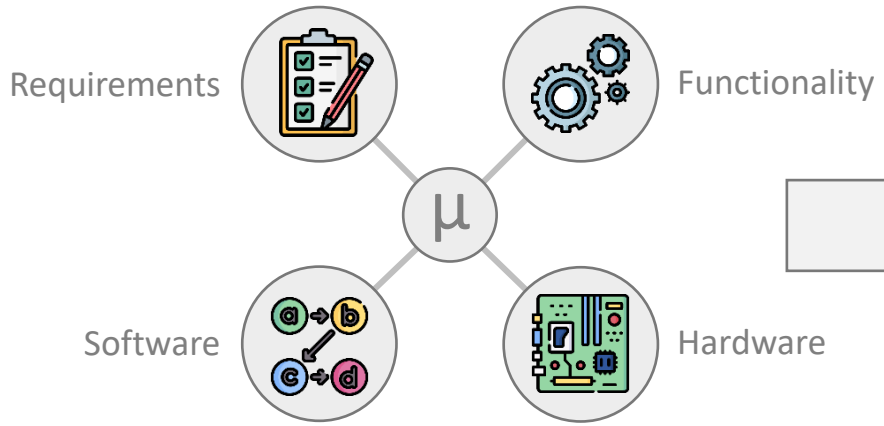
µRTE

A modeling framework for safe code on (Multi-Core) Controllers

Modeling Overview

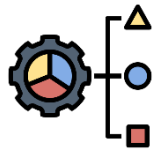
Scope



µRTE model

Generator

Code Frame
Activation Framework
Data encapsulation



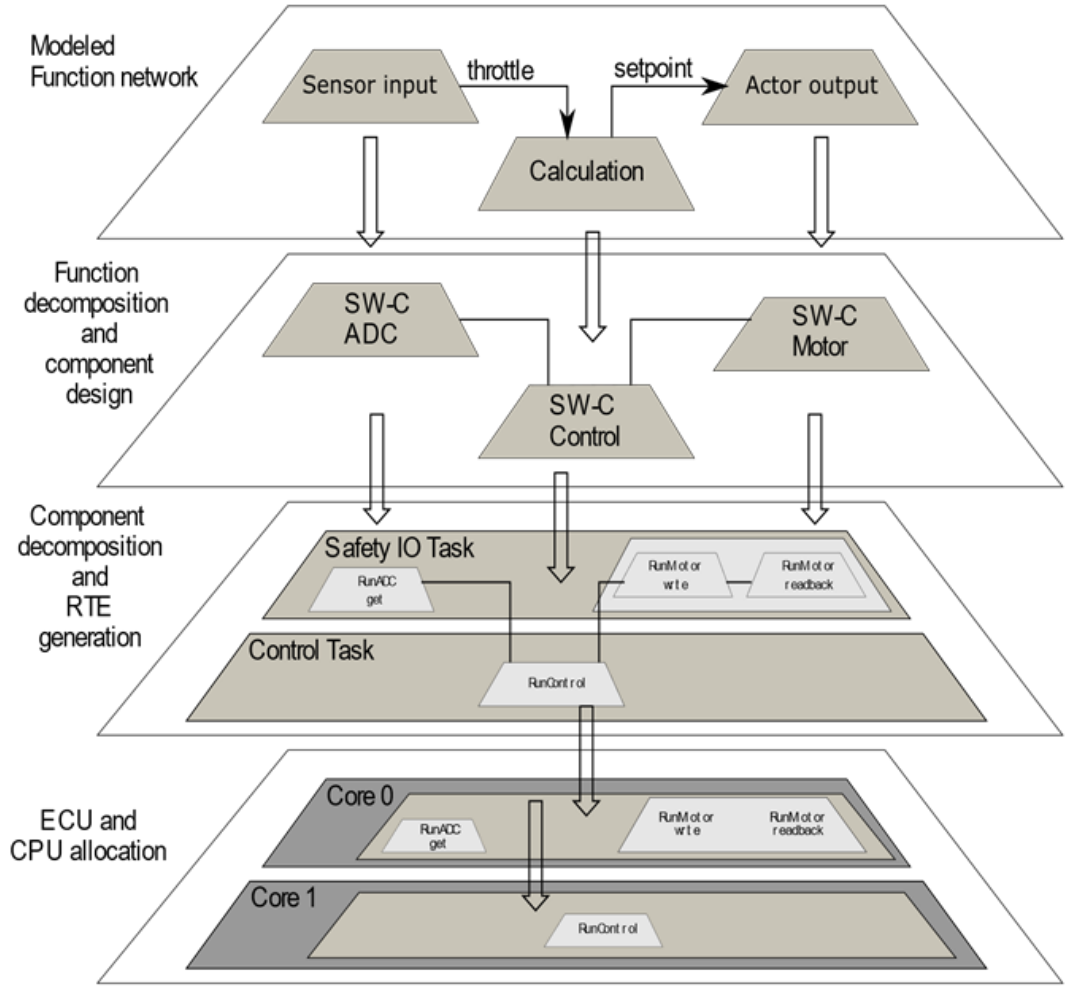
Memory allocation
Memory protection

Report

Test Frame (WIP)

Software modeling

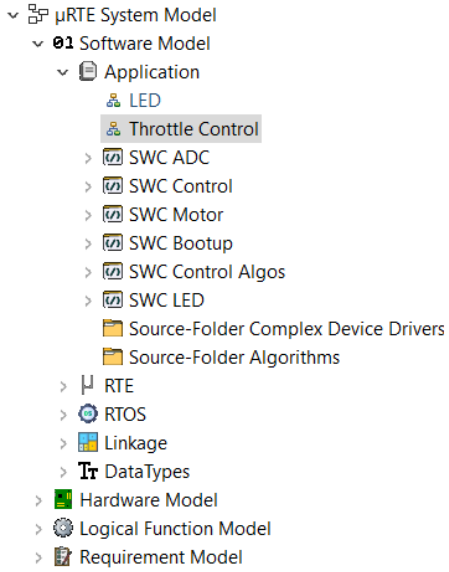
Abstract overview

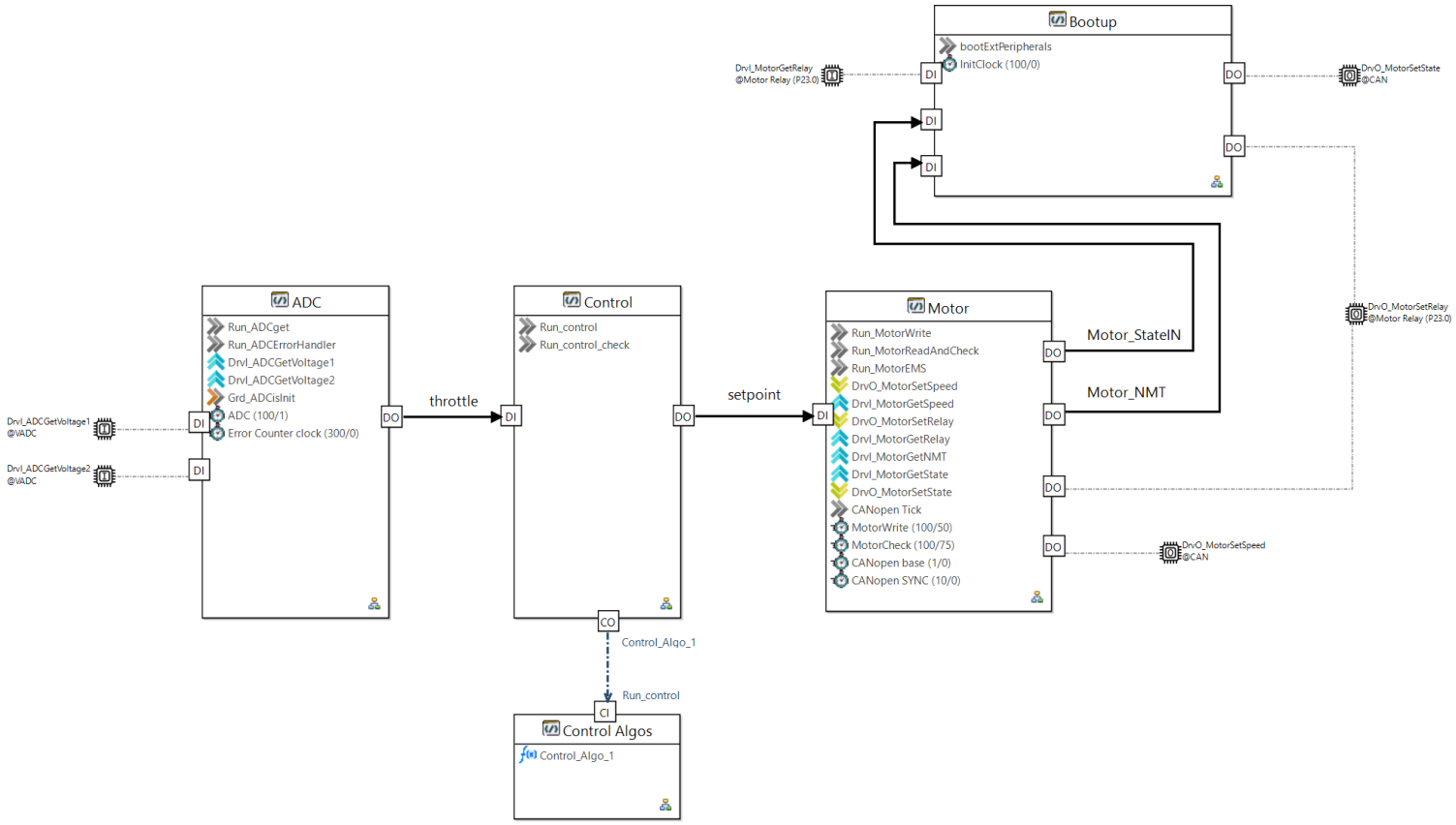


µRTE **Modeling overview**

Software modeling

Each block represents a code file in which software functions are contained
Arrows represent data exchange
Chip-Icons represent hardware interfaces

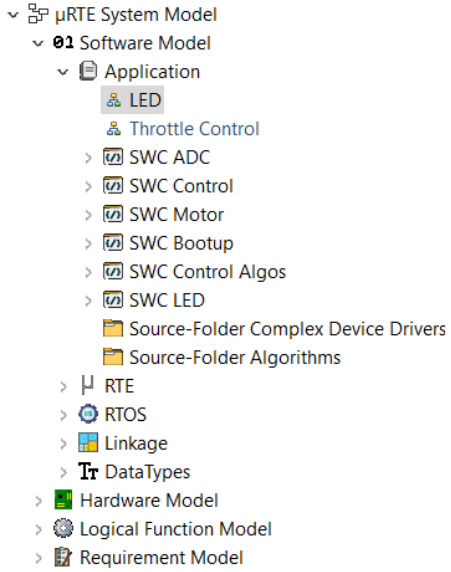


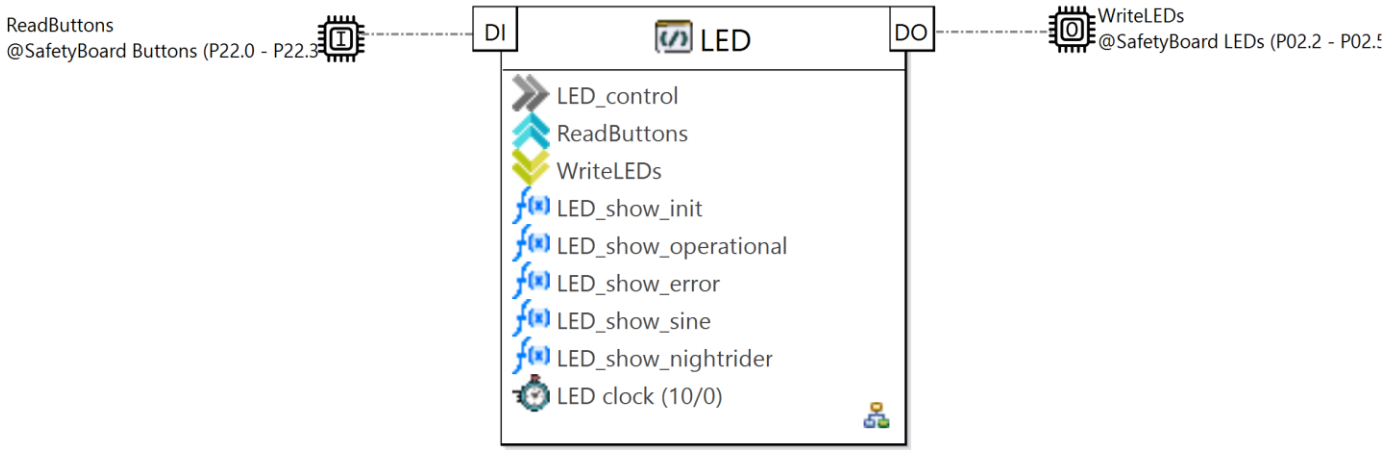


µRTE **Modeling overview**

Software modeling

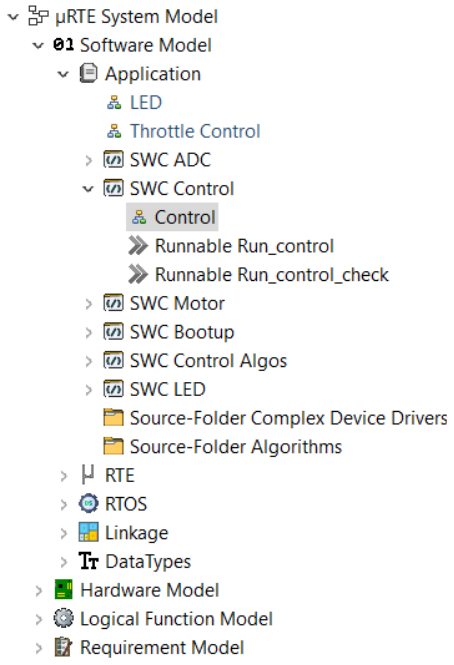
General concept:
Multiple diagrams within the same model possible with selectable data visualized.
Each graphical element can be selected and edited directly.
Rich toolset for diagram editing based on the SIRIUS framework.

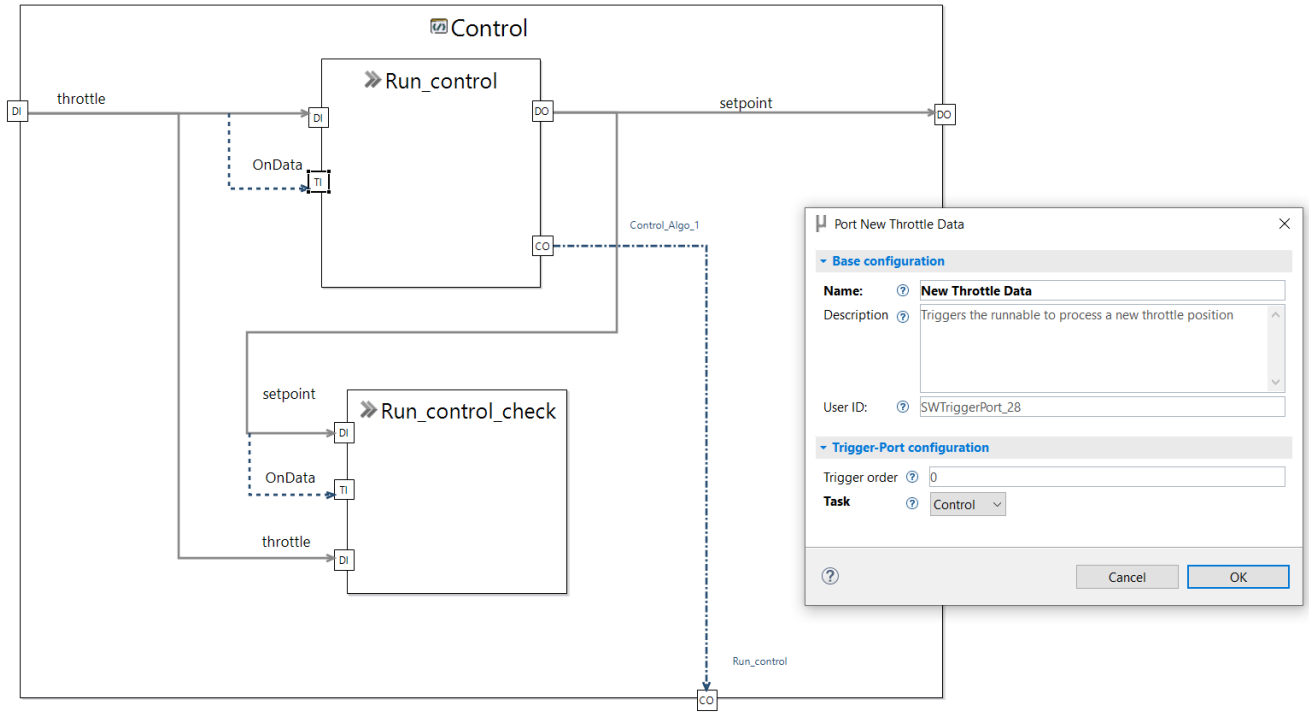




Software modeling

Detailed view describes runnable execution

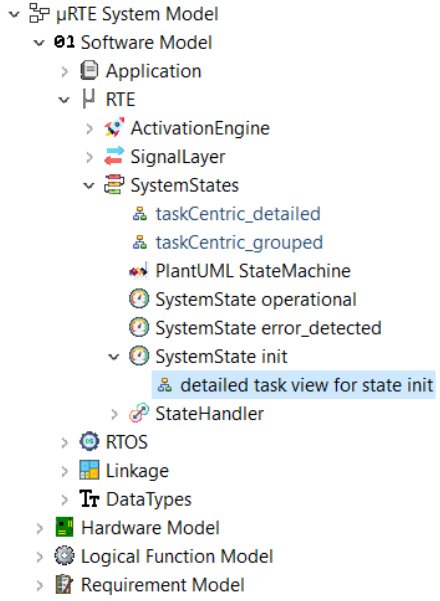


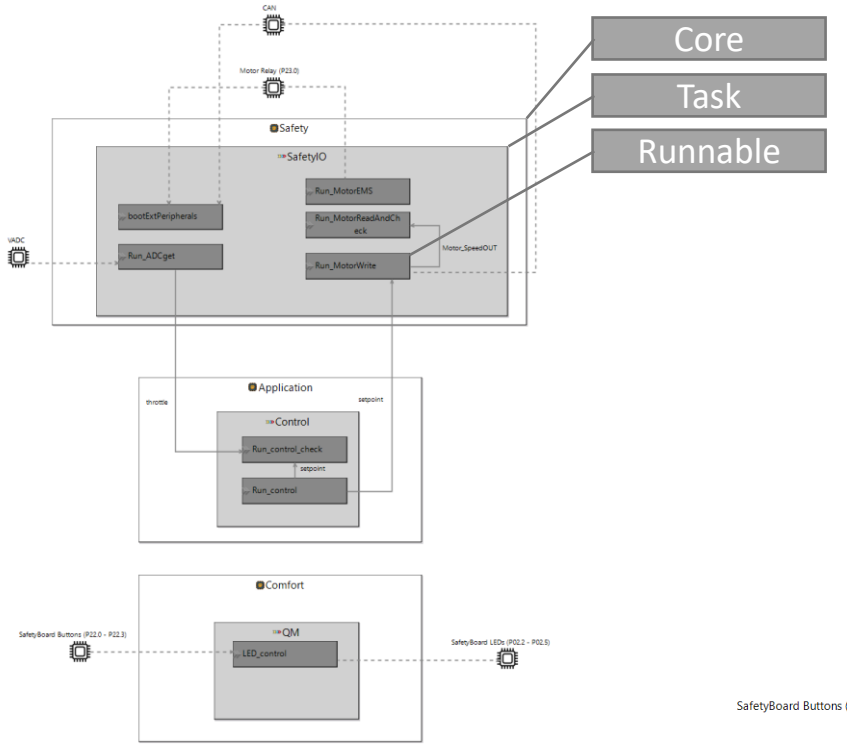


µRTE **Modeling overview**

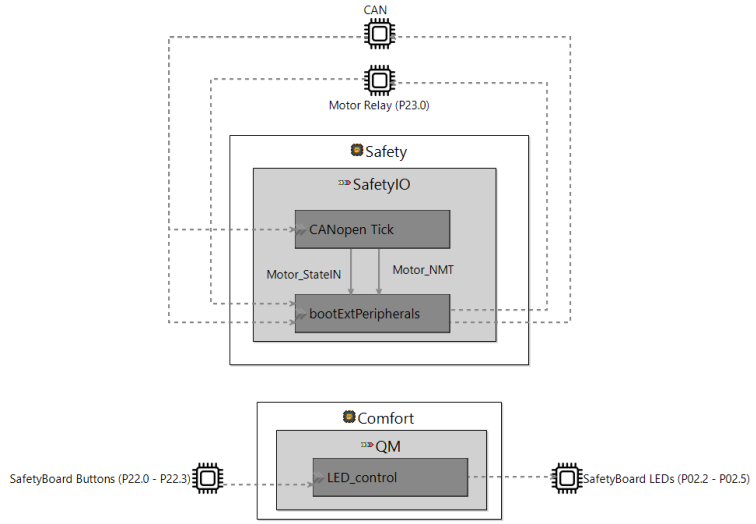
Software modeling

Core/Task centric views for the data-flow
Also for specific system-states
Shows which software is active and which data is accessed





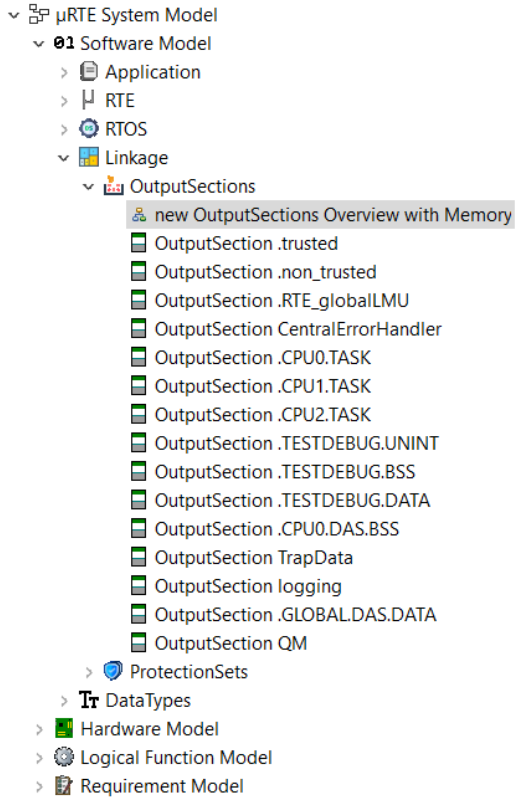
General Flow

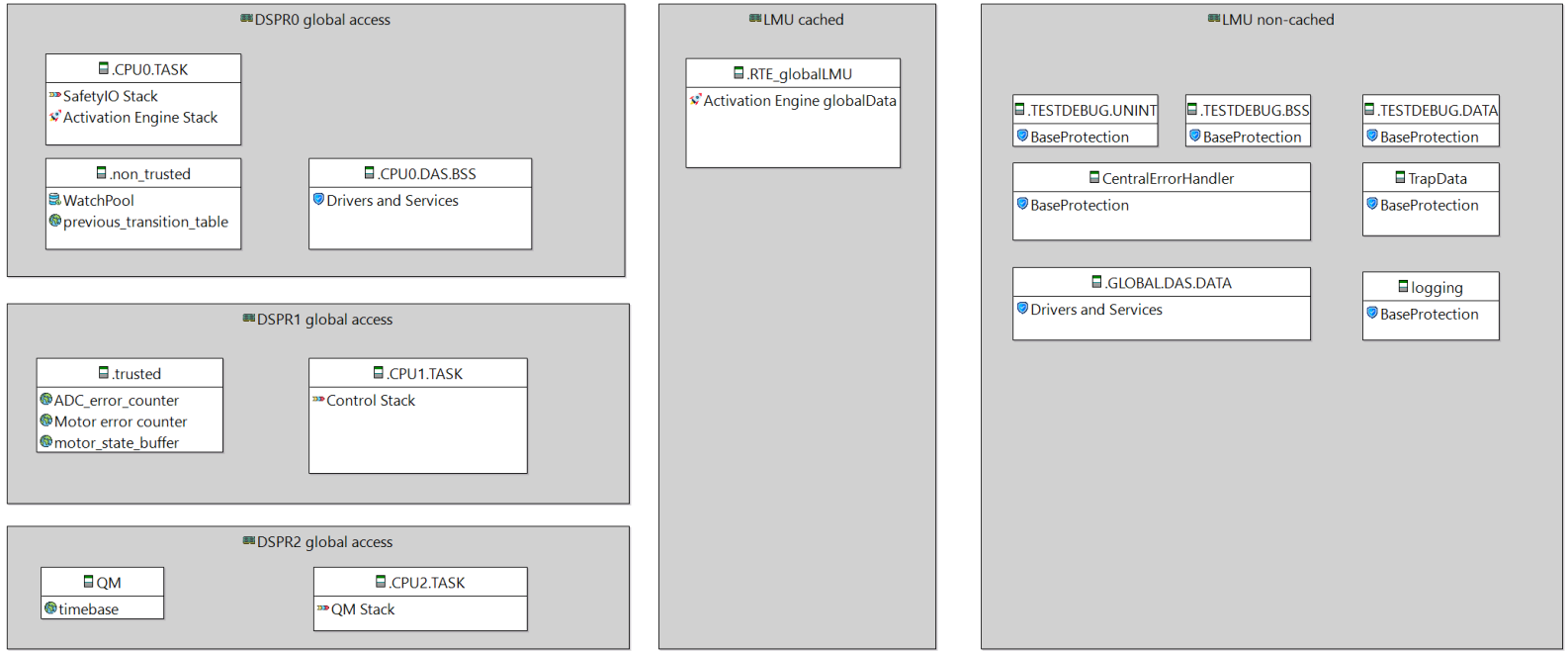


Init-State

Software modeling

Linkage overview:
memory modules with outputsections and references to the outputsections

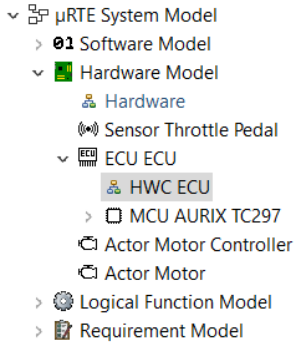


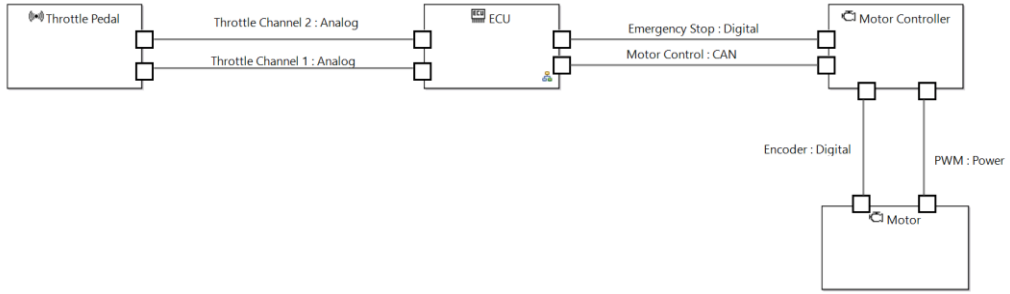


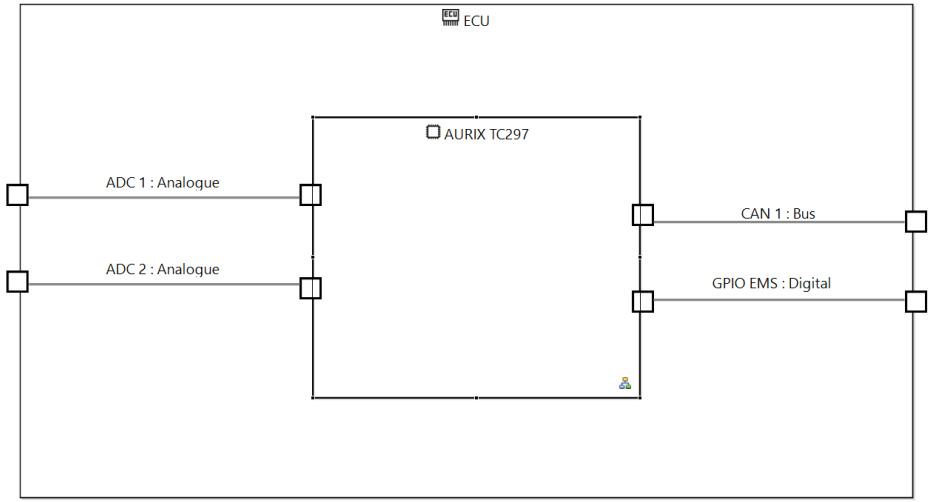
µRTE

Hardware modeling

Modeling of functional and non-functional components
Hierarchical graphical representation



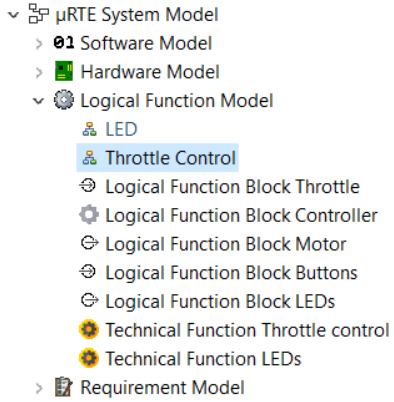


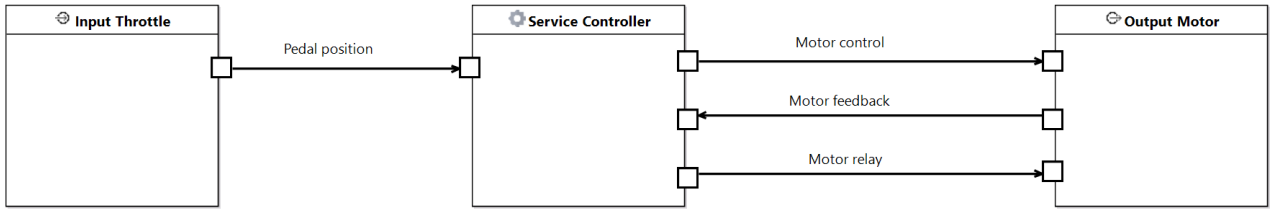


µRTE **Modeling overview**

Functional modeling

Abstract representation of the system functionality

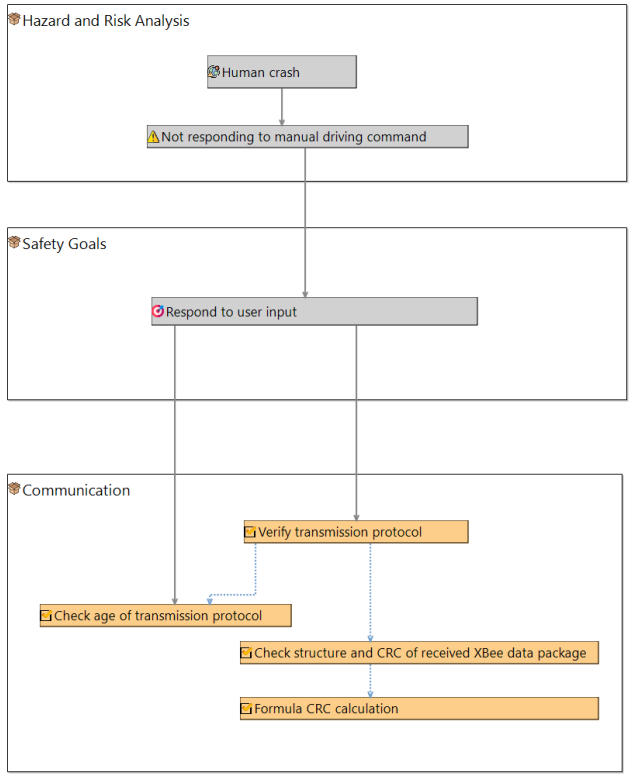




Requirements modeling

Derivation of requirements
Relationship (refinement/conflict) among requirements
Mapping to implementation units

- µRTE System Model
  - Software Model
  - Hardware Model
  - Logical Function Model
  - Requirement Model
    - Overview
    - Package Top Level Requirements
    - Package Hazard and Risk Analysis
      - Hazardous Event Not responding to manual driving command
      - Hazardous Event Not detecting obstacle
      - Hazardous Event Wrong actuator action
      - Hazardous Event Wrong targetspeed / controlspeed calculation
      - Hazard Scenario Human crash
    - Package Safety Goals
      - Safety Goal Respond to user input
      - Safety Goal Stop in front of obstacle
      - Safety Goal Supervise engine
      - Safety Goal Plausibility of targetspeed values
    - Package Communication
      - Safety Requirement Verify transmission protocol
        - refined by Check structure and CRC of received XBee data package
        - refined by Check age of transmission protocol
      - Safety Requirement Check age of transmission protocol
      - Requirement Dispatch received protocol



µRTE **Modeling overview**

Modeling in general

Besides graphical editing any element in the model can be edited with a lightweight GUI
The model is saved as XML for good manageability