 61508



Ilustracja 4. Przykłady układów redundanntnych

szkód u ludzi, w środowisku i mieniu materialnym. Bezpieczeństwo funkcjonalne uzyskuje się, gdy funkcje bezpieczeństwa działają niezawodnie w takiej sytuacji. Typowymi funkcjami bezpieczeństwa są na przykład wyłączenie awaryjne lub kontrola ciśnienia w kotle.

W zakresie armatury mają znaczenie w pierwszym rzędzie następujące funkcje bezpieczeństwa:

- Bezpieczne otwieranie
- Bezpieczne zamykanie
- Bezpieczne zatrzymanie / stop
- Bezpieczna sygnalizacja pozycji końcowej

Przykład: bezpieczne otwieranie zaworu maksymalnego ciśnienia (zaworu bezpieczeństwa). W przypadku kotła pracującego w warunkach zagrożenia wystąpieniem nadciśnienia, jako funkcję bezpieczeństwa przewidziano otwieranie zaworu bezpieczeństwa.

Czujnik sprawdza w sposób ciągły ciśnienie w kotle (*ilustr. 2*). Gdy ciśnienie w układzie wrasta do niedopuszczalnego poziomu, sygnalizuje to czujnik sterownika swobodnie programowalnego realizujący funkcję bezpieczeństwa.

Sterownik swobodnie programowalny realizujący funkcję bezpieczeństwa reaguje na jeden błąd w układzie i wysyła sygnał otwarcia do napędu, aby bezpiecznie zredukować ciśnienie w kotle.

Co to jest system bezpieczeństwa technicznego (SIS)?

Funkcja bezpieczeństwa jest realizowana przez podzespoły tak zwanego systemu bezpieczeństwa technicznego (z angielskiego: Safety Instrumented System, SIS)

Taki układ składa się na ogół z takich elementów składowych, jak czujnik, nadrzędny sterownik nadzorujący bezpieczeństwo i element wykonawczo-nastawczy.

W zakresie armatury element wykonawczo-nastawczy składa się z napędu i zaworu.

Jak można zmniejszyć ryzyko?

Aby zmniejszyć ryzyko, należy najpierw przeanalizować zagrożenia, które stwarza instalacja lub proces. W tym obszarze norma DIN EN 61508 stanowi uznaną metodę oceny ryzyka (np. wykres ryzyka na *ilustr. 3*).

Dzięki zróżnicowanej ocenie bezpieczeństwa technicznego wskazywane są takie procesy, z których w rzeczywistości wynika zagrożenie. Dzięki temu można zastosować konkretne środki zaradcze w celu zmniejszenia ryzyka tylko tam, gdzie są one naprawdę potrzebne.

Zmniejszenie ryzyka można osiągnąć przez zastosowanie różnorodnych metod i rozwiązań technicznych (działania organizacyjne, systemy zabezpieczeń elektrycznych i elektronicznych lub inne rozwiązania techniczne, np. mechaniczne). Należy zauważyć, że osiągnięte zmniejszenie ryzyka wynika z niezawodności urządzeń zabezpieczających.

Określenie poziomu SIL

Poziom integralności w zakresie bezpieczeństwa jest zawsze wymagany dla ogólnej funkcji bezpieczeństwa. Dlatego nie wystarcza tylko rozważyć wartości prawdopodobieństwa awarii dla poszczególnych podzespołów. Zasadą jest określenie najsłabszego ogniwa w łańcuchu bezpieczeństwa, a tym samym urządzenia o najgorszym wskaźniku bezpieczeństwa w systemie w bezpieczeństwa technicznego dla wartości SIL całego systemu.

Poprawa poziomu SIL

Jeżeli z obliczeń wynika, że wybrane podzespoły nie zapewniają wymaganego poziomu bezpieczeństwa (SIL), to można go uzyskać przez przez zastosowanie dodatkowych środków, takich jak diagnostyka lub redundancja.

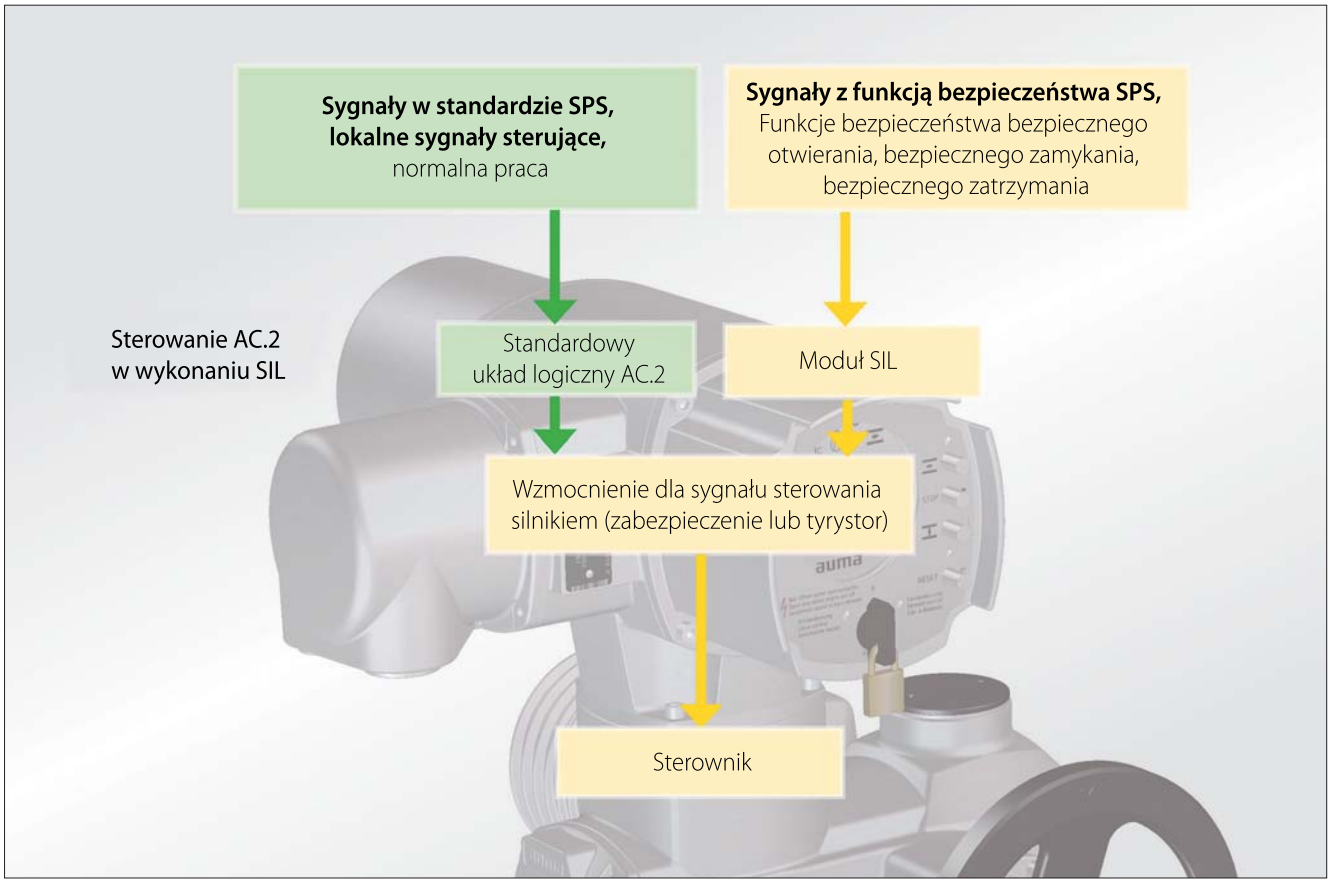
Diagnostyka przy pomocy testu częściowego skoku zaworu (PVST). Za pomocą testu częściowego skoku zaworu sprawdza się w regularnych odstępach czasu sprawność działania urządzenia. Napęd lub zawór pokonuje określony skok w kierunku otwierania, po czym jest ponownie zamykany. W ten sposób sprawdza się, czy napęd i zawór rzeczywiście się poruszają.

Test częściowego skoku zaworu jest uznanym sposobem na zwiększenie dyspozycyjności poszczególnych elementów realizujących funkcję bezpieczeństwa. Dzięki diagnostyce prewencyjnej można wykluczyć pewne błędy mające wpływ na poziom bezpieczeńswta; zmniejsza się też prawdopodobieństwo awarii.

Redundancja. Również dzięki redundancji w systemie można zwiększyć prawdopodobieństwo realizacji funkcji bezpieczeństwa w sytuacji awaryjnej.

Właśnie dlatego dwa lub więcej urządzeń systemu bezpieczeństwa technicznego pracuje w układzie redundantnym. Zależnie od wymagań bezpieczeństwa przydatne są różne konfiguracje MooN („M z N"). W przypadku konfiguracji 1oo2 („jeden z dwóch") wystarczy na przykład jedno z dwóch urządzeń, aby zrealizować funkcję bezpieczeństwa. Jak wygląda konkretny układ urządzeń zależy również od wymaganej funkcji bezpieczeństwa.

Jest to wyraźnie widoczne na *ilustr. 4* przedstawiającej bezpieczne otwieranie i bezpieczne zamykanie zaworu. Redundantna struktura zwiększa tolerancję błędu sprzętowego i dzięki temu również bezpieczeństwo. Należy przy tym brać pod uwagę typowe przyczyny błędu.



Ilustracja 5. Budowa systemu sterowania na podstawie sterowania AC.2 w wykonaniu SIL

SIL u producenta napędu

Aby przekazać uzasadnioną i zrozumiałą ocenę poziomu SIL napędów firmy **AUMA**, określono współczynniki dotyczące bezpieczeństwa.

Pierwsze działania w odniesieniu do „SIL" firma AUMA podjęła określając współczynniki bezpieczeństwa, razem z firmą **EXIDA**, na podstawie oceny urządzeń. Przeprowadzono w tym celu analizę przyczyn, skutków i diagnostyki usterki (FMEDA) zgodnie z normą DIN EN 61508.

Na podstawie danych rodzajowych uzyskano wskaźniki awaryjności poszczególnych elementów elektrycznych, które są zestawione w specjalnych bazach danych, tak zwanych „Reliability data books" . Przykładami takich baz danych są norma SIEMENS SN29500, czy podręcznik firmy EXIDA.

Do oceny podzespołów mechanicznych wykorzystuje się dane zwrotne firmy AUMA. Ponadto dla określenia mechanicznych wskaźników awarii oceniane i analizowane są komunikaty zwrotne gromadzone w okresie gwarancji.

Dzisiaj firma AUMA posiada certyfikowane urządzenia, które zostały w pełni ocenione pod względem zgodności z normą DIN EN 61508 i uzyskały stosowny certyfikat. Ponadto we wszystkich fazach cyklu życia produktu rozpatrywane są nie tylko przypadkowe, ale także systematyczne błędy, począwszy od określenia specyfikacji aż do wycofania urządzenia z eksploatacji. Jednym z takich produktów jest sterownik siłownika AC .2 w wykonaniu SIL, dla którego uzyskano certyfikat od **TÜV Nord**.

Celem było połączenie nowych trendów w technice automatyzacji, takich jak na przykład zarządzanie zasobami (Asset Management), które wymagają coraz bardziej inteligentnych urządzeń obiektowych wyposażonych w rozbudowane funkcje diagnostyczne, z wymogami poziomu SIL 2.

Funkcje te są oparte na oprogramowaniu, dotyczy to również napędów firmy AUMA ze sterownikiem mikroprocesorowym AC. Norma dla bezpieczeństwa funkcjonalnego DIN EN 61508 definiuje takie urządzenia jak urządzenia typu B, przed którymi postawiono większe wymagania dla uzyskania wysokiego poziomu SIL niż dla urządzeń bez oprogramowania (typ A) na urządzenia pracujące bez oprogramowania (urządzenia typu A).

Dzięki modułowi SIL zabudowanemu w sterowniku AC .2 w wykonaniu SIL (*ilustr. 5*) podwyższony zostaje poziom SIL inteligentnych napędów firmy AUMA. Moduł zabudowany w sterowniku AC zawiera tylko stosunkowo proste elementy, takie jak tranzystory, rezystory, kondensatory i bramki logiczne, procesy przewidziane do realizacji w przypadku awarii są oprzewodowane na stałe i związku z tym są niezależne od oprogramowania. W razie potrzeby moduł przejmuje sterowanie napędem. Przez to system napędowy zmienia się w urządzenie typu A, dzięki któremu można osiągnąć wyższy poziom SIL dla sterowania AC. Otrzymane w testach współczynniki bezpieczeństwa umożliwiają stosowanie w układach wymagających poziomu SIL 2, w wykonaniu redundantnym (1oo2) oraz poziomu SIL 3.

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

*) *Steffen Preg* – AUMA Riester GmbH & Co. KG, Müllheim (Niemcy); *Heike Bull-Schmeding* – AUMA Riester GmbH & Co. KG, Müllheim (Niemcy).