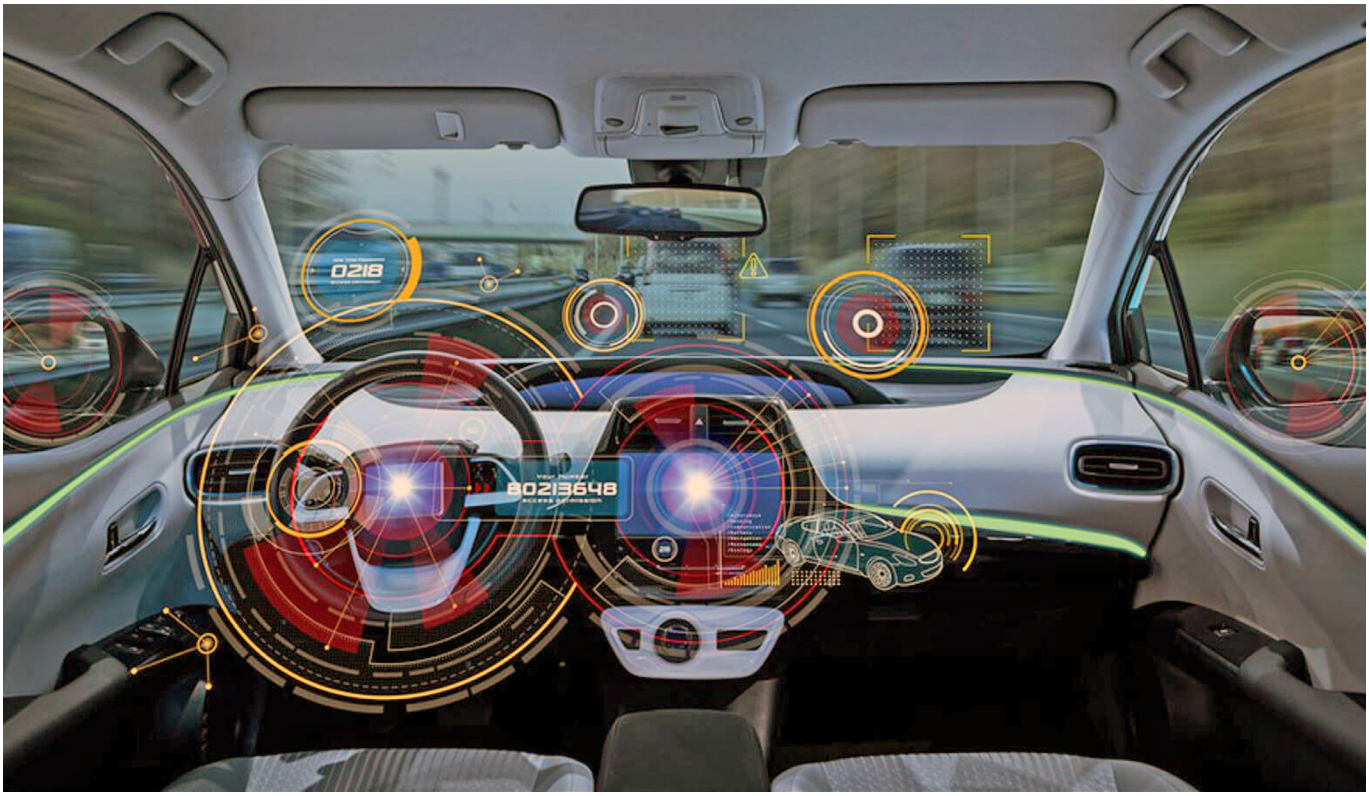


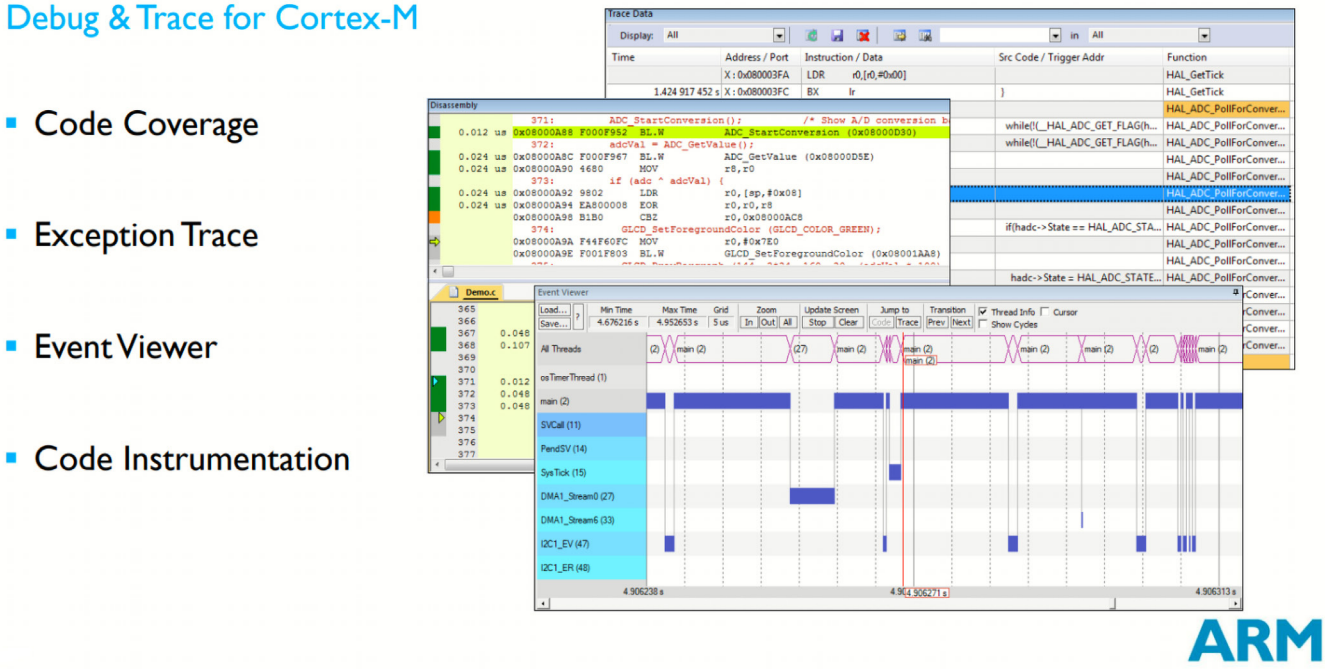
Bezpieczeństwo funkcjonalne ARM

Warunkiem wprowadzenia na rynek wielu produktów w takich branżach, jak: sprzęt gospodarstwa domowego, motoryzacja, przemysł lub medyczna, jest spełnienie wymagań prawnych potwierdzających ich zgodność z normami bezpieczeństwa funkcjonalnego. Uzyskanie certyfikatu jest jednym z warunków dopuszczenia artykułu do sprzedaży i polega na spełnieniu norm bezpieczeństwa, co czyni dany produkt bezpiecznym dla użytkowników. Producentów obowiązują normy: IEC 61508 dla systemów przemysłowych, ISO 26262 dla przemysłu motoryzacyjnego, IEC62304 dla systemów medycznych czy EN 50128 dla aplikacji kolejowych. Zaprojektowanie i wdrożenie systemu zarządzania bezpieczeństwem funkcjonalnym nie różni się znacząco od wdrażania innych systemów zarządzania, wymaga jednak spełnienia szczególnych warunków.

W ramach standardów powstało kilka poziomów integralności bezpieczeństwa. Dla branży motoryzacyjnej jest to norma ASIL, a dla pozostałych norma SIL. Standardy te określają, między innymi, formalne metody pracy i kontroli jakości dla opracowania kodu aplikacji. Nie bez znaczenia jest dobór odpowiednich składników oprogramowania i zestawów narzędzi, bezpiecznych dla zamierzonego zastosowania. Dla przykładu, podzespoły z klasą bezpieczeństwa ASIL A mają najmniejszy wpływ na zdrowie człowieka. Taka certyfikacja dotyczy, sterowania oświetleniem wewnętrznym w samochodzie. Wpływ jego uszkodzenia na bezpieczeństwo użytkowników jest raczej niewielki, a kierowca w czasie awarii jest w stanie zapanować nad pojazdem bez bezpośredniego zagrożenia życia.

Awaria elementów ważniejszych z punktu widzenia bezpieczeństwa (choćby hamulców lub wspomagania kierownicy) może przyczynić się do bezpośredniego zagrożenie zdrowia, a nawet życia. Elementy składowe takich układów muszą spełniać wymagania najwyższej klasy poziomu bezpieczeństwa – ASIL D. Wiąże się to z koniecznością znaczącego ograniczenia ryzyka, tak aby potencjalna awaria układu nie stała się przyczyną urazów kierowcy, pasażerów i innych uczestników ruchu. Aby zapobiegać ewentualnym sytuacjom niebezpiecznym, stosuje się różne metody ograniczania ich wystąpienia, miedzy innymi FMEA, czyli analizę przyczyn i skutków możliwych błędów. Metoda ta ma na celu zapobieganie skutkom wad, które mogą wystąpić w fazie projektowania oraz w fazie wytwarzania produktu.

Opracowywanie i optymalizacja złożonych aplikacji związanych z bezpieczeństwem jest zadaniem trudnym, zwłaszcza gdy ważnym czynnikiem jest czas wprowadzenia produktu na rynek. ARM dysponuje oprogramowaniem, narzędziami i platformami przeznaczonymi do tworzenia aplikacji dla bezpieczeństwa funkcjonalnego – upraszcza projektowanie systemu i przyśpiesza proces weryfikacji. Obejmuje to certyfikowany system bezpieczeństwa dla procesorów, w tym system operacyjny czasu rzeczywistego do programowania aplikacji.



Siłę łączenia powszechnie używanych funkcji bibliotecznych C z certyfikowanym przez TÜV zestawem narzędzi kompilatora ARM i systemem operacyjnym Keil RTX5 w czasie rzeczywistym zapewnia niezawodna, bezpieczna i zoptymalizowana platforma programowa µVision ARM KEIL MDK-Professional. Jeżeli dodamy Qualification Kit, czyli dokumentację Functional Safety dostępną w pakiecie MDK-Pro w postaci raportów, instrukcji i analiz, to proces certyfikacji znacząco ulegnie skróceniu.

Do głównych narzędzi oprogramowania MDK-Pro wspomagających proces certyfikacji należą debugger z wbudowanymi narzędziami do testowania kodu oraz kompilator Arm C/C ++. Za pomocą analizy strumieniowej ETM, przy użyciu adaptera debugowania ULINK*pro* można korzystać z dodatkowych funkcji analizy. Arm Keil MDK-Professional zawiera debugger z wbudowanymi narzędziami do testów pokrycia kodu i profilowania wykonania. Funkcja oprogramowania, którą jest tzw. pokrycie kodu (*code coverage*), identyfikuje wykonywanie programu instrukcja po instrukcji, zapewniając dokładne testowanie aplikacji. Jest to podstawowe wymaganie pełnej weryfikacji oprogramowania i certyfikacji. Funkcjonalne normy bezpieczeństwa wymagają testów pokrycia kodu dla wielu poziomów integralności bezpieczeństwa. Z kolei *Execution Profiler* rejestruje statystyki czasu i wykonania instrukcji dla całego kodu programu. Wartości te są wyświetlane w edytorze µVision lub oknie *Disassembly*.

Mówiąc o bezpieczeństwie funkcjonalnym, należy je rozpatrywać w 3 aspektach, to znaczy na poziomie rdzenia, systemu i oprogramowania.

Grzegorz Cuber
FAE Computer Controls
Computer Controls – oficjalny dystrybutor ARM Keil w Polsce