SIL – wskaźniki i certyfikaty – wymagania i pułapki

*Jörg Isenberg – Müllheim *)*

Bezpieczeństwo funkcjonalne – określane często skrótowcem „SIL” – zyskuje coraz bardziej na znaczeniu w projektowaniu, tworzeniu i eksploatacji instalacji procesowych krytycznych pod względem bezpieczeństwa. Podstawą oceny przydatności elementów składowych przeznaczonych do zastosowania w systemach bezpieczeństwa jest norma IEC 61508. Doświadczenia wynikające z praktyki dowodzą jednak, że interpretacja informacji zawartych w certyfikatach często budzi wątpliwości.

W artykule opisano kryteria, które należy wziąć pod uwagę podczas przyporządkowywania elementów składowych i systemów do określonych poziomów SIL. W warunkach praktycznych nie zawsze są one jednak uwzględniane w całości. Stosuje się uproszczone metody, które pozwalają trafnie dobrać komponenty na podstawie mniejszego zakresu danych z certyfikatów. Dowiedziemy, że „odpowiedni dla SIL 2” niekoniecznie musi oznaczać „odpowiedni dla SIL 2”.

Systemy bezpieczeństwa charakteryzujące się bezpieczeństwem funkcjonalnym

W przemyśle procesowym często występują instalacje, które w przypadku awarii sterowania procesem stanowią poważne zagrożenia dla ludzi i środowiska. Zgodnie z dzisiejszymi standardami technicznymi w tego rodzaju instalacjach stosuje się tak zwane przyrządowe systemy bezpieczeństwa (ang. *Safety Instrumented System* – SIS). Systemy te rozpoznają krytyczne zdarzenia i wprowadzają proces w bezpieczny stan lub utrzymują go w nim.

Pierwszą, podstawową wiążącą regulacją o zasięgu międzynarodowym dla tego rodzaju systemów bezpieczeństwa była opublikowana w 1998 roku norma IEC 61508, której obowiązujące obecnie wydanie pojawiło się w 2010 roku. Szczegółowe wymagania dla przemysłu procesowego precyzujące zapisy PN-EN 61508 zawarto w normie PN-EN 61511.

Aby umożliwić w pełni automatyczną reakcję systemów, SIS składają się zazwyczaj z co najmniej jednego czujnika, jednego układu logicznego i organu wykonawczego, na przykład napędu z armaturą (*ilustr. 1*).

Na podstawie analizy zagrożenia i ryzyka dla każdego systemu SIS obowiązkowo określa się poziom nienaruszalności bezpieczeństwa, tak zwany SIL (ang. *Safety Integrity Level*). Istnieją cztery jego poziomy, przy czym SIL 1 oznacza najmniejsze, a SIL 4 największe ograniczenie ryzyka.

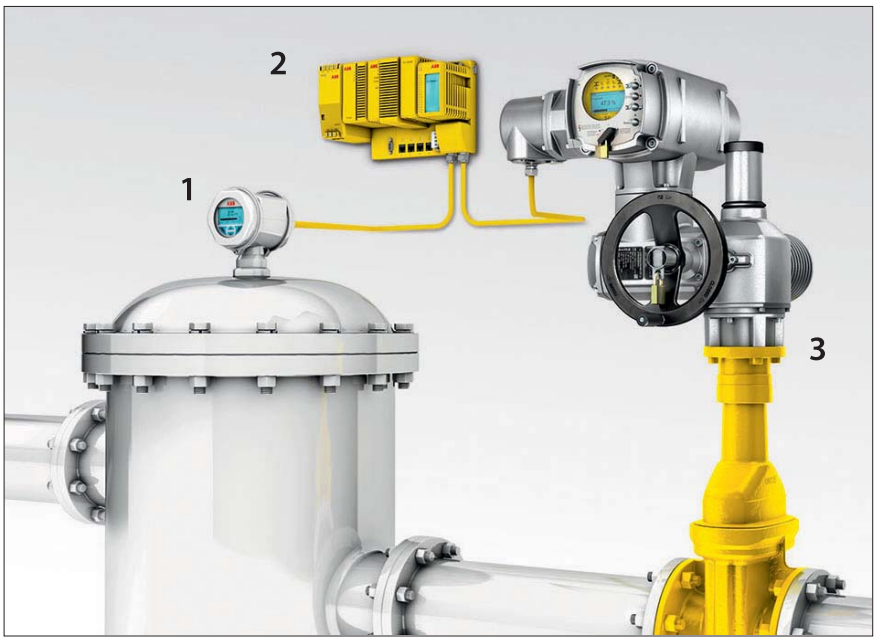
Aby przyrządowy system bezpieczeństwa zakwalifikować do określonego poziomu SIL, operator musi spełnić wiele wymagań, między innymi na etapie planowania, realizacji, eksploatacji i konserwacji systemu. Niektóre wytyczne normy IEC 61508 wymagają zastosowania specjalnych, zatwierdzonych elementów składowych, które muszą posiadać określone techniczne informacje dodatkowe. Dane te określa zazwyczaj producent elementu w ramach zatwierdzania produktu zgodnie z normą PN-EN 61508 i udostępnia w formie deklaracji producenta lub certyfikatu wydanego przez jednostkę kontrolną.

Podczas projektowania systemu SIS istotne jest właściwe odczytywanie owych deklaracji producenta lub certyfikatów i unikanie błędnych interpretacji.

Kwalifikowanie elementów przeznaczonych dla przyrządowych systemów bezpieczeństwa

Ważnym kryterium przydatności elementu w systemie SIS jest zgodność z określonymi w specyfikacji warunkami zastosowania. Oprócz czynników środowiskowych, takich jak temperatura, wilgotność, ciśnienie i zanieczyszczenie należy uwzględnić również oddziaływanie medium oraz niezbędne dla armatury i danego zastosowania warunki wyłączenia napędu. Zwłaszcza w zakresie warunków wyłączenia nie wszystkie napędy oferują tę samą możliwość wyboru jak w wypadku funkcji eksploatacyjnych, co często może prowadzić do nieprawidłowego doboru.

Podczas dobierania elementów niekiedy w pierwszym rzędzie zwraca się uwagę na przyporządkowanie do poziomu SIL. W razie wątpliwości od urządzenia optymalnie dopasowanego



Ilustracja 1. Przykład przyrządowego systemu bezpieczeństwa (SIS) składającego się z czujnika (1), układu logicznego (2) i organu wykonawczego (3), w tym wypadku napędu z armaturą

Ilustracja 2. Przykład certyfikatu, w którym wyeksponowano przydatność urządzenia dla poziomu SIL 3

Tabela 1. Przykład wyznaczenia poziomu SIL funkcji bezpieczeństwa będącej elementem systemu SIS

Przypisanie poziomu SIL w odniesieniu do	Maksymalna wartość SIL możliwa do uzyskania
Przydatności systemowej	SIL 3
Ograniczenia architektury	SIL 1
Prawdopodobieństwa uszkodzenia	SIL 2
Końcowa klasyfikacja SIL	**SIL 1**

do warunków procesu i otoczenia przypisanego do poziomu SIL 1 można oczekiwać większej redukcji ryzyka niż w przypadku produktu zgodnego z SIL 3, ale nieodpowiadającego spodziewanym warunkom środowiskowym.

Jak oceniać certyfikaty?

Gdy wyjaśnimy kwestię przydatności elementu dla danego zastosowania, można przejść do oceny z uwzględnieniem wymagań bezpieczeństwa funkcjonalnego.

W wielu certyfikatach na stronie tytułowej zawarta jest informacja o przyporządkowaniu urządzenia do konkretnego poziomu SIL. Przykład przedstawiono na *ilustr. 2*. Jednak co oznacza logo „Certified SIL 3 capable?" Zazwyczaj nie oznacza to, że certyfikowany element bez dodatkowej weryfikacji może zostać zastosowany w systemach SIL 3. Z reguły konieczne są dodatkowe działania, żeby osiągnąć wymieniony poziom SIL. Jedyną możliwością uzyskania większej jednoznaczności w tym zakresie jest zweryfikowanie szczegółowych informacji zawartych w certyfikacie.

Trzy zasadnicze wymagania normy PN-EN 61508. Ocena i klasyfikacja przyrządowego systemu bezpieczeństwa zgodnie z normą PN-EN 61508 następuje zasadniczo na podstawie trzech kryteriów:

- przydatność systemowa,
- ograniczenia architektury,
- prawdopodobieństwo uszkodzenia na przywołanie (PFD).

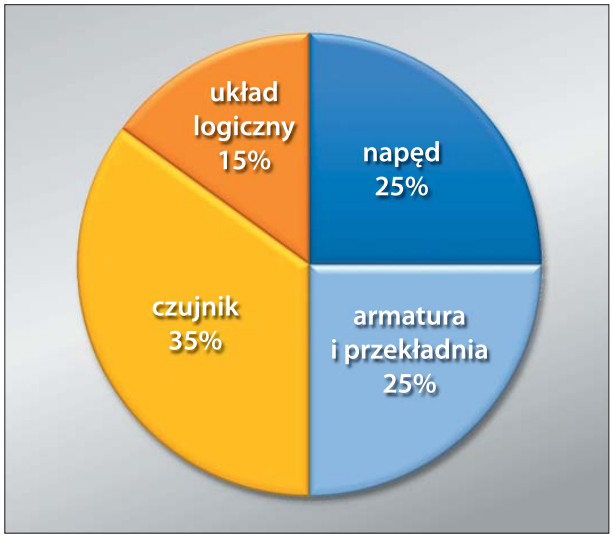
Należy zaznaczyć, że osiągnięty poziom SIL jest zawsze minimalną wartością poszczególnych ocen (*tabela 1*).

Przydatność systemowa. W wielu certyfikatach jest podana wprost, często jako „Systematic Capability" lub „SC" (patrz *ilustr. 2*). Niekiedy nie można jej odczytać bezpośrednio. Sformułowania takie jak: „jest odpowiedni dla aplikacji związanych z bezpieczeństwem do poziomu SIL 3" (patrz *ilustr. 5*) mogą wskazywać na przydatność systemową. Czasem informacja o przydatności systemowej umieszczana jest na wyeksponowanym miejscu, w rezultacie czego po pobieżnym przeczytaniu dokumentu możemy odnieść wrażenie, że wartość ta oznacza ogólną przydatność urządzenia.

Ograniczenia architektury. Norma IEC 61508-2:2010 określa dwie dopuszczalne drogi określenia maksymalnego dopuszczalnego poziomu SIL na podstawie ograniczeń wynikających z architektury systemowej:

- Droga 1H przewiduje klasyfikację według parametrów udział uszkodzeń bezpiecznych (*safe failure fraction* – SFF) oraz odporność na defekty sprzętu (*hardware fault tolerance* – HFT).
- Droga 2H umożliwia uproszczoną klasyfikację na podstawie parametru HFT. W tym wypadku należy spełnić jednak dodatkowe wymagania, które związane są z obszernymi doświadczeniami z eksploatacji danego urządzenia. Z drogi 2H wolno skorzystać tylko wtedy, gdy wymagania te są spełnione.

Szczegółowe informacje na temat ograniczeń architektury rzadko są umieszczane w certyfikatach. Czasem można spotkać dokładne informacje, jak choćby „Type A Element SIL 2 @ HFT=0; Route 2H". Niekiedy pojawia się na przykład wzmianka „SIL 2 can be reached in 1oo1 architecture" („SIL 2



Ilustracja 3. Zalecany podział maksymalnego prawdopodobieństwa uszkodzenia na przywołanie (PFDavg) przypadający na poszczególne podsystemy w ramach SIS

można osiągnąć w architekturze 1oo1"). Zazwyczaj oznacza to, że zarówno według ograniczeń architektury, jak i parametru PFD przydatność dla poziomu SIL 2 można osiągnąć bez redundancji. Krytycznie należy oceniać certyfikaty, które zawierają na przykład sformułowanie: „Architectural Constraints must be verified for each application" („ograniczenia architektury należy zweryfikować dla każdej aplikacji") (patrz *ilustr. 2*). W takiej sytuacji jedynym rozwiązaniem jest wykonanie ponownych obliczeń we własnym zakresie.

Należy zaznaczyć, że ograniczenia architektury trzeba rozpatrywać, biorąc pod uwagę zespoły, a nie poszczególne elementy składowe. Jeżeli już pojedynczy element nie spełnia wymagań, inne komponenty wchodzące w skład zespołu – o ile w ogóle takie występują – muszą być nieproporcjonalnie dobre, żeby wyrównać ten niedobór.

Prawdopodobieństwo uszkodzenia na przywołanie.

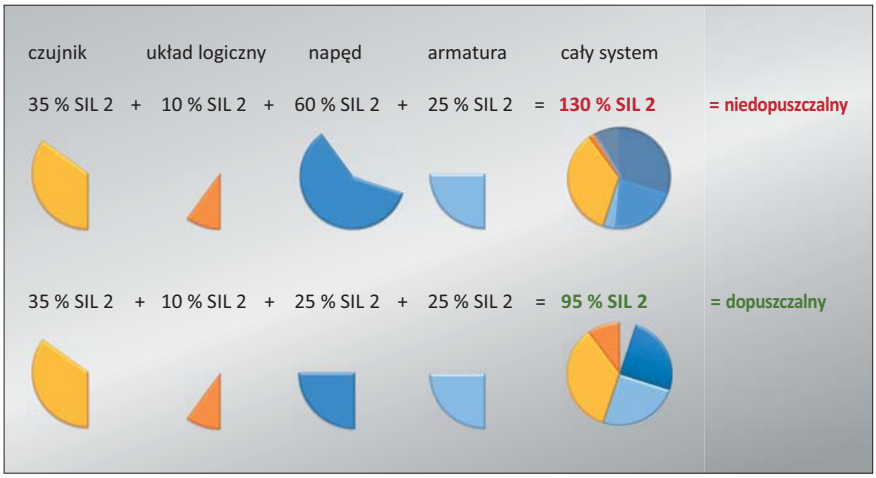
Funkcje bezpieczeństwa o niskiej intensywności przywołania nie mogą przekraczać – określonego w normie PN-EN 61508-1 – średniego prawdopodobieństwa uszkodzenia na przywołanie (PFD_{avg}) dla wymaganego poziomu SIL. Ponieważ ta wartość maksymalna dotyczy całej funkcji bezpieczeństwa, poszczególne elementy nie powinny jej całkowicie wyczerpywać. Jako powszechny (jednak nie wynikający z norm) podział w branży armatury przemysłowej przyjęto wartości przedstawione na *ilustr. 3*.

Na *ilustr. 4* pokazany jest podział maksymalnego dopuszczalnego parametru PFD_{avg} przyrządowego systemu bezpieczeństwa. Również w sytuacji gdy jeden z elementów wykracza poza zalecaną wartość maksymalną, może to skutkować niedopuszczalnie dużą wartością PFD_{avg} całego systemu.

Ponadto należy wziąć pod uwagę, że wartości PFD podane w deklaracjach producenta mogą być tylko wartościami orientacyjnymi, ponieważ ich obliczanie uwzględnia założenia zależne od zarządzania instalacją.

Kolejne kryteria. Aby ocenić przydatność komponentu, oprócz wymienionych powyżej głównych kryteriów należy uwzględnić także inne czynniki:

Aktualnie obowiązujące normy. W 2010 roku opublikowano nową wersję normy PN-EN 61508, która zwłaszcza pod względem oceny parametru udział uszkodzeń bezpiecznych (SFF) jest bardziej rygorystyczna niż pierwsze wydanie. Mogą z tego wynikać znaczne



Ilustracja 4. Przykład podziału maksymalnej dopuszczalnej wartości PFDavg na elementy systemu SIS

różnice w ocenie ograniczeń architektury. Przykładem jest napęd niepełnoobrotowy SQ .2 firmy **AUMA** ze sterownikiem AM. Zgodnie z normą PN-EN 61508, wyd. 2, napęd został oceniony według kryterium ograniczeń architektury jako „odpowiedni dla SIL 2" (*ilustr. 5*). Dla porównania w *tabeli 2* przedstawiono ocenę wynikającą z pierwszego wydania normy. Ze względu na lepszy parametr SFF uzyskujemy ocenę „odpowiedni dla SIL 3" w kontekście ograniczeń architektury.

Tryb pracy. Norma PN-EN 61508 rozróżnia tryby pracy charakteryzujące się małym, dużym natężeniem przywołania oraz przywołaniem ciągłym. W przemyśle procesowym zazwyczaj istotny jest tryb pracy z małym natężeniem przywołania (ang. low demand mode), co odpowiada maksymalnie jednemu przywołaniu funkcji bezpieczeństwa w ciągu roku.

Przy małym natężeniu przywołania intensywność wystąpienia uszkodzenia funkcji w razie żądania wynika głównie ze starzenia się, natomiast w warunkach wysokiego zapotrzebowania przyczyną jest z reguły zużycie. Wobec tego zazwyczaj uzyskuje się różne intensywności wystąpienia uszkodzenia funkcji. Dlatego też certyfikaty oraz intensywność wystąpienia uszkodzenia funkcji mogą być odnoszone tylko do trybu pracy, dla którego zostały wyznaczone.

Funkcja bezpieczeństwa. Każdy certyfikat oraz każdy projekt systemu SIS musi zawierać jednoznaczną definicję, jaką funkcję lub funkcje bezpieczeństwa ma wykonywać system SIS lub da-

Tabela 2. Porównanie oceny napędu niepełnoobrotowego SQ.2 ze sterownikiem AM według 1. i 2. wydania normy PN-EN 61508

SQ.2 + AM [V2]	S[1] [FIT][2]	DD[3] [FIT][2]	DU[4] [FIT][2]	SFF[5] [FIT][2]	ograniczenia architektury
IEC 61508, wyd. 2.	21	667	104	86,5%	**przydatność dla SIL 2**
IEC 61508, wyd. 1.	607	667	104	92,4%	**przydatność dla SIL 3**

[1] safe failures – uszkodzenia bezpieczne
[2] failures in time – uszkodzeń w jednostce czasu
[3] dangerous detected – wykryte uszkodzenia niebezpieczne
[4] dangerous undetected – niewykryte uszkodzenia niebezpieczne
[5] safe failure fraction – udział uszkodzeń bezpiecznych

Tabela 3. Intensywność wystąpienia uszkodzenia zamieszczona na drugiej stronie certyfikatu przedstawionego na ilustr. 2

	SD[1]	SU[2]	DD[3]	DU[4]	SFF[5]
Bezpieczne otwieranie/zamykanie bez PVST	404 FIT[6]	185 FIT[6]	1920 FIT[6]	974 FIT[6]	–
Bezpieczne otwieranie/zamykanie z PVST	461 FIT[6]	185 FIT[6]	2510 FIT[6]	388 FIT[6]	–

[1] safe detected – wykryte uszkodzenia bezpieczne
[2] safe undetected – niewykryte uszkodzenia bezpieczne
[3] dangerou sdetected – wykryte uszkodzenia niebezpieczne
[4] dangerous undetected – niewykryte uszkodzenia niebezpieczne
[5] safe failure fraction – udział uszkodzeń bezpiecznych
[6] failures in time – uszkodzeń w jednostce czasu

DAkkS Deutsche Akkreditierungsstelle D-ZE-11074-01-00

TÜV NORD

Certificate

No. SEBS-A.150445/14 V1.0

TÜV NORD Systems GmbH & Co. KG hereby certifies

AUMA Riester GmbH & Co. KG

Aumastraße 1
79379 Müllheim, Germany

that the

electric actuator system with the actuators SA(R)07.1 – SA(R)16.1/ SA(R)ExC 07.1 – SA(R)ExC16.1, SA(R)07.2 – SA(R)16.2/ SA(R)Ex07.2 – SA(R)Ex16.2 and SQ(R)05.2- SQ(R)14.2/ SQ(R)Ex05.2- SQ(R)Ex14.2 with the actuator controls AC01.2/ACExC01.2 in SIL version

with the safety functions „Safe Emergency Shut Down (ESD)" and „Safe Stop" is capable for safety related applications up to SIL 3 and meets the requirements listed in the following standard.

DIN EN 61508: 2011 part 1 and part 2

SIL 2 can be reached in a 1oo1 architecture and SIL 3 in a 1oo2 architecture.

Base of certification is the report SEBS-A.150445/14TB in the valid version.

This certificate entitles the holder to use the pictured safety approved mark.

Valid until: 2020-01-28
File reference: 8111837863

Hamburg, 2015-01-29

Bianca Pfuff

Certification Body SEECERT
TÜV NORD Systems GmbH & Co. KG
Große Bahnstraße 31, 22525 Hamburg, Germany

TÜV NORD Safety Approved Electric Actuator

DIN EN 61508-1;-2: 2011 capable up to SIL 3

Ilustracja 5. Certyfikat napędów ze sterownikiem AC.2 SIL firmy AUMA potwierdzający zgodność z normą PN-EN 61508 w wersji z 2011 roku, co odpowiada wydaniu drugiemu

ny element. Wskaźniki bezpieczeństwa dla różnych funkcji bezpieczeństwa mogą się znacznie różnić, wobec czego można je stosować tylko dla wskazanej funkcji.

Interpretacja certyfikatu – przykład zaczerpnięty z praktyki

Przykład przedstawiony na *ilustr. 2* wyraźnie wskazuje, gdzie mogą wystąpić nieporozumienia w interpretacji certyfikatu. Oceniany element reklamowany jest jako „Certified SIL 3 capable". Podkreśla się również, że przydatność systemowa jest odpowiednia dla poziomu SIL 3.

Jednak czy ten element faktycznie może pracować w zastosowaniach SIL 3?

Certyfikat odpowiada normie „PN-EN 61508:2010", co oznacza, że mamy do czynienia z oceną według najnowszego wydania PN-EN 61508. Na drugiej stronie certyfikatu scharakteryzowano funkcję bezpieczeństwa jako niezawodne zamykanie/otwieranie z testem częściowego skoku zaworu (PVST) lub bez niego. Trybu pracy oraz zasadniczej przydatności dla planowanego zastosowania nie można bezpośrednio odczytać z certyfikatu – jak często ma to miejsce. Pod tym kątem należy zweryfikować dodatkową dokumentację techniczną urządzenia.

Jeżeli na podstawie tych danych stwierdzimy zasadniczą przydatność dla planowanej funkcji bezpieczeństwa, należy zweryfikować trzy główne kryteria wynikające z normy IEC 61508.

Przydatność systemowa jest bezpośrednio podana jako „SIL 3 capable".

Na temat **ograniczeń architektury** i parametru **PFD_{avg}** stwierdzono tylko, że muszą zostać zweryfikowane oddzielnie dla każdego zastosowania. A zatem użytkownik musi przeprowadzić ocenę elementu we własnym zakresie. Ułatwia to zamieszczone na drugiej stronie zestawienie intensywności wystąpienia uszkodzenia, które przedstawiono w *tabeli 3*.

Ograniczenia architektury wynikają z udziału uszkodzeń bezpiecznych (SFF), odporności na defekty sprzętu (HFT) i typu rozpatrywanego elementu. Certyfikat widoczny na *ilustr. 2* informuje, że mamy do czynienia z elementem typu B, czyli urządzeniem złożonym. Wartość HFT wynosi 0, SFF możemy obliczyć na podstawie *tabeli 3*, otrzymując $SFF_{bez\ PVST} = 72\%$ oraz $SFF_{z\ PVST} = 89\%$. Według *tabeli 3* norma PN-EN 61508-2 na poziomie elementu określa w obu przypadkach przydatność dla poziomu SIL 1, biorąc pod uwagę ograniczenia architektury. Zakładając obecność testu częściowego skoku zaworu (PVST) oraz zastosowanie dodatkowych, ponadprzeciętnie dobrych elementów składowych w obrębie tego samego zespołu, można pomyśleć o przydatności dla poziomu SIL 2, jednak inne składowe muszą skompensować niedobory ocenianego elementu.

Aby ocenić kwalifikację z uwzględnieniem parametru PFD_{avg}, należy sformułować założenia związane z zarządzaniem eksploatacją. W podręczniku dotyczącym bezpieczeństwa rozpatrywanego elementu dla typowych scenariuszy udostępniono następujące wartości: $PFD_{avg\ bez\ PVST} = 5{,}24 \cdot 10^{-3}$ i $PFD_{avg\ z\ PVST} = 2{,}96 \cdot 10^{-3}$. Stanowi to około 52% lub około 30% maksymalnie dopuszczalnego PFD_{avg} dla całego systemu na poziomie SIL 2. A zatem przy dokonanych założeniach przydatność komponentu dla SIL 2 na podstawie parametru PFD jest wątpliwa bez testu częściowego skoku zaworu, ponieważ dla innych elementów systemu zostawia się zbyt mały udział w całkowitym dopuszczalnym prawdopodobieństwie uszkodzenia. Zakładając obecność PVST, umowna granica 25% dla napędów jest wprawdzie przekroczona, ale odpowiednio dobrej jakości pozostałe elementy systemu umożliwiają zastosowanie na poziomie SIL 2 – biorąc pod uwagę kryterium PFD.

Ponieważ uzyskany poziom SIL jest zawsze najniższą wartością spośród określonych dla trzech kryteriów, można przyjąć, że elementy w systemach pozbawionych redundancji kwalifikują się tylko do poziomu SIL 1 (bez PVST) i ewentualnie do SIL 2 (z PVST). W systemach redundantnych możliwe wydaje się zastosowanie do poziomu SIL 2 (bez PVST) lub do SIL 3 (z PVST).

W podsumowaniu można stwierdzić, że podczas projektowania systemów bezpieczeństwa certyfikaty SIL poszczególnych elementów należy poddać dokładnej weryfikacji, aby można było zagwarantować uzyskanie wymaganego poziomu SIL.

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

*) Dr *Jörg Isenberg* – AUMA Riester GmbH Co. KG, Müllheim (Niemcy).

Tłumaczenie artykułu z „Industriearmaturen", z. 4/2015, ss. 48-52.