Safety Node

Links:

[Safety Node.docx](https://uoafsae.sharepoint.com/:w:/s/F1-Tenth/EX0ZGIR_mPVFqyPslDIBN8sBAutkobgWWH_kE36s13Lx9w?wdOrigin=TEAMS-MAGLEV.undefined_ns.rwc&wdExp=TEAMS-TREATMENT&wdhostclicktime=1750914761724&web=1) - Brief

### **FSG25\_AS\_Beginners\_Guide\_v1.0.pdf - in general files**

### **FS-Rules\_2024\_v1.0 - EBS Checkoff.pdf pp68 - in general files**

Rules and guidelines - beginners guide

In rules - T14 & T15

**Data in**

Ackerman message - throttle, steering, angular velocity, acceleration, jerk?

From CAN to safety - break sensors, power status, if breaks are engaged

**Data Out**

From safety to CAN - reflecting what we got from ackerman (modified to be within particular range)

From safety to assi - status

Project Timeline

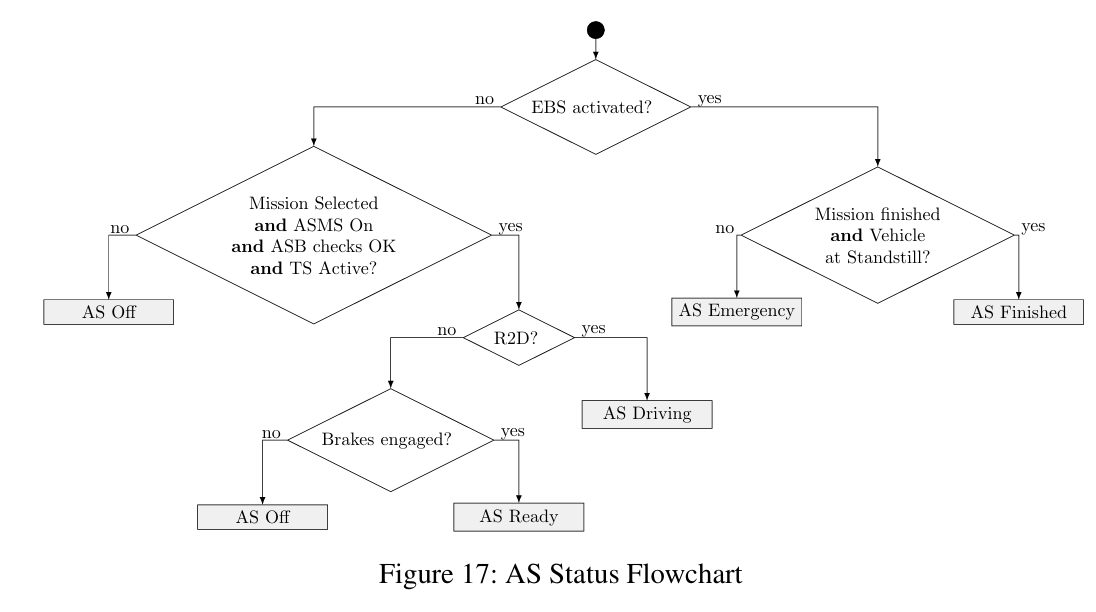
* Read rules
* Formulate full requirements list for node
* Find existing files to connect to
* New node
* Pseudo code

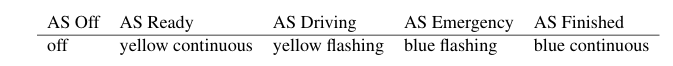
SYSTEM CRITICAL SYSTEMS

Signal monitoring is an essential part of every well-engineered system. It is required to

achieve functional safety goals and prevent uncontrolled behavior of the AS. Concerning the functional safety goals, the system must transition to the safe state as soon as it cannot ensure a fully redundant emergency brake maneuver. In case of a signal failure, it might not be possible to properly diagnose the system. Therefore the safe state has to be entered. This could be either a broken wire, a faulty sensor with out-of range data, or a signal distorted by electromagnetic inferences. Concerning the high-level parts of the AS that rely on a variety of different sensor inputs, the system shall detect, if any of those is malfunctioning. If the proper vehicle operation cannot be ensured (e.g. loss of environmental perception) the system shall react by activating the EBS immediately. This significantly decreases the time between a failure and the brake maneuver compared to a brake maneuver that is manually triggered via the RES. This may protect the vehicle from crashing and thus should be in every team’s own interest to implement such a diagnosis properly. The signals that require such a monitoring are called System Critical Signals (SCSs). The respective monitorings for the EBS and the AS shall be implemented as described above.

**Status Indicator**





**Status Determining Factors**

Mission Selected, ASMS On, ASB checks ok, TS Active

R2D

Brakes Engaged

EBS Activated

Mission Finished + Vehicle Stationary

**Events**Response signal not found

**Possible vehicle states**

**AS Off**:

Explanation

* AS not fully functional yet

State

* TSAL lights up green
* engine not running
* ABS checked as operational -> transitions to AS Ready

**AS Ready**:

* ASMS on
* TS activated by ASR via TS activation button
* Brakes must be closed
* Watchdog on

**AS Driving**:

* vehicle has been launched via RES go signal
* Signals to CAN allowed to go through (Mission In Progress)
* Monitoring Watchdog signal
* Watchdog on

**AS Finished**:

* mission completed
* CAN messages are 0
* Breaks on
* only method of successfully completing driverless events.

**AS Emergency**:

* EBS has been activated (opening SDC via RES, or detecting internal failure)
* Watchdog on

**“AS Off**”: This status shows that the AS is not fully functional (yet) e.g. after switching the LVMS to “On”. In order to know if it is safe for anyone to approach the vehicle, the ASMS shall be checked to be in “Off” position and the TS shall be switched off ([EV ONLY] TSAL lights up green/[CV ONLY] Engine is not running). In any other case the vehicle might be about to either change its status to “AS ready”, see below, or is about to be driven manually, see chapter 13.

“**AS Ready**”: This status usually follows after “AS Off”, if the ASB is checked to be operational, the ASMS has been switched “On” and the TS is activated by the ASR via the external TS activation button. The vehicle is prepared to be launched soon but it is ensured that the brakes are still closed. Being in close distance to the ve hicle is only allowed for the ASR and the officials. The time the vehicle remains in “AS Ready” should be kept to the possible mini mum required due to the event procedure.

“**AS Driving**”: The vehicle has been launched via the go signal sent by the RES (considering the safety delay of 5s, see Figure 2) and is allowed to execute its mission. It has to be expected that the vehicle moves suddenly or conducts any other dangerous behavior. It is strictly forbidden for anyone to approach the vehicle.

“**AS Finished**”: The AS considers the mission to be completed, the vehicle has reached standstill and changed its status to “AS Finished” on its own behalf. Any of the driverless dynamic events is only considered to be successfully completed, if the vehicle comes to a stop in the designated area and enters “AS Finished” (no Un safe Stop (USS)). The vehicle must be retrieved by the ASR and an additional team member immediately after approval from the officials.

“**AS Emergency**”: The EBS has been activated, see T14.8.1. This can be either caused by opening the SDC (e.g. by pressing the shutdown button on the RES remote device) or in case the vehicle has detected an internal failure. After coming to a full stop the vehicle must be retrieved by the ASR and an additional team member immediately after approval from the officials.

“**Manual Driving**”: The vehicle is operated in manual mode. This is only possible, if all actuators are switched off via the ASMS and the AShascheckedthattheASBcannot interact with the brake system.

Manual Driving: only possible if all actuators are switched off via ASMS, AS has checked ASB not able to interact with the brake system.

ASSI: reflects current status via LED, additional speaker to warn of emergency

Startup procedure

(D2.6) has been defined which also limits the time to get to “AS Ready”. Thus, every

team should aim at minimizing the preparation time required in the queue or directly at

the starting line. This is not only a benefit to the event organization, but also reduces the

likelihood of failures. A typical startup may be performed (by the ASR) as follows:

1. Check and fill the energy storage of the ASB already inside the pit.

2. Move the vehicle to the dynamic area with the ASMS and LVMS in “Off” position and the ASB detached/decoupled (e.g. by shut-off valves).

3. Turn on the LVMS and check/setup the AS once the vehicle arrives in the preparation area.

4. Queue and wait to approach the starting line. The LVMS may remain in “On” position.

5. Make sure that the correct “e-key” is inserted into the RES: practice-key for technical inspection and testing race-key for dynamic events (will be provided by the officials)

6. Once the vehicle is properly aligned at the starting line, attach/arm the ASB (e.g. by operating the shut-off valves).

7. Double check that the steering actuator is connected to the steering system.

8. Select the correct mission and check on the AMI, if the selection of the mission has succeeded within the AS.

9. Turn on the ASMS and activate the TS after the approval of the officials. (Hint: Shutdown buttons and RES remote devices shall be checked in advance.)

10. Leave the area near the vehicle and proceed to the area designated for the ASR carrying the RES remote device.

11. Wait for the vehicle to reach “AS Ready” and send the go-signal after the approval of the officials.

### **Core Functions of a Safety Node**

1. **Health Monitoring**
   * Subscribes to key system topics: sensor status, localization confidence, controller output, velocity, etc.
   * Checks for missing or delayed messages (e.g., watchdog timers).
   * Monitors for anomalies like erratic steering, GPS jumps, or excessive speed.
2. **Decision Logic**
   * Defines safety conditions (e.g., emergency stop if speed > threshold and no valid control commands).
   * May use **finite state machines (FSM)** or **rule-based systems** to decide actions.
   * Optionally integrates with high-level mission logic or fallback modes.
3. **Control Override**
   * Publishes zero or safe values (e.g., brake hard, steer straight) to the vehicle's drive-by-wire system.
   * Can block unsafe commands from reaching actuators.
4. **Failsafe Trigger**
   * In serious cases, triggers:  
     + Emergency stop.
     + Switch to manual control.
     + Shutdown or recovery behavior.
5. **Communication with Human Operator**
   * Sends alerts via dashboard or telemetry.
   * Optionally logs data for post-race debugging or black-box recording.