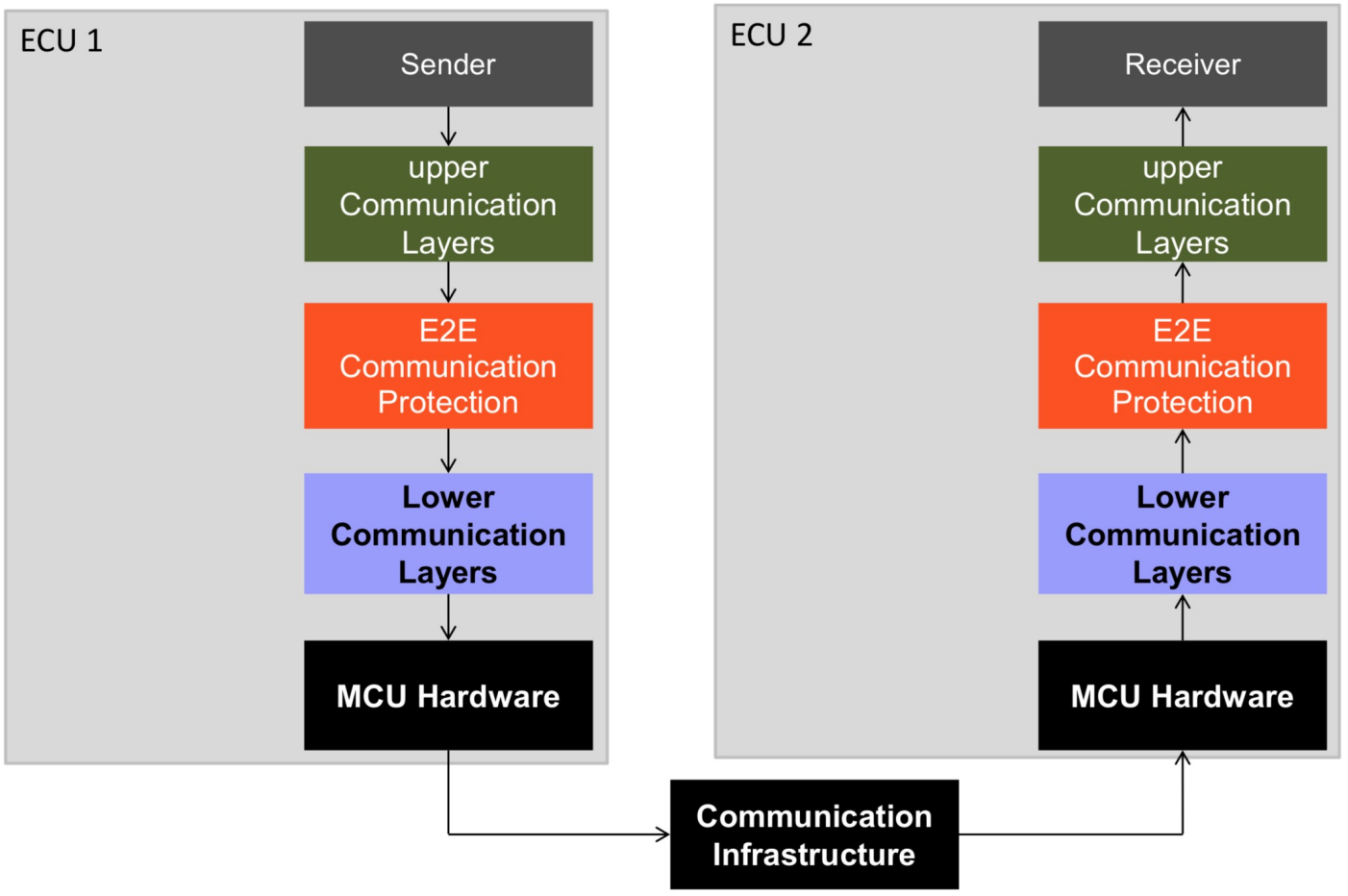
Bezpieczeństwo funkcjonalne - komunikacja

Infrastruktura komunikacji E2E



Wymagania stawiane komunikacji E2E w AUTOSAR

- Wymagania bezpośrednio odzwierciedlają zapisy ISO26262:2011 w zakresie:
  - Bezpieczeństwa funkcjonalnego i komunikacji
  - Źródeł błędów

Wykrywanie błędów E2E (1/2)

- Wykrywanie błędów w E2E, odbywa się w odniesieniu do:
  - Powtórzenia informacji (ang. repetition of information) – informacja odebrana jest więcej niż 1 raz
  - Utraty informacji (ang. loss of information) – całość lub część informacji została usunięta ze strumienia i nie dotarła do odbiorcy
  - Opóźnienia dostarczenia informacji (ang. delay of information) – informacja nadeszła później niż się tego spodziewano
  - Dodaniu informacji (ang. insertion of information) – dodatkowa informacja została dodana do strumienia
  - Maskarada informacji (ang. masquerade) – brak części uwierzytelniającej nadawcę informacji

Wykrywanie błędów E2E (2/2)

- Wykrywanie błędów (cd.):
  - Złe adresowanie informacji (ang. incorrect adressing) – informacja została zaakceptowana przy złym nadawcy lub odbiorcy
  - Utrata sekwencyjności informacji (ang. incorrect sequence of information) – informacja dotarła w nieodpowiedniej do spodziewanej kolejności
  - Uszkodzenie informacji (ang. corruption of information) – informacja została uszkodzona
  - Asymetria informacji (ang. asymmetric information) – informacja rozgłaszana do wielu odbiorców, dociera do nich w różnej postaci

Źródła błędów komunikacji E2E

- ISO26262 (a także AUTOSAR E2E), wyróżnia następujące źródła błędów:
  - Systematyczne błędy oprogramowania – systematycznie powtarzają się więc… źródłem jest oprogramowanie (w praktyce złe zarządzanie buforami lub kolejkami)
  - Losowe błędy sprzętu – nie da się przewidzieć/odtworzyć warunków zajścia błędu więc… źródłem jest sprzęt (upływności, pojemności pasożytnicze …)
  - Błędy zachodzą w wyniku zmiany warunków zewnętrznych – źródło błędu jest systematyczne lub nie a wykluczono sprzęt więc… źródłem jest EMI, ESD, wilgotność, korozja, uszkodzenie mechaniczne, temperatura…

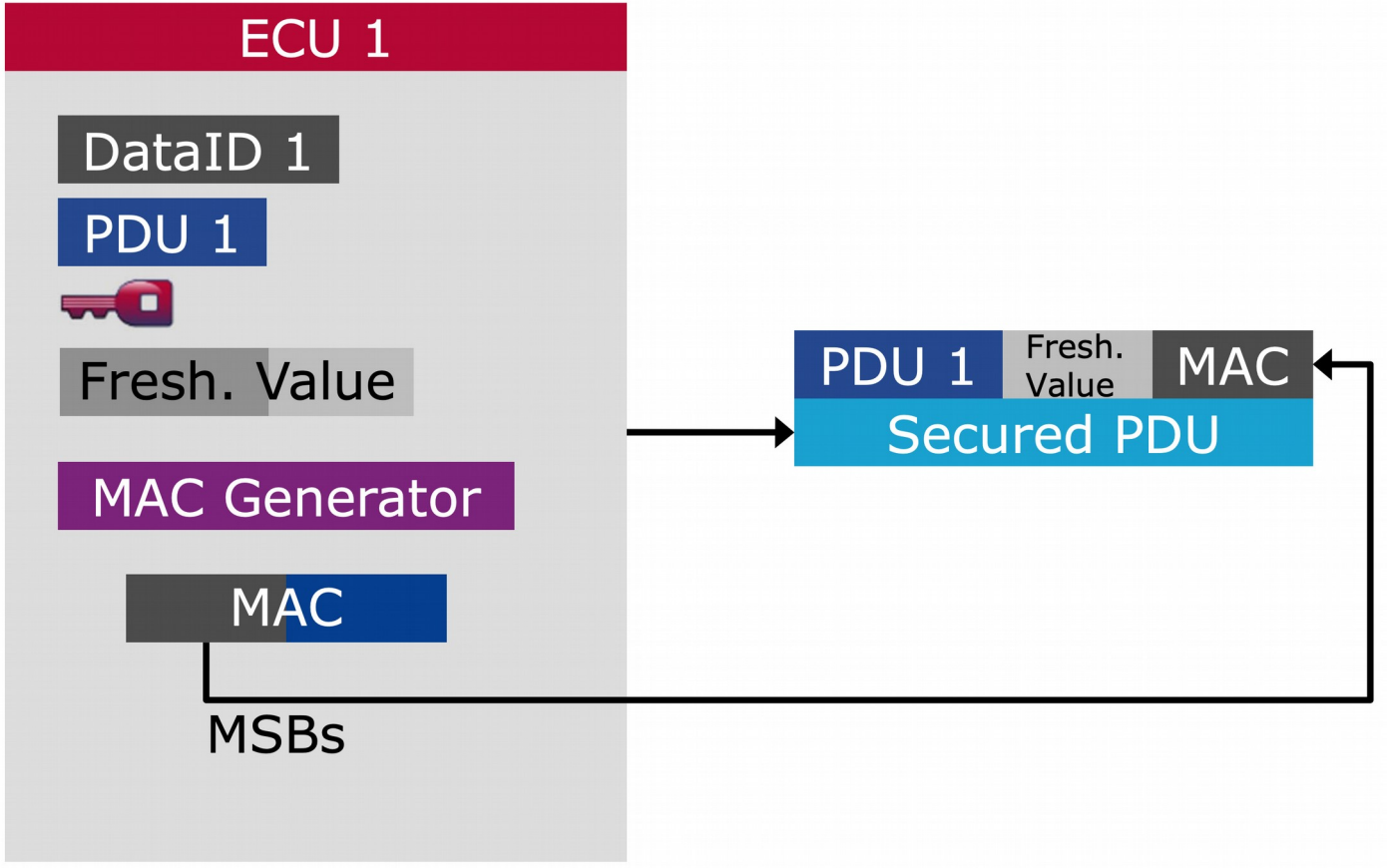
Protokoły komunikacji E2E

- Wybrany protokół komunikacji, powinien zapewniać wykrywanie tychże błędów na poziomie warstwy sprzętu jak i logiki
- Wymaga się by korekcja CRC na warstwie sprzętu i logiki bazowała na odmiennych wielomianach. Takie same redukują skuteczność wykrycia przekłamania:
- W warstwie sprzętu:
  - CAN – 8-bit
  - FlexRay – 16-bit
  - Ethernet – 32/64-bit
- Komunikacja powinna wspierać funkcję timeout oraz restartu nadawania
- Warstwa sprzętowa powinna być obsługiwana z niezawodnością ASIL D

Profile komunikacji E2E

- Profile komunikacji E2E, odpowiadają modelowi uszkodzeń (ang. fault model) z ISO26262
- Różnią się jedynie dobranymi mechanizmami sumy kontrolnej, liczników i zachowań w przypadku wykrycia błędu
- Zawierają:
  - Sumę kontrolną CRC
  - Licznik (niewielki 4-bitowy) inkrementowany w każdej transmisji
  - Licznik życia (ang. alive counter) – sprawdzana poprawna implementacja po stronie odbiorcy
  - Specyficzne ID dla danego ECU
  - Detekcję upływu czasu (ang. timeout)
- Poszczególne profile wyczerpująco opisane są w części Foundation → Protocols

Przesłanie bezpiecznego komunikatu (CSM) (1/2)



Przesłanie bezpiecznego komunikatu (CSM) (1/2)