Main ECU Software Requirements Analysis

# Rules

## A6.4.6

The following listed requirements are considered the minimum of what should be met to qualify as a safe testing/running environment. This does not mean that following these guidelines guarantees safety under all circumstances:

* Working TSAL, IMD, AMS, ASSI, RES, EBS, APPS/brake pedal plausibility check, APPS, and ETC plausibility check if applicable.

## System Critical Signals:

### T 10.3 System Critical Signals (SCSs)

#### T 10.3.1

System critical sensor signals and system critical general signals are defined as all electrical signals which Influence actions on the shutdown circuit, see CV 4.1 and EV 5.1

* Influence the requested wheel torque.
* [EV ONLY] Influence indicators according to EV 3.7.6, EV 4.13 or EV 5.4.6.
* ~~[DV ONLY] Influence indicator according to DV 3.2.5.~~

#### T 10.3.2

Any of the following signal failures must result in a safe state of all connected systems:

1. Failures of signals transmitted by wire:
   * Open circuit
   * Short circuit to ground
2. Failures of analog sensor signals:
   * Short circuit to supply voltage
3. Failures of sensor signals used in programmable logic:
   * Implausibility due to out of range signals, e.g. mechanically impossible angle of an angle sensor.
4. Failures of digitally transmitted signals by wire or wireless:
   * Data corruption (e.g. checked by a checksum)
   * Loss and delay of messages (e.g. checked by transmission time outs)

Signals might be a member of multiple signal classes, e.g. analog signals transmitted by wire might be member of (a), (b) and (c).

#### T10.3.3

Indicators per T 10.3.1 with safe state “illuminated” (e.g. absence of failures is not actively indicated) must be illuminated for 1 s to 3 s for visible check after power cycling the Grounded Low Voltage Master Switch (GLVMS).

## Brake Signal:

### EV 2.3 Brake System Encoder (BSE)

#### EV 2.3.1

A BSE or switch to measure brake pedal position or brake system pressure must be fitted to check for plausibility, see EV 2.4. ~~[DV ONLY] The BSE must be a pressure type.~~

#### EV 2.3.2

The encoder must have a connector that allows disconnection of the encoder signal during technical inspection.

#### EV 2.3.3

The encoder signal is a system critical signal, see T 10.3.

#### EV 2.4 APPS / Brake Pedal Plausibility Check

#### EV 2.4.1

The power to the motors must be immediately shut down completely if the mechanical brakes are actuated and the APPS (see T 10.2) signals more than 25 % pedal travel at the same time. This must be demonstrated when the motor controllers are under load.

#### EV 2.4.2

The motor power shut down must remain active until the APPS signals less than 5 % pedal travel, no matter whether the brakes are still actuated or not.

### EV 4.10 Activating the Tractive System

#### EV 4.10.5

After the tractive system has been activated, additional actions must be required by the driver to set the vehicle to ready-to-drive mode (e.g. pressing a dedicated start button). One of these actions must include the brake pedal being pressed while ready-to-drive mode is entered

## APPS

### T10.2 Accelerator Pedal Position Sensor (APPS)

#### T10.2.1

Rules T10.2 only apply for electric vehicles, see chapter EV, or internal combustion vehicles using Electronic Throttle Control (ETC), see CV1.6.

#### T10.2.2

The APPS must be actuated by a foot pedal.

#### T10.2.3

Pedal travel is deﬁned as percent of travel from fully released position to a fully applied position where 0 % is fully released and 100 % is fully applied.

#### T10.2.4

The foot pedal must return to the 0 % position when not actuated. The foot pedal must have a positive stop preventing the mounted sensors from being damaged or overstressed. Two springs must be used to return the foot pedal to the 0 % position and each spring must work when the other is disconnected. Springs in the APPS are not accepted as return springs.

#### T10.2.5

At least two separate sensors must be used as APPSs. Separate is deﬁned as not sharing supply or signal lines.

#### T10.2.6

If analog sensors are used, they must have different transfer functions, each having a positive slope sense with either different gradients and/or offsets to the other(s). This will insure that even in case of a short circuit of the signal lines the APPSs will only agree at 0 % pedal position.

#### T10.2.7

The APPS signal is a System Critical Signal, see T10.3.

#### T10.2.8

If an implausibility occurs between the values of the APPSs and persists for more than 100 ms

* [EV ONLY] The power to the motor(s) must be immediately shut down completely. It is not necessary to completely deactivate the tractive system, the motor controller(s) shutting down the power to the motor(s) is sufﬁcient.

~~• [CV ONLY] The power to the electronic throttle must be immediately shut down.~~

#### T10.2.9

Implausibility is deﬁned as a deviation of more than ten percentage points pedal travel between any of the used APPSs or any failure according to T10.3.

#### T10.2.10

If three sensors are used, then in the case of an APPS implausibility, any two sensors that are plausible may be used to deﬁne the torque target and the 3rd APPS may be ignored.

#### T10.2.11

Each APPS must have a separate detachable connector that enables a check of these functions by unplugging it. If not, an inline switchable break-out box must be made available during technical inspection that allows disconnection of each APPS signal

#### T10.2.12

A fully released accelerator pedal must result in:

* [EV ONLY] A wheel torque of ≤0 Nm
* ~~[CV ONLY] An idle position or lower throttle set-point. This may only be exceeded during a gearshift~~
* ~~for maximum 500 ms.~~

## Brake Pedal Plausibility Check

### EV2.4 APPS / Brake Pedal Plausibility Check

#### EV2.4.1

The power to the motors must be immediately shut down completely if the mechanical brakes are actuated and the APPS (see T10.2) signals more than 25 % pedal travel at the same time. This must be demonstrated when the motor controllers are under load.

#### EV2.4.2

The motor power shut down must remain active until the APPS signals less than 5 % pedal travel, no matter whether the brakes are still actuated or not.

## EV 3 TRACTIVE SYSTEM ENERGY STORAGE

## EV3.7 Accumulator Management System (AMS)

#### EV3.7.6

The AMS must switch off the tractive system by the shutdown circuit, if critical voltage, temperature or current values according to the cell manufacturer’s datasheet or this rules are detected. The accuracy of the measurement must be taken into account for this. A red indicator light in the cockpit that is easily visible even in bright sunlight and clearly marked with the lettering “AMS” must light up if the AMS opens the shutdown circuit. It must stay illuminated until the error state has been manually reseted, see EV5.1.6. Signals controlling this indicator are SCS, see T10.3.

#### EV3.7.7

The action of opening the shutdown circuit may be delayed by 250 ms to signal the failure to the motor controllers and reduce the tractive system current before the AIRs are opened.

#### EV3.7.10

All voltage, temperature and current signals are system critical signals, see T10.3.

## EV4 Tractive System General Requirements

### EV4.10 Activating the Tractive System

#### EV4.10.1

The driver must be able to activate and deactivate the tractive system from within the cockpit without the assistance of any other person.

#### EV4.10.3

The vehicle is ready to drive as soon as the motor(s) will respond to the input of the APPS.

#### EV4.10.4

Closing only the shutdown circuit must not set the vehicle to ready-to-drive mode.

#### EV4.10.5

After the tractive system has been activated, additional actions must be required by the driver to set the vehicle to ready-to-drive mode (e.g. pressing a dedicated start button). One of these actions must include the brake pedal being pressed while ready-to-drive mode is entered.

#### EV4.11 Ready-To-Drive Sound

#### EV4.11.1

The vehicle must make a characteristic sound, continuously for at least one second and a maximum of three seconds when it enters ready-to-drive mode.

## Motor

# Internal requirements:

## GLV:

Voltage monitoring.

# Additional requirements

## Sensors list:

### Wheel speed sensors

### Suspension displacement sensors

### IMU and accelerometer

### Dashboard info

### Telemetry info

## Building blocks list

### CAN

#### Main, PT, AMS

### Setups

### PowerMode

### Diagnostics

### Sensors

### Vehicle Dynamics

### Inverters

### Indicators

### AMS

### Calibration