Bezpieczeństwo funkcjonalne: normy, analizy i sposoby jego uzyskiwania w platformach mikrokontrolerowych

W latach ’80 XX wieku zaczęło rosnąć wykorzystanie elektronicznych komponentów programowalnych, takich jak mikrokontrolery (MCU) i mikroprocesory, w przemysłowych systemach sterowania. Międzynarodowa Komisja Elektrotechniczna (IEC) powołała wówczas specjalne grupy badawcze. Miały one na celu zbadanie bezpieczeństwa funkcjonalnego tych systemów i opracowania wytycznych dotyczących rozwoju bezpiecznych urządzeń je wykorzystujących. Od tego czasu zgodność z normami bezpieczeństwa funkcjonalnego stała się wymogiem dla twórców urządzeń elektronicznych m.in. w przemyśle motoryzacyjnym czy w zastosowaniach przemysłowych.

Termin „bezpieczeństwo funkcjonalne” pojawił się w dokumentach stworzonych przez Podkomitet 65A IEC w 1985 roku. Urząd Dozoru Technicznego (UDT) definiuje bezpieczeństwo funkcjonalne, jako „ogólne podejście do wszystkich działań w cyklu życia bezpieczeństwa systemów zawierających elektryczne i/lub elektroniczne i/lub programowalne elektroniczne elementy składowe”. W ogólności zasady te mówią o sposobie projektowania urządzeń elektronicznych, by były one bezpieczne dla użytkownika. Jest to szczególnie ważne np. w systemach zabezpieczających w przemyśle, motoryzacji, lotnictwie czy kolei.

Pierwszą normą przeznaczoną do stosowania w szerokiej gamie systemów przemysłowych była **IEC 61508**, która została opublikowana w 1998 roku. W 2011 roku ukazała się motoryzacyjna norma bezpieczeństwa funkcjonalnego **ISO 26262**. Celem obu norm jest ustalenie wymagań, które zmniejszają potencjalne ryzyko obrażeń fizycznych czy uszczerbku na zdrowiu ludzi z powodu awarii danego produktu. Normy te wymagają wdrożenia ścisłego procesu rozwoju produktu, przeprowadzenia wstępnej analizy zagrożeń i ryzyka oraz wdrożenia zabiegów zmniejszających ryzyko, związane z produktem. Wykorzystuje się je zarówno w projekcie sprzętu, jak i jego oprogramowania. Normy te współdzielą wiele elementów, mają bardzo zbliżony cykl rozwoju produktu i wiele takich samych rozwiązań wspierających projektowanie. Istnieje jednak wiele innych, branżowych norm bezpieczeństwa, opierających się na tych dwóch normach. Są one zazwyczaj zgodne z **IEC 61508**, uzupełniając ją o dodatkowe wymagania architektoniczne czy obecność autotestu dla systemu w konkretnych zastosowaniach. W **tabeli 1** zebrano podsumowanie różnych międzynarodowych norm bezpieczeństwa funkcjonalnego i ich związki z normą **IEC 61508**.

Aby dany projekt mógł spełniać normy bezpieczeństwa funkcjonalnego, musi istnieć ocena bezpieczeństwa funkcjonalnego urządzenia końcowego, a także wszelkich jego elementów krytycznych dla bezpieczeństwa funkcjonalnego, które są zastosowane w projekcie, a które są już zgodne z tymi normami. Końcowa ocena zgodności jest niezależna od zespołu projektowego, a wymagany poziom bezpieczeństwa określają obowiązujące normy. Ocena taka może być przeprowadzona na przykład przez niezależną grupę roboczą w przedsiębiorstwie lub przez niezależne organizacje, takie jak Technischer Überwachungs-Verein (TÜV) czy Underwriters Laboratories (UL).

Najprostszą drogą do spełnienia norm, jest wykorzystanie sprawdzonych i zgodnych z normami podzespołów. Na rynku dostępnych jest wiele precertyfikowanych układów i elementów elektronicznych, spełniających normy bezpieczeństwa funkcjonalnego. W dalszej części artykułu przyjrzymy się, jak z zagadnieniem tym radzą sobie mikrokontrolery.

Mikrokontrolery z certyfikatem bezpieczeństwa

Normy bezpieczeństwa funkcjonalnego są zazwyczaj stosowane do elementów elektrycznych, elektronicznych i programowalnych elektronicznych systemów bezpieczeństwa w urządzeniu końcowym. Podczas certyfikacji sprawdzane są m. in. poszczególne komponenty układu na zgodność z normami. Mikrokontrolery są złożonymi i kluczowymi elementami wielu systemów bezpieczeństwa funkcjonalnego, w związku z czym są często dogłębnie analizowane w procesie certyfikacji. Często zadawane są pytania takie jak:

- Czy dany układ opracowano zgodnie ze standardem bezpieczeństwa funkcjonalnego?
- Jak mikrokontroler radzi sobie z przypadkowymi awariami?
- W jaki sposób układ radzi sobie z awariami systematycznymi?

Ponieważ normy IEC 61508 i ISO 26262 wymagają uwzględnienia bezpieczeństwa funkcjonalnego od samego początku fazy rozwoju produktu, bardzo ważne jest, aby wybrać mikrokontroler, który został zaprojektowany do zastosowań w zakresie tego rodzaju systemów. Takie układy mogą same posiadać odpowiednie certyfikaty np. dla konkretnego poziomu SIL. Precertyfikowany mikrokontroler, to taki układ, którego projekt został sprawdzony i nadaje się do stosowania w systemach bezpieczeństwa funkcjonalnego.

IEC 61508 przewiduje certyfikację mikrokontrolerów od SIL 1 (najniższy) do SIL 3. Tylko cały system może otrzymać najwyższy poziom – SIL 4. Analogicznie ISO 26262 wykorzystuje wskaźnik ASIL, od A do D. ASIL A jest najniższym poziomem, a ASIL D najwyższym. Zgodnie z ISO 26262, mikrokontrolery mogą być certyfikowane na wszystkich czterech poziomach ASIL. Normy wymagają, aby certyfikowane układy dostarczały odpowiednią dokumentację i narzędzia, (takie jak instrukcje bezpieczeństwa, tryb awaryjny lub rozbudowana diagnostyka automatyczna). Ma to pomóc użytkownikom zrozumieć mechanizmy bezpieczeństwa układu i obliczyć odpowiednie wskaźniki.

Przykładami precertyfikowanych mikrokontrolerów są układy z rodziny Hercules firmy Texas Instruments – TMS570 oraz RMxx, które dedykowane są do stosowania wraz z IEC 61508 do SIL3 i ISO 26262 do ASIL D, oraz mikrokontrolery Infineon Aurix, precertyfikowane do ASIL D. Są to najwyższe poziomy nienaruszalności bezpieczeństwa w normach. Chociaż w większości norm bezpieczeństwa

Tabela 1. Branżowe normy bezpieczeństwa funkcjonalnego i ich relacje z IEC 61508

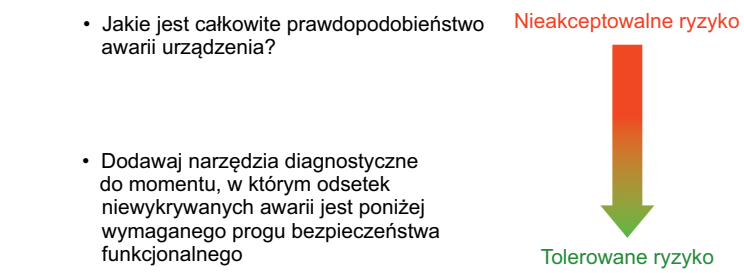
Norma	Branża	Integralność bezpieczeństwa	Metryka oceny architektury	Wymagania stawiane architekturze	Współczynnik awaryjności	Specyficzne wymagania stawiane autotestowi mikrokontrolera
IEC 61508	Systemy programowalne	SIL – 1, 2, 3, 4	SFF	HFT > 0 dla SIL 4	PFD, PFH	brak
ISO 26262	Motoryzacja	ASIL – A, B, C, D	SPFM/LFM	brak	PMHF	brak
EN 50129	Kolejowa	SIL – 1, 2, 3, 4	-	Wg IEC 61508	THR	CPU, pamięć
ISO 22201	Windy	SIL – 1, 2, 3	-	Dwukanałowe dla SIL 3	-	CPU, pamięć, przerwania, zegar, interfejsy IO i komunikacyjne
IEC 61800	Sterowniki silników elektrycznych	SIL – 1, 2, 3 (SIL 4 wg IEC 61508)	SFF	Zależnie od funkcji	PFH (brak PFD)	brak
IEC 62061	Maszyny	SIL – 1, 2, 3 (SIL 4 wg IEC 61508)	SFF	Wsparcie dla kategorii ISO 13849	PFH_D	brak
IEC 61511	Automatyka	SIL – 1, 2, 3 (SIL 4 wg IEC 61508)	SFF	Wg IEC 61508	$PFD_{śr}$	brak
ISO 13849	Maszyny	PL – a, b, c, d, e	$DC_{śr}$	Kategorie B, 1, 2, 3, 4	$MTTF_D$	brak
IEC 60730	Sprzęt domowy	Klasy A, B, C	brak	Tylko dla klasy C	brak	CPU, pamięć, przerwania, zegar, interfejsy IO i komunikacyjne

Skrót pojęcia	Objaśnienie
SIL, ASIL	Poziom integralności bezpieczeństwa; ogólny opis przynależności do jednej z dyskretnych klas bezpieczeństwa funkcjonalnego, gdzie 1 to najniższa klasa, a 4 to klasa najwyższa
SFF	Odsetek niegroźnych awarii; stosunek ilości nieszkodliwych awarii urządzenia (w tym wykrytych i zdiagnozowanych błędów) do całkowitej częstotliwości awarii systemu
SPFM	Prawdopodobieństwo wystąpienia błędu pojedynczego komponentu systemu bezpieczeństwa, który nie zostanie wykryty i w ten sposób uczyni system bezpieczeństwa funkcjonalnego niezdolnym do działania
LFM	Prawdopodobieństwo wystąpienia błędów utajonych wielu elementów, które nie są dostrzegane przez kierowcę, ani system bezpieczeństwa, a jednocześnie powodują awarię systemu bezpieczeństwa
$DC_{śr}$	Średnie (w czasie) pokrycie diagnostyczne systemu; stosunek wykrywanych błędów do ogólnej ilości awarii monitorowanego systemu
PFD	Prawdopodobieństwo nie zadziałania urządzenia na żądanie
$PFD_{śr}$	Średnie prawdopodobieństwo nie zadziałania urządzenia na żądanie
PFH_D	Prawdopodobieństwo (na godzinę) wystąpienia groźnej awarii urządzenia
PMHF	Prawdopodobieństwo wystąpienia dowolnego, losowego błędu w systemie (suma m.in. SPFM, LFM)
THR	Współczynnik tolerowalnego zagrożenia
$MTTF_D$	Średni czas pomiędzy niebezpiecznymi awariami
HFT	Odporność na uszkodzenia sprzętu, tj. maksymalna ilość dopuszczalnych usterek, która nie spowoduje utraty funkcji bezpieczeństwa systemu

funkcjonalnego zasadniczo nie wymaga się, aby system wykorzystywał tego rodzaju elementy, taki zabieg może znacznie zredukować wysiłek i koszty certyfikacji systemu. Komponenty takie są dostarczane wraz z potrzebnymi danymi i dokumentacją potrzebną do certyfikacji urządzenia.

Zarządzanie przypadkowymi awariami systemu

Pierwszym krokiem jest zrozumienie modów awarii i oszacowanie ich prawdopodobieństwa. Wymaga to przeprowadzenia analizy zagrożeń i oceny ryzyka zgodnie z wymogami odpowiednich norm. Deweloperzy muszą określić funkcje bezpieczeństwa i poziom redukcji ryzyka (SIL/ASIL) odpowiedni dla ich systemu. Następnie, w oparciu o niego, programiści muszą zdefiniować odpowiednią architekturę i wskaźniki. Konieczne są również odpowiednie mechanizmy bezpieczeństwa – diagnostyka – implementowane do momentu osiągnięcia wystarczającej redukcji ryzyka.



Rysunek 1. Ogólny mechanizm zarządzania bezpieczeństwem i awaryjnością urządzenia

Aby zrozumieć sposób, w jaki systemy bezpieczeństwa radzą sobie ze swoją awaryjnością, prześledźmy trzy zagadnienia z tym związane:

- Tryby awarii i wskaźniki awarii.
- Wskaźniki bezpieczeństwa funkcjonalnego architektury i parametry opisujące losowe awarie sprzętu.
- Mechanizmy bezpieczeństwa, pozwalające zredukować prawdopodobieństwo niebezpiecznej awarii.

Tryby awarii i wskaźniki awarii

Rozważmy nowoczesny system sterowania samochodem lub produktem przemysłowym, który posiada elektroniczne elementy programowalne i obwody wejścia/wyjścia. Zrozumienie trybów awarii tych elementów będzie pomocne w oszacowaniu całkowitego wskaźnika awaryjności produktu. Istnieją trzy główne tryby awarii wpływające na mikrokontroler w tym przypadku:

Trwała awaria obudowy układu, taka jak np. uszkodzenie jej z powodu różnej rozszerzalności cieplnej elementu i płytki drukowanej (PCB).

- Trwała awaria struktury półprzewodnikowej, taka jak rozwarcie lub zwarcie ścieżek metalizacji, wyciek ze złącza któregoś z tranzystorów, zablokowanie bramek i inne problemy wynikające ze zużycia struktury.
- Przejściowa awaria układu, taka jak na przykład wywołane promieniowaniem kosmicznym odwrócenie pojedynczego bitu w pamięci SRAM.

Tabela 2. Wymagania poszczególnych klas ASIL dotyczące parametrów SPFM, PMHF i LFM			
Klasa ASIL	SPFM	PMHF(FIT)	LFM
ASIL B	>90%	<100	>60%
ASIL C	>97%	<100	>80%
ASIL D	>99%	<10	>90%

Tabela 3. Wymagania poszczególnych klas SIL dotyczące parametrów SFF oraz PFH		
Klasa SIL (typ B)	SFF	PFH (FIT)
SIL 1	60..90%	<10000
SIL 2	90..99%	<1000
SIL 3	>99%	<100

Definiuje się tzw. wskaźnik awaryjności (FIT), gdzie FIT=1 oznacza jedną awarię na miliard godzin pracy. FIT to odwrotność średniego czasu pomiędzy awariami (MTBF), który typowo wykorzystywany jest do szacowania awaryjności w elektronice.

Norma IEC/TR 62380 zapewnia model matematyczny do oszacowania wskaźnika trwałej awaryjności obudowy układu na podstawie warunków jego użytkowania. Model pozwala również na oszacowanie prawdopodobieństwa trwałej awarii samego półprzewodnika na podstawie złożoności elementu i warunków jego eksploatacji, takich jak temperatura, czas cykli pracy i tym podobne. Ponadto większość producentów układów scalonych publikuje tego rodzaju wskaźniki trwałości dla swoich produktów, podane jako dane w FIT lub MTBF. Dane te są obliczane na podstawie badań niezawodności układu przeprowadzonych przez producenta.

Nie ma jednak znormalizowanej w branży metody szacowania wskaźnika awaryjności przejściowej. Idealnie, dane do oszacowania powinny pochodzić z rzeczywistych eksperymentów z wykorzystaniem tych układów. Texas Instruments dostarcza takie dane dla układów z rodziny Hercules – opiera się na danych zebranych z chipów testowanych w Los Alamos National Laboratory i wykorzystuje standard testowy JEDEC JESD89A. Ponieważ awaryjność przejściowa mikrokontrolerów może być od jednego do trzech rzędów wielkości wyższa niż awaryjność stała, precyzyjne dane pomagają zminimalizować ryzyko niedoszacowania ogólnego wskaźnika awaryjności. Dzięki temu, że tego rodzaju dane są dostępne, elektronicy projektujący systemy bezpieczeństwa funkcjonalnego nie muszą samodzielnie badać awaryjności mikrokontrolerów. Obniża to koszty i redukuje czas, potrzebny do stworzenia tego rodzaju systemu.

Wskaźniki bezpieczeństwa funkcjonalnego architektury i parametry opisujące losowe awarie sprzętu

Projektanci systemów muszą przeprowadzić analizę zagrożeń i ocenę ryzyka w celu oszacowania poziomu redukcji ryzyka wymaganego dla danej aplikacji. Wynik oceny jest celem bezpieczeństwa, na przykład klasyfikacja SIL 1...4, jak opisano w IEC 61508 lub poziom ASIL A...D w ISO 262626. W odniesieniu do elementów półprzewodnikowych, najwyższy możliwy do osiągnięcia poziom SIL to SIL 3; SIL 4 jest osiągalny tylko dla całego urządzenia, a nie jego składowych.

Normy określają wskaźniki, które służą do oceny mechanizmów bezpieczeństwa implementowanych tak na poziomie architektury, jak i rozwiązań zmniejszających ryzyko awarii czy prawdopodobieństwo wystąpienia błędów. W tym celu wykorzystywane są parametry takie jak SPFM (uszkodzenia jednopunktowe), LFM (uszkodzenia utajone) i SFF (odsetek niegroźnych uszkodzeń). Są to współczynniki pozwalające mierzyć architektoniczną skuteczność redukcji awaryjności. Z kolei parametry takie jak PMHF (prawdopodobieństwo wystąpienia losowych awarii) i PFH (prawdopodobieństwo awarii na godzinę) to parametry probabilistyczne pokazujące ogólny poziom ryzyka.

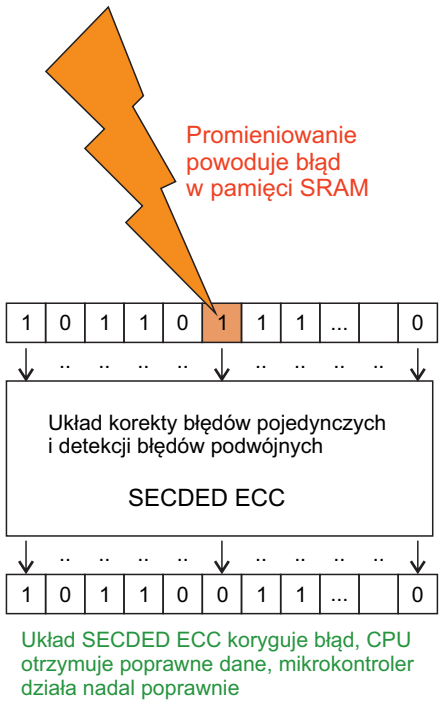
Przykłady zastosowania tych wskaźników przedstawiono w **tabeli 2**. Pokazuje ona wymagania dla poszczególnych klas ASIL (dla normy ISO 26262), dotyczące pojedynczego punktu uszkodzenia (SPFM), ukrytego wskaźnika uszkodzenia (LFM) i probabilistycznego opisu losowych awarii sprzętu (PMHF). **Tabela 3** z kolei pokazuje wymagania normy IEC 61508 dla poszczególnych klas SIL (typ B) dla SFF przy tolerancji na awarię sprzętu (HFT) równej zero i dla prawdopodobieństwa awarii na godzinę (PFH).

Mechanizmy bezpieczeństwa, pozwalające zredukować prawdopodobieństwo niebezpiecznej awarii

Znając wymagania dotyczące redukcji ryzyka, twórcy systemów muszą przestrzegać różnych procedur, aby uzyskać pewność, że osiągnięto cele dotyczące wskaźników losowej awaryjności. Dlatego też stosowane są mechanizmy bezpieczeństwa, które mają pomóc w wykrywaniu awarii. Funkcje krytyczne dla bezpieczeństwa wymagają monitorowania działania mikrokontrolera w czasie rzeczywistym. Projektant powinien wykorzystywać te mechanizmy, aby skonfigurować system tak, aby po wykryciu usterki system naprawił usterkę albo układ przechodzi w stan bezpieczny.

Poniżej znajduje się kilka przykładów wykorzystywanych w mikrokontrolerach mechanizmów. **Rysunek 2** prezentuje obwód korekcji błędów pamięci ECC. Obwód SECDED pozwala na korekcję pojedynczego błędu (pojedynczego bitu) – SEC – lub detekcję błędów podwójnych – DED. Błędy w pamięci SRAM powstają np. na skutek promieniowania kosmicznego, bądź innych losowych zdarzeń, które są w stanie zmienić wartość jednej z komórek pamięci operacyjnej, powodując błędy w danych. System ECC pozwala na korekcję lub wykrywanie tych awarii.

Tak jak w przypadku pamięci SRAM, np. kwant promieniowania kosmicznego, po uderzeniu w rdzeń mikrokontrolera może spowodować zmianę jakiegoś losowego bitu. Oczywiście spowoduje to niepoprawne działanie układu. Problemy te zasadniczo rozwiązuje się z pomocą redundancji – dodając drugi, równolegle pracujący układ. W ten sposób otrzymamy system, w którym uszkodzenie jednego z dwóch elementów nie powoduje jeszcze katastrofalnej awarii. Niestety w przypadku mikrokontrolerów nie jest to takie proste. Nie da się ich w prosty sposób zrównoleglić, bo nie jest możliwe wykrycie ich awarii – jeśli monitorujemy np. wyjście CPU, nie wiemy jakie ono powinno być, jeśli nie wykonamy takiej samej operacji, efektywnie



Rysunek 2. Działanie obwodu korekcji błędów SECDED ECC dla pamięci SRAM w mikrokontrolerze

potrzebując dwóch CPU. Nawet w takiej sytuacji, nie wiemy, który z równolegle pracujących mikrokontrolerów uległ awarii. Dlatego też stosuje się układy głosujące – w systemie implementuje się więcej procesorów, które „głosują" nad poprawnym wynikiem. W większości przypadków każdy procesor wykonuje operacje tak samo, a każde odstępstwo od tego jest uznawane za awarię.

Architektury z głosowaniem i/lub redundancją określa się jako N spośród M – N out of M – NooM, co oznacza, że w systemie znajduje się ogólnie M podmodułów, a do awarii całego systemu potrzebna jest awaria co najmniej N podmodułów. W systemie takim znajduje się M głosujących, równorzędnych podmodułów. HFT takiego układu równe jest M – N.

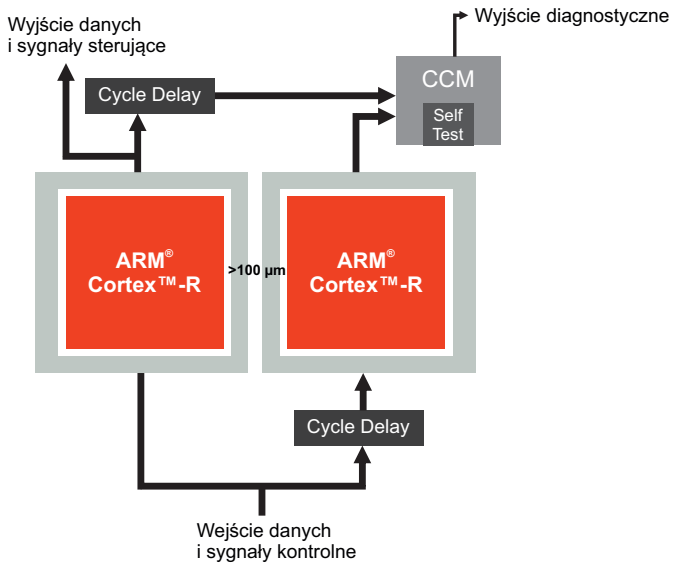
Na **rysunku 3** zaprezentowano, wykorzystywany przez mikrokontrolery z rodziny TI Hercules układ dwóch rdzeni w architekturze nazwanej 1oo1D. Pozwala ona na eliminację wpływu błędów losowych na działanie systemu oraz bardzo ziarnistą diagnostykę procesora. Od klasycznej architektury 1oo1 układ ten odróżnia się posiadaniem dwóch równoległych rdzeni, których wyniki pracy porównywane są ze sobą przez specjalny moduł CCM, będący częścią układów diagnostycznych w mikrokontrolerze.

W układach z serii TI Hercules stosuje się dwa rdzenie ARM Cortex-R w celu zapewnienia podwyższonego poziomu bezpieczeństwa – odporności na losowe awarie. Do obu rdzeni trafiają te same dane i te same sygnały kontrolne. Informacje wyjściowe z układu są następnie porównywane ze sobą przez moduł CCM. Aby zredukować szansę, że dane zdarzenie losowe (np. promieniowanie elektromagnetyczne, czy kosmiczne) wywoła usterkę w obu rdzeniach w tym samym momencie, są one od siebie izolowane przestrzennie (rdzenie są odsunięte od siebie w układzie o ponad 100 mikronów, a ponadto drugi rdzeń jest obrócony o 90° i odbity lustrzanie), elektrycznie (wokół każdego rodzenia rozciągnięty jest ochronny pierścień metalizacji) i czasowo (rdzenie działają asynchronicznie – ich działania przesunięte są względem siebie w czasie o 1,5 lub 2 cykle zegarowe, zależnie od implementacji). Mikrokontrolery Infineon Aurix wykorzystują podobną technologię – rdzenie, wykorzystywane w tych układach działają również w architekturze 1oo1D, jednakże w pojedynczym mikrokontrolerze Aurix znajdować się może do trzech rdzeni (z których dwa są podwojone i pracują jako 1oo1D). Oznacza to, że istnieje możliwość skonfigurowania ich do pracy w topologii 2oo2D lub 2oo3, zapewniając zwiększony poziom odporności na awarię i redundancji (HFT > 0).

Analiza zagrożeń i ocena ryzyka

Elementy używane w produkcie końcowym mogą podlegać systematycznym lub przypadkowym awariom. Normy bezpieczeństwa funkcjonalnego zostały opracowane tak, aby powodować zmniejszenie potencjalnego ryzyka obrażeń fizycznych i szkód materialnych z powodu tego rodzaju awarii. Najpierw jednak należy zidentyfikować zagrożenia i przeanalizować ich skutki, aby można było wdrożyć odpowiednie metody minimalizacji prawdopodobieństwa zidentyfikowanych awarii.

We wcześniejszej części tego artykułu opisaliśmy awarie przypadkowe i metody zarządzania nimi. Konieczne jest teraz zbadanie zagrożeń i ocena ryzyka na poziomie gotowego urządzenia, wykorzystującego programowalne elementy, aby określić wymogi zmniejszenia ryzyka zgodnie z wybraną klasą ASIL/SIL. Gdy znane są te wymogi, programiści będą musieli wdrożyć wystarczającą liczbę mechanizmów diagnostycznych, aby wykrywać awarie i osiągnąć



Rysunek 3. Koncepcja bezpieczeństwa dwurdzeniowego 1oo1D, wykorzystana w układach z rodziny TI Hercules (źródło: http://bit.ly/2kDTMug)

Tabela 4. Zarządzanie awariami w/g norm bezpieczeństwa w urządzeniu końcowym

Bezpieczeństwo funkcjonalne	Analiza	Przykład
Definicja systemu	Jaka jest funkcja urządzenia?	Sterownik silnika elektrycznego w pojeździe elektrycznym
Analiza zagrożeń i ocena ryzyka	Zidentyfikuj jakie są zagrożenia, skategoryzuj występujące w systemie ryzyka.	Zbyt wysoki moment obrotowy silnika, powodujący ryzyko kolizji.
Klasyfikacja wymaganego stopnia ASIL/SIL	Jakie jest maksymalne tolerowalne ryzyko w systemie?	ASIL-C
Wyznaczenie celów bezpieczeństwa	Wymagania bezpieczeństwa + Tryby awarii i jej prawdopodobieństwo + Implementacja diagnostyki	Unikaj zbyt wysokiego momentu silnika
Implementacja wymaganych rozwiązań		Implementacja diagnostyki w mikrokontrolerze do monitorowania działania generatora PWM
Obliczenie metryk bezpieczeństwa funkcjonalnego	Czy redukcja ryzyka jest dostateczna?	Wyznaczenie metryk.

wystarczającą redukcję ryzyka. Mierzy się ją wskaźnikami opisanymi w obowiązującej dany produkt normie.

W **tabeli 4** zaprezentowano schematyczne przedstawienie postępowania, wraz z przykładowym zadaniem – sterownikiem silnika elektrycznego, zgodnego z normą ISO 26262. Podobne metody będą miały zastosowanie również w przypadku innych norm bezpieczeństwa funkcjonalnego. W przykładzie tym mamy do czynienia ze sterownikiem silnika w pojeździe elektrycznym. Jego głównym zadaniem jest kontrola momentu obrotowego silnika za pomocą przebiegu PWM. Moduł taki ma bardzo kompleksowe tryby awarii. Jednym z nich jest wygenerowanie zbyt dużego momentu obrotowego na silniku, co przełożyć może się na wywołanie wypadku komunikacyjnego – uderzenia w barierkę na autostradzie, zjechanie do rowu etc. Rozważmy ten przypadek dokładniej, gdyż jest on bardzo poważnym zagrożeniem dla zdrowia i życia kierowcy oraz pasażerów.

Zgodnie z normą ISO 26262, analiza zagrożeń opiera się na ocenie każdej z awarii w trzech kategoriach – poważności (S1...S3), prawdopodobieństwa niebezpiecznego wydarzenia w czasie awarii (E1...E4) oraz sterowalności sytuacją w danej awarii (C1...C3). W opisanym powyżej przypadku awaria klasyfikowana jest jako S3, ponieważ zagraża życiu; E4, ponieważ istnieje duże ryzyko, że auto w czasie awarii poruszać będzie się po autostradzie, drodze sąsiadującej z rowem melioracyjnym itp, oraz jako C2, ponieważ pomimo tego rodzaju awarii, autem można nadal kierować i hamować. Na podstawie tych klasyfikacji z normy można odczytać, iż system bezpieczeństwa funkcjonalnego musi mieć klasyfikację co najmniej ASIL-C, aby ryzyko było na tolerowanym poziomie. W tabeli 2 odczytać możemy towarzyszące tej klasie bezpieczeństwa metryki bezpieczeństwa – SPFM, PMHF (FIT) oraz LFM, które omawialiśmy we wcześniejszej części tekstu.

W tym przykładzie załóżmy, że momentem obrotowym silnika steruje inny komputer w pojeździe za pośrednictwem sieci CAN. Mikrokontroler steruje momentem obrotowym silnika przebiegiem PWM. Konieczne jest zatem zrozumienie w jaki sposób w układzie generowane są sygnały PWM i jakie tryby awarii mogą wpłynąć na zaangażowane peryferia. Wiedząc to można obliczyć wskaźnik awaryjności (jeśli producent dostarcza odpowiednią dokumentację) i, jeśli wskaźnik awaryjności jest zbyt wysoki w stosunku do wymagań ASIL-C, zastosować dodatkową diagnostykę w oprogramowaniu, w celu redukcji prawdopodobieństwa niewykrytej awarii systemu.

W takim systemie pozycja silnika jest określana poprzez enkoder kwadraturowy i pomiar prądu fazowego na mostku sterującym silnikiem. Procesor odczytuje swój program z pamięci Flash, a w pamięci SRAM wykonuje się algorytm FOC (*Field Oriented Control*). Algorytm ten ma na celu ustalenia odpowiednich sygnałów PWM do sterowania silnikiem z pożądanym momentem obrotowym. Wbudowany zegar PWM generuje następnie sygnały napędzające sterownik mostka. Ten prosty opis jest dostateczny, do przeprowadzenia analizy ryzyka w układzie. Oto przykładowa lista awarii mikrokontrolera, które mogą spowodować wygenerowanie nieprawidłowego sygnału PWM. Należy pamiętać, że nie jest to w żadnym wypadku wyczerpujące i jest przeznaczone wyłącznie jako przykład w celach ilustracyjnych.

- Awaria rdzenia procesora
- Przerzucanie bitów pamięci Flash i/lub SRAM
- Brak zasilania
- Awaria zegara
- Błąd komunikacji CAN
- Awaria modułu (timera) PWM

Nieprawidłowe działanie któregokolwiek z tych modułów, może potencjalnie spowodować wystąpienie niebezpiecznego zdarzenia. Aby wdrożyć funkcję bezpieczeństwa polegającą na „unikaniu zbyt wysokiego dodatniego momentu obrotowego silnika", projektant musiałby zastosować diagnostykę do elementów o krytycznym znaczeniu dla bezpieczeństwa, tak aby w przypadku wykrycia awarii system mógł podjąć działania w celu złagodzenia awarii lub przejścia do zdefiniowanego, bezpiecznego stanu.

Informacje na temat dedykowanych systemów diagnostycznych, zaimplementowanych w danym mikrokontrolerze, projektanci systemu znaleźć mogą w dokumentacji, o ile dany układ dostosowany jest do „zastosowań specjalnych" w systemach bezpieczeństwa funkcjonalnego. Dokumentacja ta, wraz z narzędziami FMEDA (do systematycznej analizy trybów i efektów awarii oraz badania systemów diagnostycznych), pozwala na oszacowania częstości FIT układu, jak i wyznaczenie wskaźników bezpieczeństwa (SPFM, LFM, PMHF). Tego rodzaju dokumentacja dostępna jest tak dla normy ISO 26262, jak i dla IEC 61508 w precertyfikowanych mikrokontrolerach.

Podsumowanie

Systemy bezpieczeństwa funkcjonalnego, to układy elektroniczne, często wykorzystujące mikrokontrolery do zapewnienia bezpieczeństwa ludziom, pracującym w przemyśle, kierowcom i pasażerom samochodów, pociągów itp. Każdy z tych sektorów opisany jest szeregiem norm, definiujących tolerowane ryzyko w tych systemach, jak i sposoby jego badania i oceny.

Jednym ze sposobów na uproszczenie procesu projektowania systemu bezpieczeństwa funkcjonalnego, jest wykorzystanie precertyfikowanych układów, dedykowanych do tego rodzaju specjalnych zadań. Są to często mikrokontrolery specjalnie zoptymalizowane do takich zastosowań. Przykładami takich układów są m.in. mikrokontrolery z rodziny Hercules firmy Texas Instruments czy Aurix firmy Infineon.

Nikodem Czechowski

Źródła:

- *https://ubm.io/2kO6h6o*
- *https://ubm.io/2lSlxPW*
- *http://bit.ly/2lTfpXy*
- *http://bit.ly/2kDTMug*
- Norma PN-EN 61508
- Norma ISO 26262
- *http://bit.ly/2lUmk2G*