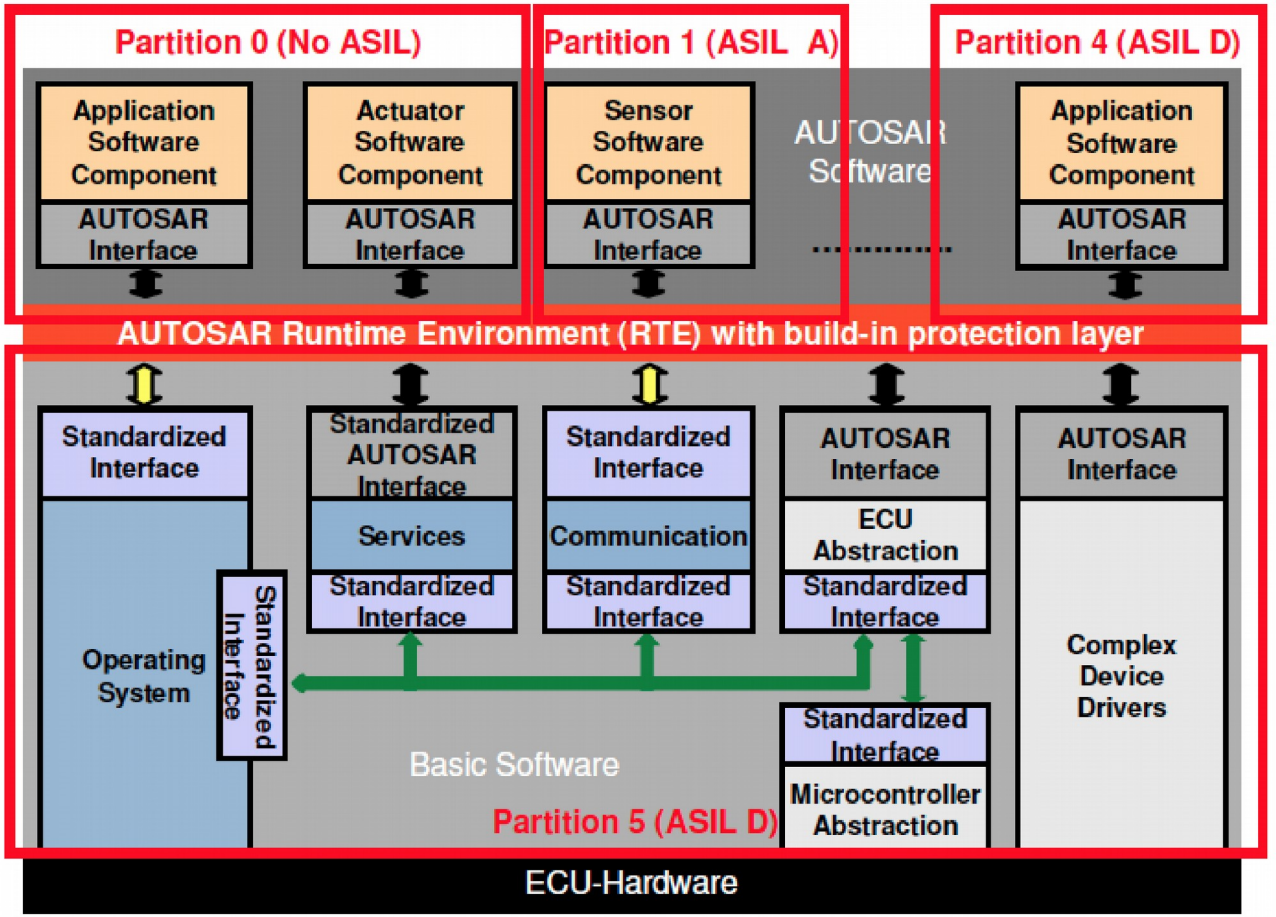
Mechanizmy bezpieczeństwa funkcjonalnego AUTOSAR dla platformy CLASSIC

Partycjonowanie ECU

- Wymagania stawiane systemowi operacyjnemu ECU (w ramach platformy classic), obejmują międzyinnymi:
  - Izolację pamięci danego komponentu oprogramowania
  - Statyczne zarządzanie priorytetami grup procesów
  - Wywłaszczenie w przypadku wystąpienia warunków przerwania na wysokim priorytecie
  - Konfigurowanie priorytetu każdego z zadań w ramach komponentu oprogramowania
  - Zachowanie reżimu czasu rzeczywistego
- Możliwe jest więc deterministyczne partycjonowanie zasobów z punktu widzenia potrzeb ASIL

Partycje BSW



Konfiguracja partycjonowania

- Partycjonowanie komponentów wymuszanie jest na etapie konfiguracji pojedynczego ECU i nie może ulec zmianie (jest statyczne)
- W ramach definicji RTE, można także dokonać autoryzacji BSW do wykonywania kluczowych operacji (np. wyłączenia samego ECU)
- Te defensywne właściwości obejmują także procedury odczytu i zapisu w pamięci NVM.
- Pamięć ta jest blokowa i zabezpieczona sumą kontrolną
- W przypadku jej błędu, blok może zostać odznaczony przez platformę jako uszkodzony (przewidziane są metody detekcji przed wystąpieniem takiego uszkodzenia i metody mirrorowania bloków)

Komunikacja E2E

- W trakcie konfiguracji platformy, można wymusić implementację profilu bezpieczeństwa komunikacji pomiędzy uczestnikami konwersacji
- Konwersacja może odbywać się pomiędzy wieloma ECU a także w ramach jednego ECU pomiędzy komponentami BSW
- Niezawodność warstwy sprzętowej zakładana jest na poziomie ASIL D

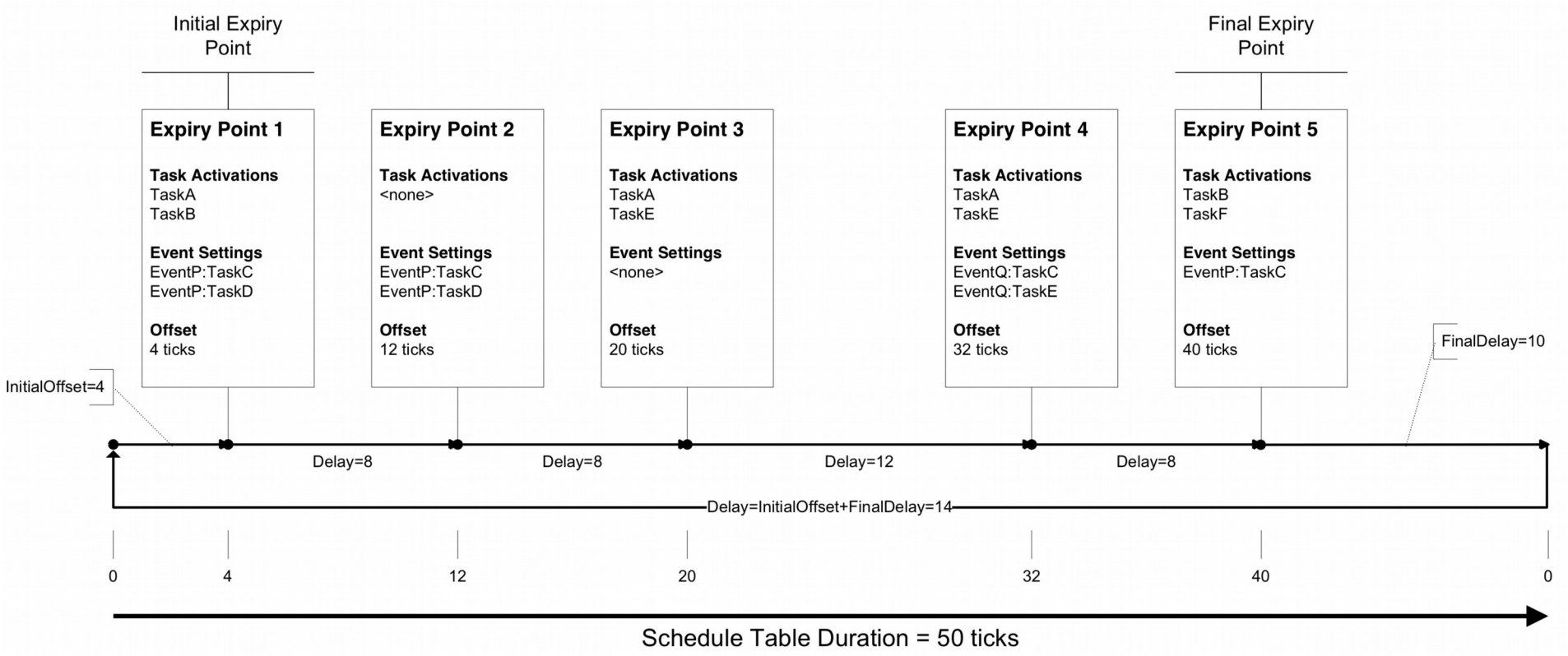
Monitorowanie logiki działania komponentu

- Na etapie projektowania, można uruchomić monitorowanie logiki działania programu
- W wybranych punktach, komponent oprogramowania odkłada informacje w sekwencji (czasu i wartości) świadczących o jego prawidłowym działaniu.
- Nadzorca kontroluje te wartości i w przypadku odstępstwa, może wykonać operację restartu samego komponentu lub wręcz całości ECU
- Mechanizm nadzorcy działa na poziomie nadrzędnym dla innych zadań

Synchronizacja czasu

- Synchronizacja czasu ECU, może odbyć się z użyciem ogólnie znanego NTP lub dedykowanych (podstawa czasu z CAN - TTCAN, FlexRay….)
- Podstawa czasu służy także do kontroli pracy zadań asynchronicznych i szeregowania zadań w slotach czasowych

Tablica szeregowania zadań



Przekroczenie reżimu czasu

- Jeśli zadanie nie będzie ukończone w przewidzianym dla niego slocie czasu, nadzorca może wykonać operacje związane z:
  - Restartem samego zadania/grupy zadań
  - Wyłączeniem danej tablicy zadań
  - Wykonać inne operacje (nawet wpływające na całe ECU)
- Pojedyncze ECU może obsługiwać wiele tablic zadań z których każda może posiadać własny konfigurowany statycznie priorytet
- Dopuszcza się (ale obecnie nie wymaga) by platforma sprzętowa posiadała wiele rdzeni
- Każdy z nich ma jednak na stałe przypisane tablice zadań

Programowany Watchdog

- Podsystem zarządzania WatchdogManager, umożliwia uruchomienie działania w wyniku:
  - Przekroczenia reżymu czasu (ang. deadline)
  - Po przekroczeniu czasu absolutnego (ang. alive)
  - W reakcji na wystąpienie błędów logiki uruchomienia (ang. Logical supervision)
- Uruchomienie akcji to nie tylko restart platformy sprzętowej ale także uruchomienie innej akcji (np. kontrolowanego wyłączenia komponentu sprzętowego lub ECU)

Właściwości programowe platformy

- Językiem referencyjnym dla budowania oprogramowania dla ECU jest C
- Inne języki są dopuszczalne lecz wymagana jest od nich umiejętność wykonania wywołań z języka C
- Platforma powinna posiadać instrukcje atomowe (jednostkowe operacje) oraz instrukcje z rodziny test_and_set
- Wymagany jest od platformy sprzętowej mechanizm wyłączenia na żądanie (w trakcie statycznej konfiguracji), wyłączenie przestrzeni adresowych z buforowania poprzez cache
- Wymagane jest mechanizm oznaczania kodu jako uprzywilejowany i nie
- Niezbędne jest także zachowanie mechanizmów komunikacji poprzez pamięć współdzieloną na poziomie sprzętu a nie oprogramowania RTOS

Komunikacja wieloma drogami

- W celu zapewnienia niezawodnej komunikacji, systemy mogą mieć definiowane wiele ścieżek przesyłania komunikatu
- Szyny mogą być statyczne aktywowane na etapie statycznej konfiguracji jako active-active (połączenie pasma), mirror (zwiększenie niezawodności), active-standby (uruchomienie zapasowej drogi przesyłu danych)
- Mechanizmy takie występują także na poziomie sprzętu (np.. CAN)
- Zarządzaniem elementami sieci, zajmuje się dedykowany komponent NM (ang. Network Manager)
- Dane BSW, może zgłosić do niego także zapotrzebowanie na pasmo komunikacyjne lub zgłosić że już jest ono niepotrzebne

Mechanizmy bezpieczeństwa AUTOSAR – podsumowanie

- Statyczna alokacja (czas, zasoby) oraz wydzielone przestrzenie pamięci
- Pamięć wirtualna – w CLASSIC nie jest specyfikowana
- DAC i MAC – nie jest specyfikowany explicite
- Filtr pakietów (ang. firewall) – możliwe proste odrzucenie pakietu(ów), brak nadzorcy komunikacji
- MAC – pełna specyfikacja ze wsparciem sprzętowym
- Kontenery – słabe zabezpieczenie na poziomie wydzielonych SSW
- Hypervisor – jedynie mechanizmy szeregowania bez dedykowanych mechanizmów sprzętowych