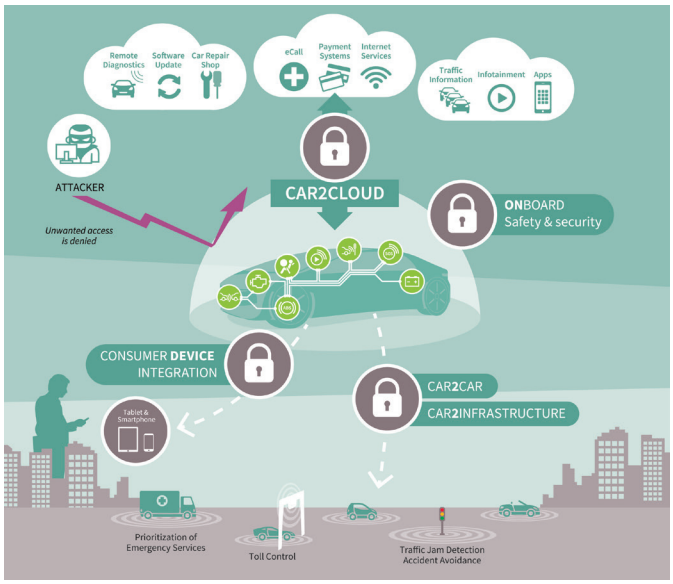
Cyberbezpieczeństwo w aplikacjach motoryzacyjnych

Przy stale rosnącej liczbie aplikacji internetowych i sterowanych zdalnie, a także aktualnie testowanych rozwiązaniach umożliwiających jazdę autonomiczną, bezpieczeństwo cybernetyczne w pojazdach staje się coraz ważniejsze. Mimo że jest ono częścią codziennej rutyny w tradycyjnej przestrzeni IT, zabezpieczenia nie są jeszcze powszechnie implementowane w pojazdach.



Na pierwszy rzut oka nie wydaje się to większym problemem, ponieważ istnieje już wiele rozwiązań z innych dziedzin, które mogą być użyte także dla samochodów. Jednak środowisko specyficzne dla motoryzacji ogranicza ich zastosowanie.

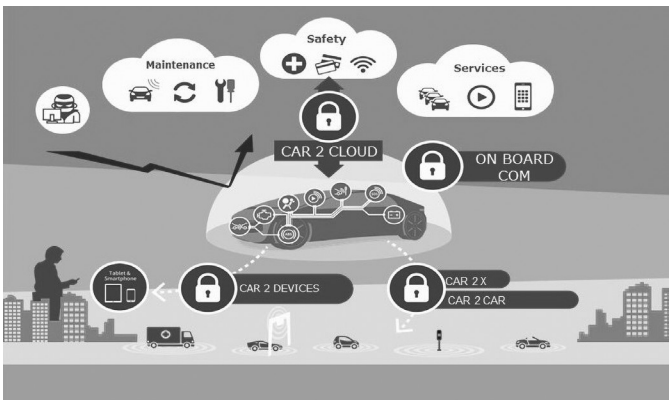
Klienci oczekują nieograniczonej możliwości i połączenia smartfonu i innych osobistych urządzeń mobilnych w centrum multimedialnym w pojeździe, a także korzystania z najnowszej nawigacji satelitarnej zapewniającej dobrą dokładność wyznaczania pozycji oraz odbierającej aktualne informacji drogowe. W przyszłości komunikacja będzie wymagała także stałego połączenia danych z zewnętrzną infrastrukturą lub urządzeniami zewnętrznymi (**rysunek 1**). To wszystko sprawia, że pojazd może stać się celem hakerów, którzy będą próbowali dokonywać w nim pewnych manipulacji lub pozyskiwać poufne informacje. Dlatego powinno się kłaść szczególny nacisk na zapewnienie poufności, integralności i autentyczności, co wymaga dodatkowych środków ochronnych. Różne jednostki komunikacyjne – od zaplecza OEM do serwisu oraz w poszczególnych jednostkach sterujących (np. ECU, sterowanie ogrzewaniem itp.) wymagają bezpiecznego uwierzytelniania i ochrony przed manipulowaniem danymi. Aby to zapewnić, do komunikacji używa się procedur kryptograficznych opartych na kluczach bezpieczeństwa.

Szyfrowanie jest metodą przekształcania informacji jawnej za pomocą klucza bezpieczeństwa w szyfrogram, z którego można ją odczytać za pomocą tajnego klucza. Zachowanie tajemnicy i ochrona tych kluczy bezpieczeństwa są – obok innych czynników – podstawowym wymaganiem architektury bezpieczeństwa. Jeśli poufność klucza jest zagrożona, to jest również zagrożone ogólnie rozumiane bezpieczeństwo użytkownika. W przypadku przemysłu motoryzacyjnego może to mieć katastrofalne skutki związane z koniecznością poniesienia ogromnych kosztów i utratą wizerunku przez producenta. Jeśli atakujący zna używane klucze, może wpłynąć na komunikację. Oznacza to, że pojazdy muszą być sprowadzone w warsztacie lub w fabryce i ponownie zabezpieczone, co wiąże się z dużym nakładem czasu i pieniędzy. W tym kontekście zachowanie w tajemnicy i ochrona zarchiwizowanych kluczy ma zasadnicze znaczenie dla bezpieczeństwa cybernetycznego, jak również bezpieczeństwa funkcjonalnego w pojazdach (zgodnie z ISO 262262).

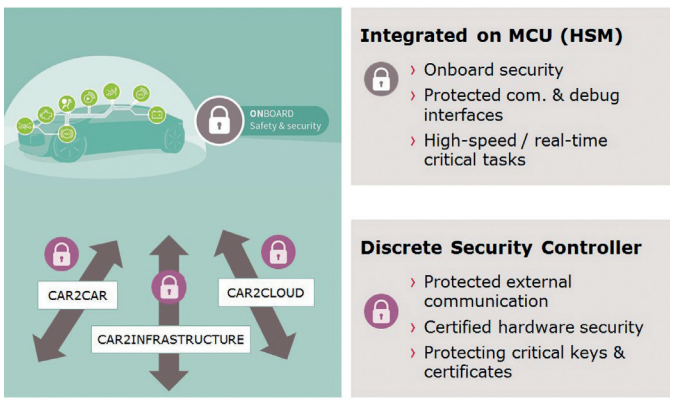
Kotwica bezpieczeństwa

Depozyt kluczy bezpieczeństwa może być chroniony przez tak zwane sprzętowe kotwice bezpieczeństwa (Trust Anchor). Przy ich użyciu należy podjąć działania w celu zapewnienia, że tylko uprawniona jednostka ma dostęp do usługi kryptograficznej w zaufanej kotwicy (**rysunek 2**). Kotwice bezpieczeństwa są bezpiecznym, odizolowanym środowiskiem, w którym przechowywane i przetwarzane są klucze lub certyfikaty. Różne ataki hakerskie pokazały, że implementacja tych kotwic zabezpieczających w oprogramowaniu (jako części systemu operacyjnego mikrokontrolera) jest niewystarczająca. Bardziej skuteczną i lepszą ochronę zapewnia Implementacja sprzętowa.

W tym celu opracowano moduły SHE (Security Hardware Extension) i HSM (Hardware Security Modules), które są zintegrowane w strukturze mikrokontrolera. Na przykład, mikrokontrolery Infineon AURIX mają zintegrowany HSM, przy czym HSM drugiej generacji (TC3xx) obsługuje również asymetryczną kryptografię (para kluczy z prywatnego i publicznego klucza, **rysunek 3**).



Rysunek 1. Komunikacja w obrębie pojazdu



Rysunek 2. Funkcje kotwicy bezpieczeństwa

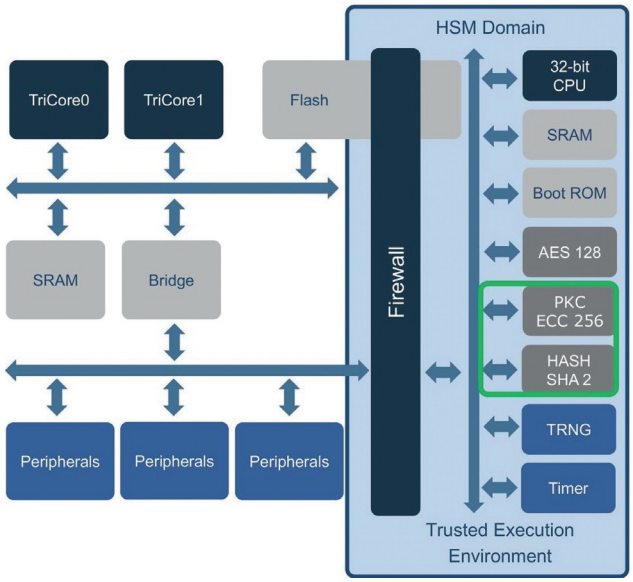
Wyjątkowo skuteczna ochrona, w szczególności w obszarach o kluczowym znaczeniu dla bezpieczeństwa, takich jak komunikacja z pojazdami na zewnątrz lub strefa infotainment, jest możliwa dzięki specjalnym kontrolerom bezpieczeństwa, takim jak OPTIGA TPM (Trusted Platform Module). Moduł TPM zapewnia bezpieczne uwierzytelnianie. W tym celu przechowuje długoterminowo używane certyfikaty i odpowiednie klucze w chronionym środowisku.

W sprzętowych kotwicach zabezpieczających zaimplementowano różne funkcje, aby móc chronić przetwarzanie o krytycznym znaczeniu dla bezpieczeństwa i na przykład przekazywanie kluczy. Zastosowanie wymienionych wyżej modułów kontrolnych umożliwia zmniejszenie nakładu pracy przy tworzeniu oprogramowania. Ułatwia też wszechstronne testowanie.

Wykorzystanie rozwiązań opartych na modułach HSM, TPM lub SIM jako kotwic bezpieczeństwa w samochodach jest możliwe przez odpowiednie aplikacje (**rysunek 4**). Zastosowanie zintegrowanego z mikrokontrolerem modułu HSM ma na celu przede wszystkim zabezpieczenie komunikacji „na pokładzie", w której jest wymagana duża wydajność obliczeniowa i niezawodne działanie w czasie rzeczywistym. Natomiast specjalne sterowniki TPM zabezpieczają komunikację zewnętrzną, która jest narażona na cyberataki. Ponadto, moduły mogą być używane jako pamięć centralna dla kluczy i certyfikatów o kluczowym znaczeniu dla bezpieczeństwa. Zapewniają one także ochronę przed tak zwanymi atakami z kanału bocznego. Analizują one np. czas działania algorytmu, pobór mocy procesora podczas obliczeń lub promieniowanie elektromagnetyczne w celu wyciągnięcia wniosków na temat autentyczności kluczy.

W odniesieniu do bezpieczeństwa danych w samochodach obowiązują następujące zasady:

- integralność kluczy elektronicznych jest podstawowym wymogiem dla systemu elektronicznego chronionego danymi,
- możliwość manipulacji kluczami elektronicznymi wyklucza bezpieczeństwo danych,
- sklonowane lub symulowane klucze elektroniczne nie pozostawiają żadnych śladów,
- obsługa kluczy elektronicznych musi być zapewniona przez cały okres użytkowania produktu,
- kotwice zabezpieczające umożliwiają zarządzanie kluczami i korzystanie z nich w niebezpiecznych środowiskach (np. Użytkowania pojazdu).



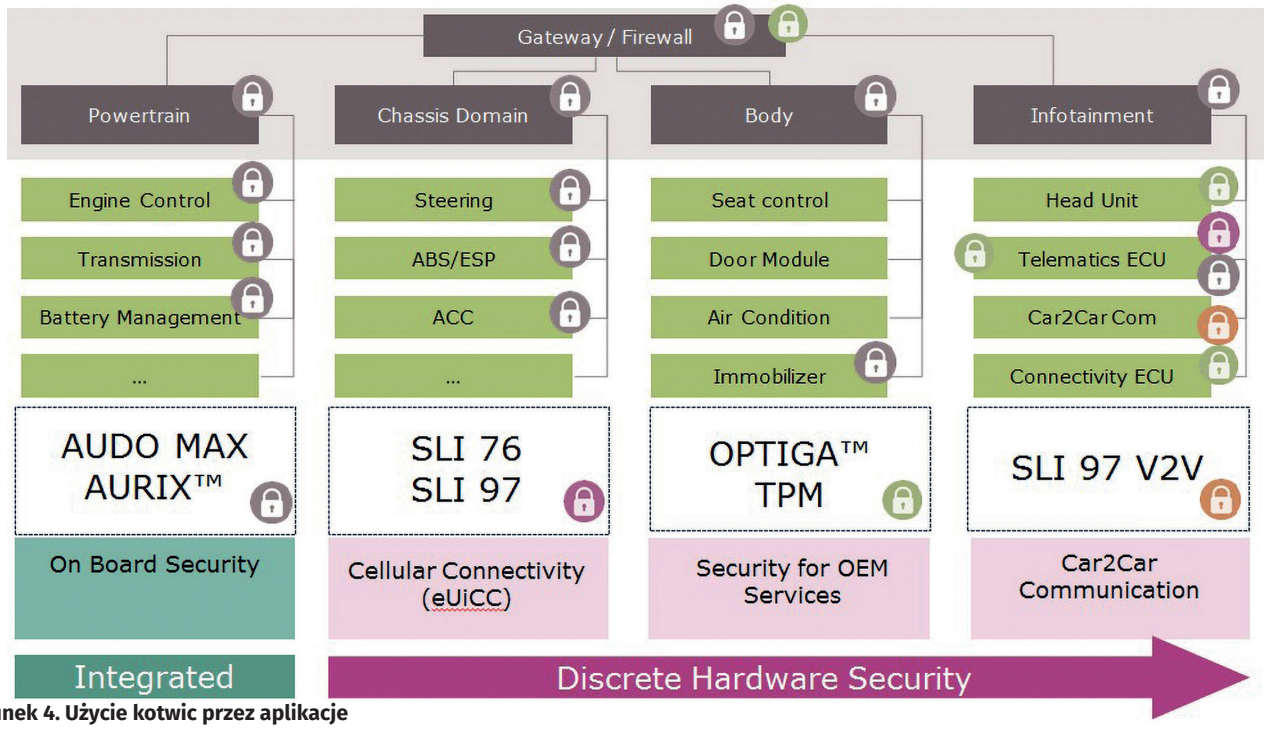
Rysunek 3. Moduł HSM drugiej generacji

Skuteczna ochrona przy użyciu standardów

Producenci samochodów klasyfikują dane pod kątem ich znaczenia dla bezpieczeństwa. Odpowiednia klasyfikacja wpływa również na niezbędne środki lub ochronę uzasadnioną dla odpowiednich kluczy. Ważna jest również żywotność kluczy elektronicznych. Klucze elektroniczne o dłuższej żywotności warto chronić bardziej, niż klucze elektroniczne używane przez ograniczony czas (klucz sesyjny).

Użycie standardowych, powszechnie stosowanych algorytmów i procedur zabezpieczających zmniejsza koszt poniesiony na zapewnienie bezpieczeństwa pojazdu. Po negatywnych doświadczeniach z zastosowaniem autorskich algorytmów producenta oraz algorytmów zastrzeżonych, w branży motoryzacyjnej ustalono znormalizowane techniki szyfrowania, w tym znane z innych dziedzin AES, RSA i ECC.

O ile jest pożądane zastosowanie już istniejących, sprawdzonych technologii zabezpieczenia danych, w motoryzacji obowiązują specyficzne wymagania, które należy wziąć pod uwagę – samochody powinny spełniać wysokie standardy bezpieczeństwa w różnorodnych warunkach użytkowania, zapewniając przy tym podwyższony poziom niezawodności i długi czas użytkowania.



Rysunek 4. Użycie kotwic przez aplikacje

W powszechnym użyciu, nie tylko w pojazdach, są rozwiązania stosowane w kartach chipowych. Używając tej techniki w pojazdach należy dodatkowo uwzględnić rozszerzony zakres temperatury oraz standardy obowiązujące w motoryzacji.

Ochrona przez cały okres funkcjonowania

Klucze bezpieczeństwa stosowane w samochodach muszą być, w zależności od systemu zarządzania kluczami i procedur autentykacji, chronione przez cały okres eksploatacji pojazdu – od opuszczenia taśmy produkcyjnej, przez eksploatację aż po złomowanie. Fazą krytyczną jest w szczególności produkcja, ponieważ tam klucze muszą być przekazywane w postaci jawnej. Jeśli nie odbędzie się to w sposób odpowiednio chroniony, atakujący może uzyskać większą liczbę kluczy. Ponadto, przekazywanie klucza może również odbywać się w kilku lokalizacjach i za pośrednictwem dostawców, co utrudnia stosowanie zabezpieczeń.

Skutecznym rozwiązaniem jest zastosowanie spersonalizowanego kontrolera bezpieczeństwa. Spersonalizowanie oznacza tutaj, że kontroler bezpieczeństwa ma indywidualny osobisty klucz przypisany do chipa, który został przygotowany przez producenta półprzewodników w certyfikowanym procesie produkcyjnym. Ponieważ te kontrolery bezpieczeństwa są chronione przed atakami sprzętowymi, mogą być dostarczane również bez zachowania specjalnych procedur logistycznych. Dzięki spersonalizowanemu kontrolerowi bezpieczeństwa TPM ulega uproszczeniu również proces personalizacji ECU, ponieważ chroniony klucz prywatny w kontrolerze umożliwia przekazywanie dalszych kluczy za pośrednictwem bezpiecznej komunikacji.

Bezpieczeństwo produktu zależy od jakości procesów bezpieczeństwa mających początek już w fazie opracowywania i produkcji. Na przykład, proces projektowania i wytwarzania OPTIGA TPM jest certyfikowany zgodnie z Common Criteria. Common Criteria opublikowano w 1999 roku jako standard międzynarodowy ISO/IEC 15408. Zapewnia kryteria oceny i certyfikacji zabezpieczeń produktów IT. Ponadto, TPM są wytwarzane i personalizowane zgodnie z procesami produkcyjnymi, które podlegają audytom i są również certyfikowane jako bezpieczne. Ta ścisła kontrola procesów bezpieczeństwa przez niezależne strony trzecie lub państwowe organy kontrolne jest podstawą wysokiej jakości zabezpieczeń modułów TPM firmy Infineon.

Innym aspektem jest długi okres eksploatacji pojazdów – 20 lat lub więcej. Z tego wynika wymaganie, że stosowane algorytmy kryptograficzne są bezpieczne przez cały okres użytkowania. Aby było to możliwe, architektura bezpieczeństwa powinna umożliwiać łatwą zmianę funkcji szyfrowania, równolegle obsługiwać stare i nowe algorytmy oraz mieć wystarczające zasoby sprzętowe (magistrale, pamięci itp.) dla nowych, dłuższych kluczy. Tak zwana „zdolność kryptologiczna" jest obsługiwana np. w standardzie TPM 2.0.

Przykład zastosowania – SOTA

Kosztowne akcje serwisowe wzywające do usunięcia problemów z oprogramowaniem w jednostkach sterujących pojazdu skłaniają producentów pojazdów do coraz częstszego rozważania sposobów przeprowadzania aktualizacji oprogramowania za pośrednictwem interfejsu bezprzewodowego (Software Update Over The Air – SOTA). Oprócz oszczędności na serwisie, połączenie mobilne z pojazdem i możliwość pobierania nowego oprogramowania za pośrednictwem tego interfejsu komunikacyjnego umożliwia zaoferowanie nowych funkcji i aplikacji. Dedykowane rozwiązania bezpieczeństwa (**rysunek 5**) zapewniają sprzętowe mechanizmy bezpieczeństwa dla różnych funkcji aplikacji SOTA w pojeździe.

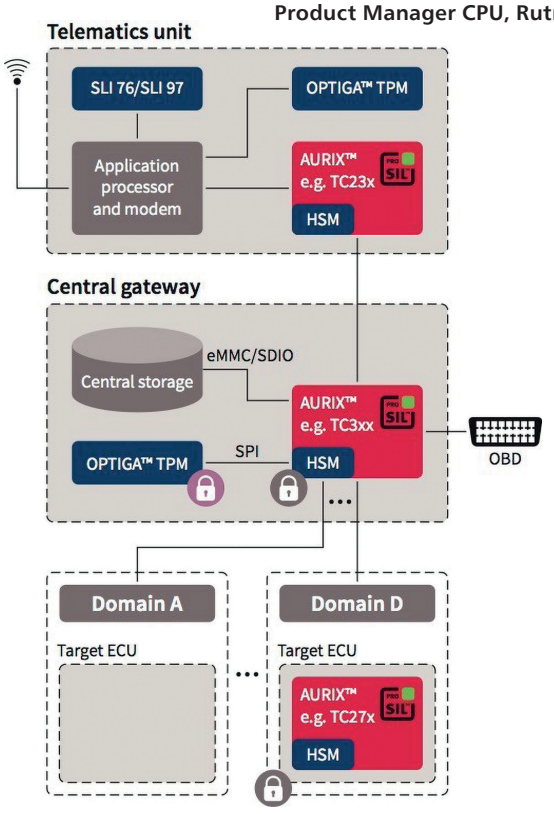
Oprócz kompleksowej komunikacji między serwerem OEM a docelową jednostką sterującą, architektura pojazdu współpracująca z SOTA może być realizowana za pośrednictwem trzech jednostek sterujących (bloków ECU): sterownik telematyki, brama centralna i docelowa jednostka sterująca. Usługi autoryzacji i szyfrowania są aktywowane w module telematyki za pośrednictwem połączenia radiowego, a następnie przesyłane dane (od producenta OEM) są odbierane i/lub deszyfrowane za pomocą protokołu bezpiecznego. W wypadku krytycznej funkcji uwierzytelniania jest zalecane użycie kontrolera bezpieczeństwa TPM w celu ochrony kluczy i certyfikatów o kluczowym znaczeniu dla bezpieczeństwa. Następnie, w pamięci jednostki centralnej jest zapisywana aktualizacja oprogramowania. Po uwierzytelnieniu OEM i weryfikacji (w centralnej bramce), deszyfrowane są odpowiednie pakiety danych dla jednostek sterujących. Teraz rozpoczyna się faktyczny proces aktualizacji oprogramowania, przy czym pakiety danych wysyłane są do ECU w małych blokach. W ECU bloki danych są następnie odszyfrowywane, dekompresowane, a nowy kod zapisywany jest w docelowej pamięci flash ECU za pomocą bootloadera Secure Flash.

Bootloader Secure Flash jest ważnym elementem procesu SOTA w jednostce sterującej. Główne funkcje bezpieczeństwa są wykonywane, na przykład, przez HSM w mikrokontrolerze AURIX: bezpieczne uruchamianie, uwierzytelnianie, odszyfrowywanie i szyfrowanie, zarządzanie kluczami i sprawdzanie integralności. Autoryzacja dostępu do pamięci Flash zapobiega nieautoryzowanej manipulacji danymi w tejże pamięci. Dostęp do zasobów Flash jest dozwolony przez HSM tylko po pomyślnym uwierzytelnieniu centralnej bramy i po wysłaniu odpowiedniego polecenia. Po pomyślnej weryfikacji aktualizacji oprogramowania zostanie to zgłoszone serwerowi aktualizacji.

Podsumowanie

Nowoczesne komponenty półprzewodnikowe umożliwiają wykonanie systemów zabezpieczenia pojazdów zapewniających duży poziom bezpieczeństwa funkcjonalnego i odporność na cyberataki. Dzięki temu są chronione zarówno pojazd, jak i pasażerowie czy pozostali użytkownicy dróg. Producenci komponentów półprzewodnikowych, tacy jak Infineon oferują mikrokontrolery z rdzeniem 32-bitowym ze zintegrowanymi sprzętowymi modułami HSM, SIM, TPM, AES i innymi. Dodatkowo, są oferowane obsługujące je pakiety oprogramowania. Umożliwia to dostosowanie odpowiednich mechanizmów zabezpieczających do wymagań bezpieczeństwa określonej aplikacji, korzystanie ze sprawdzonych algorytmów kryptograficznych, takich jak AES i ECC, a także zapewnienie zgodności z normami, takimi jak SHE, EVITA i TPM. Zmniejsza to ryzyko i skraca czas opracowywania pojazdu przez producentów OEM, ich dostawców i podwykonawców.

Martin Motz
Product Manager CPU, Rutronik



Rysunek 5. Boki funkcjonalne interfejsu SOTA