Autonomous System Beginners Guide 2021/22

Martin Stollberger / Mathias Gebhardt
Nicolas Velz / Alexander Wischnewski / Moritz Hörsch

2021-11-24

Contents

Changelog

Section	Version	Change
	V0.9	Transferred the Emergency Brake System (EBS) Reference Guide to a more general Autonomous System (AS) guide and aligned it with the 2022 V0.9 Rules.
	V1.0	Updated to new common layout.
12.1	V1.0	Adapted logic location inside the Shutdown Circuit (SDC) to the new rules.
13	V1.0	Adapted component placement to most recent rules version

Abstract

This document is intended to give you – as a team – a reference for implementing the AS and ASB rules. Following this guideline eases the design of your vehicle and helps us to review the safety of your design faster. Following this guide does not automatically mean that you'll pass the Autonomous System Form (ASF) review or technical inspection. This guide only delivers some suggestions for your design. More complex solutions are still welcome. Finally it is still your responsibility to ensure a safe design and explain how the safety concept works. Be prepared for critical reviewer questions. This document does not replace or extend the rules. In case of a discrepancy, the rules always supersede this document.

Introduction

The references in this document are mainly based on the Formula Student Rules 2022 Version 1.0. Its main focus is to give a general overview on the different AS parts and especially on the implementation of the ASB. This document also gives a short introduction on failure detection and failure handling during startup and operation, see T15.3. Furthermore, some suggestions are made on how to design this system to be redundant.

Other topics are about the testability during technical inspection. As the ASB signals are part of the Autonomous System, they are considered to be System Critical Signals (SCSs), see T14.6.1 and there are some points which should be kept in mind. This will speed and ease up the Driverless (DV) inspection for all of us.

Note: All references to the rules and abbreviations are linked to the rules document. This link will only work if the browser integrated PDF viewer is used. Tested with Firefox, Chrome and Edge.

1 Datalogger

The intention of the data logger is to understand and reproduce the system state in case of failure, e.g. EBS is triggered due to range loss of the Remote Emergency System (RES). To achieve this, a basic set of signals defined in the competition handbook and a set of vehicle-individual signals that have to be monitored by the ASB are to be recorded by the datalogger. To be able to evaluate the recorded data, you need to provide a DBC file that provides a definition for all the signals mentioned above. A basic template for this file can be found on the FSG website. Further hints regarding the datalogger can be found in the competition handbook.

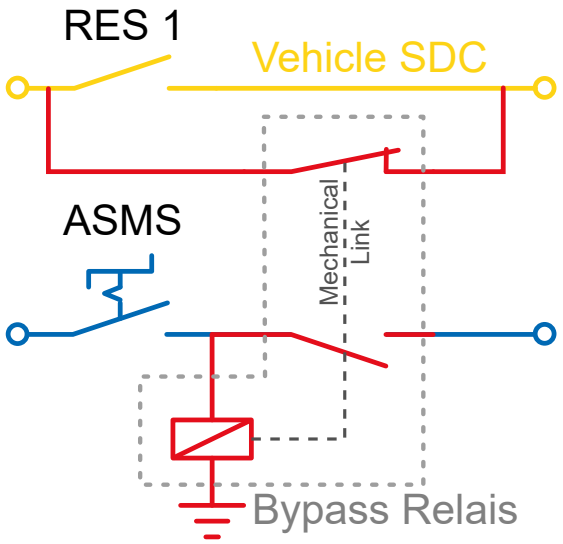

Figure 1: RES bypass circuit

2 Remote Emergency System

The Remote Emergency System (RES) is considered the most basic safety feature of the Driverless vehicle. It is connected to a vehicle side receiver unit, which is directly hard-wired into the shutdown circuit, see T14.4.4. Once the shutdown button on the RES is pressed or a signal loss occurs, the Tractive System (TS) is disabled and the EBS system gets activated. It is developed to meet the highest safety standards (SIL3). Details on its application within the vehicle can be found in Figure 6.

In addition, the RES is used to send the Go-Signal via an additional button to the vehicle. The RES receiver in the vehicle sends this signal on the CAN-Bus. The AS is only allowed to activate Ready-to-drive (R2D), if the go signal is received after a safety delay of five seconds, see Figure 2 in chapter 8.

To avoid problems during manual driving and to avoid that the RES is always required for normal (non-DV) testing, it is permitted to deactivate the RES in the 2022 rules. Due to the safety problems which may arise from this bypass the rules only permit one solution, which is shown in Figure 1. This circuit needs to be implemented thoroughly to avoid a non-functional RES.

Antenna mount: As one of it's safety features the RES will also open the SDC if the received signal strength drops below a certain threshold on the vehicles module. Thus, it is strongly recommended to place the RES-antenna away from metal parts and on a place with the least obstructions from any direction. It is also recommended to do some range tests for any vehicle orientation to find the optimal location for the RES-antenna. This will help to avoid problems during the competition, as the distances and obstacles may differ from your test area.

3 Shutdown Circuit

The SDC is the main control line for the TS within the vehicle. For a schematic overview see the rules figures 20 (CV) and 21 (EV). Closing it is a key step to get the vehicle Ready-to-drive (R2D). Therefore, it is important that all safety critical checks are passed before closing the SDC (and thus activating the TS). In addition to the vehicle specific requirements for CV and EV vehicles, the following has to be considered, also see T14.5.2:

Manual Mode: The AS has checked that the Autonomous System Master Switch (ASMS) is switched "Off" and the EBS system is not energized and cannot interact with the Brake System in any possible way. Activation of the EBS during manual driving may cause serious danger to the driver and might lead to uncontrolled vehicle behavior. Once all required conditions are met the TS

might be activated by the driver from within the cockpit, see EV4.11 and T14.1.2.

Autonomous Mode: The ASMS is switched "On" and the AS has checked that the EBS is energized. Only if all these required conditions are met, the TS might be activated by the Autonomous System Responsible (ASR) via the external activation button, see EV4.11.3/CV1.2.2.
Once the SDC is closed the vehicle is able to start moving, thus you need to ensure the brake system is working properly. Opening the SDC is a safety critical operation that must always be performed in a reliable way. It transitions the vehicle to a safe state as it includes:

- shutdown of the TS, i.e.
  - [EV ONLY] Accumulator Isolation Relays (AIRs) are opened (high voltage no longer present outside the TSAC)
  - [CV ONLY] the fuel supply to the engine and ignition is cut
- EBS is triggered which leads the vehicle to either come to a safe stop and/or prevent it from moving (again).

By this it is ensured that it is safe to approach the vehicle again, i.e. to retire the vehicle, and therefore the Autonomous System Status Indicator (ASSI) might indicate a safe state, see chapter 9.

4 System Critical Signals

Signal monitoring is an essential part of every well-engineered system. It is required to achieve functional safety goals and prevents uncontrolled behavior of the autonomous system.

Concerning the functional safety goals, the system must transition to the safe state as soon as it can not ensure a fully redundant emergency brake maneuver. In case of a signal failure, it might be not possible to properly diagnose the system. Therefore the safe state has to be entered if the diagnosis is not possible anymore. This could be either a broken wire, faulty sensor with out-of-range data, or a signal distorted by electromagnetic inferences.

If it comes to the high-level parts of the AS that rely on a variety of different sensor inputs, the system should detect if any of these is malfunctioning. If the proper vehicle operation cannot be ensured (e.g. loss of environmental perception) the system should react by triggering an emergency brake maneuver immediately. This significantly decreases the time between failure and brake maneuver compared to a brake maneuver which is manually triggered through the RES. This may protect the vehicle from crashing. Even if this topic will not completely be tested during tech inspection, it should be in your 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 as a whole shall be implemented as described above.
The respective rules also apply to optical failure indicators. In order to check for the proper function of these indicators every failure indicator must light up for 1 s to 3 s after startup to check proper function, see T11.9.5.

5 Autonomous System Master Switch

The Autonomous System Master Switch (ASMS), see T14.7, is an additional master switch, see T11.2, as its name already states. It is a hardwired (non-programmable) solution intended to ensure that all actuators of the AS can be safely deactivated.
In order to achieve this, the supply of the actuators has to be directly controlled by the ASMS. This is either achieved by directly routing the supply through the ASMS (like it is done for the Low Voltage Master Switch (LVMS)) or by using a non-programmable logic, such as a relay. In that case, all used components must be sized to the corresponding maximum operating conditions (including max. current and temperature).
Thus, the ASMS is an additional safety feature which ensures that no actuation of the steering or braking system can happen during manual driving (for details see chapter 16), or while work is carried out at the vehicle (such as (dis-) mounting of wheels, downloading a new software to the control units or performing calibration activities), or in the case of erratic software behavior.

6 Steering system

As the steering system is controlled by the AS some safety precautions are to be implemented in order to avoid unintended actuation:
Firstly the supply of the (power stages of the) steering system needs to be directly controlled by the ASMS, for details see chapter 5. This will especially protect a manual driver from experiencing an unintended steering actuation by the AS.
Additionally the AS shall be programmed to not perform any actuation of the steering system that would lead to a movement of the steering rod/linkage while the vehicle is not R2D, see T14.8.1, so that it is still safe to be around the vehicle while the ASMS is switched to the "On" position already. Nevertheless once the vehicle is in R2D the AS is allowed to actuate the steering system in any manner even though the vehicle might still be in standstill. Keep in mind that the torque required to move the steering rod/linkage will be quite high in that case. Thus, it is strongly recommended to not use steering actuators which need to perform calibration movements (e.g. in order to determine a reference angle for straight driving) at startup. One exception regarding steering only being allowed during R2D state applies during an emergency brake maneuver (EBS is activated), where the vehicle loses the R2D state due to the opened SDC. Here it is allowed to perform steering actuation until the vehicle reaches standstill, see T14.8.2, to maintain a stable driving condition.

In addition to the precautions mentioned above, the steering system also needs to be designed in a way that the manual actuation of the steering system is possible at the steering wheel whenever the ASMS is switched to the "Off" position. This is especially required during manual driving (for details see chapter 16) and in case the vehicle breaks down during the dynamic events and quickly needs to be removed from the track by the track marshals. Especially in the second case only the ASMS will be switched to the "Off" position prior to moving the vehicle as a standardized procedure (that is quick and easy to understand) which is required in order to not delay the dynamic events much further. If there is any doubt regarding the steering forces during the tech inspection, a random person may be asked to try moving around your vehicle (with connected steering actuator). This includes persons which are not regularly visiting the gym. Please consider this aspect when designing your system.

7 Actuator Decoupling

Since the 2022 rules it is also allowed to disconnect the actuators of the AS. This mainly targets the steering actuator, to enable lower steering forces for manual driving. But it must always be ensured that this decoupling adds no additional danger to a manual driver. Thus, the steering wheel must always stay connected and it must be avoided that the mechanism moves while driving. This is ensured by T14.9. You should also consider to implement the mechanism in a way that avoids an unintended actuation by the driver. This is not required by the rules, but will cause a problem during the tech inspection, if there are doubts regarding the driver's safety. Additionally you should think of implementing an easy to check indicator which gives feedback of the current position (either mechanical or electrical). This can protect you from a lot of trouble as you can check the position right on the starting line before activating the AS.
Hint: On the brake system, the best solution is, to have no need for decoupling. On the steering system, an electromagnetic clutch supplied by the ASMS might be a simple and robust option.

8 Autonomous System Statuses

In order to create a common and efficient wording within the rules and during discussions related to the AS a set of Autonomous System statuses has been defined in T14.10. These target to represent a certain internal status of the AS based on the status of its relevant subsystems, e.g. ASB (including EBS), TS or R2D state. In conjunction with the ASSI the states are a part of the overall safety concept.
Before the 2022 rules the statuses have been described as AS states represented by a

state machine, which caused a lot of confusion. With the new definition, the function remains equal to the previous rules. But the implementation is now more flexible and should be easier to understand, as it is not linked to a state machine.

Definition:
The definition and determination of the current AS Status is described within a flowchart that can be found in Figure 16 of the rules. Along with this definition one can think of the AS statuses as described in the following:

"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 and the TS shall be checked to be in "Off" position or turned off ([EV ONLY] TSAL lights up green/[CV ONLY] Engine is not running) respectively. 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 16.

"AS Ready": This status usually follows after "AS Off", if the ASB is checked to be fine, 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 vehicle is only allowed for the ASR and officials. The time the vehicle remains in "AS Ready" should be kept to the possible minimum required due to the event procedure.

"AS Driving": The vehicle has been launched via the Go signal of the RES control (considering the safety delay of 5 s, 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 to approach the vehicle (this includes also the ASR and the officials).

"AS Finished": The vehicle considers its mission to be completed, reached standstill and changes its status to this one on its own behalf.
The event is only considered to be completed if the vehicle comes to a stop and enters this state in the finish area. Only the officials and the ASR are allowed to approach the vehicle to retrieve it from the dynamic area.

"AS Emergency": An emergency brake maneuver has been triggered. This can be either caused by an opened SDC e.g. by pressing the shutdown button on the RES control or if the vehicle has detected an internal failure. After coming to a full stop, the vehicle has to be recovered by the ASR and the officials.

"Manual Driving": The vehicle is operated in manual mode. This is only possible if all actuators are turned off via the ASMS and the ASB system is checked and confirmed to be non-energized by the AS.

Implementation:
the definition of the AS statuses does not require any information about the previous status the AS has shown. Therefore the implementation for determining the AS status can be done by transforming the flowchart given in the rules, see above, into a simple set of nested if-else statements that is called with its required inputs during every software execution cycle. The computed result will then be passed to the ASSI, see chapter 9 and the datalogger, see chapter 1.

Safety delay (5 s):
The safety delay required by T14.10.3 intends to provide a time frame for the ASR and the officials to leave the area nearby the vehicle as soon at it reaches the status "AS Ready". During this time frame the vehicle would not change its status to "AS Driving" even in the case Go signal has been sent by accident.

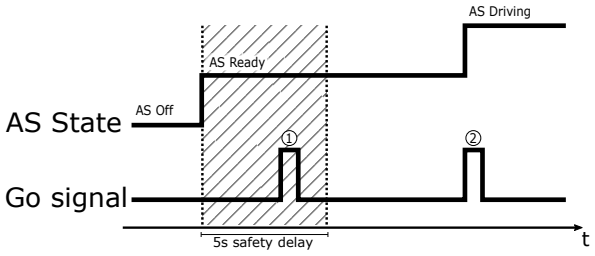

Figure 2: Example timing sequence for the safety delay

An example timing sequence that visualizes how the safety delay shall work is shown in Figure 2: The delay starts as soon as the AS reaches "AS Ready" and lasts for 5 s. During this time period the AS must not accept

but reject any Go signal from the RES control, see ①. To trigger the AS to start the selected mission (Status "AS Driving") an new Go signal needs to be sent to the vehicle after the time period of the safety delay has elapsed, see ②.

9 Autonomous System Status Indicator

The Autonomous System Status Indicator (ASSI) reflects the current status of the vehicle and is used by team members and the marshals for assessing the current behavior of the AS, see chapter 8 and has a similar purpose as the Tractive System Active Light (TSAL). For this it includes three color indicators (usually LED lights) at the vehicles sides and rear end, see T14.11.2. Additionally a sound generator is required to indicate the status "AS Emergency", see T14.11.4. It is one part of the overall safety concept and the ASSI's functionality is considered to be safety critical and will be checked during technical inspection. This includes especially the correct illumination with respect to the AS status, see T14.11.1, the ASSI's visibility and its sound level.

10 Autonomous Mission Indicator

As its name already states, the Autonomous Mission Indicator (AMI)'s purpose is to indicate the currently selected autonomous mission as specified in T14.12. It is used by the ASR and the officials to know which of the autonomous missions the AS will be executing upon releasing the vehicle at the starting line. This aims to avoid incidents where a wrong mission is selected by accident and the vehicle e.g. applies algorithms designed for the Skidpad event on an Autocross track layout. Hence the Autonomous Mission Indicator (AMI) is considered to be a SCS and shall be visibly checked to show the correct autonomous mission prior every dynamic event.

In order to serve its purpose well the AMI needs to be able to convey its indicated mission to any untrained person. Therefore its position in the vehicle is restricted to either

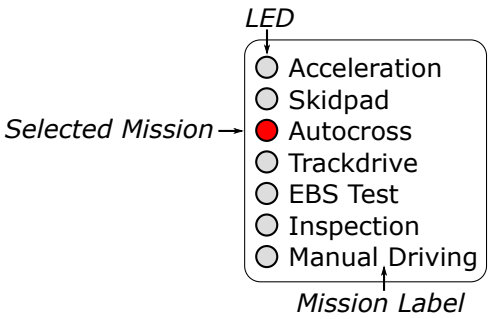

Figure 3: Schematic exmample of a simple AMI

the dashboards or the proximity of the ASMS. In addition it must be easy to read (e.g. also visible in bright sunlight) and to understand (e.g. no complicated sequence of numbers or patterns) for anyone. A quite simple proposal for the design of an AMI is schematically shown in Figure 3. As an alternative a display integrated into the vehicle's dashboard might also be considered to be used as an AMI, given that the SCS requirements can be fulfilled. If persistent displays like E-Ink are used for the AMI please consider a moving element on the screen to show that the display is still up to date.

11 Autonomous System Brake

The term Autonomous System Brake (ASB) covers all parts which are related to autonomous brake actuation. One major part of the ASB is the Emergency Brake System (EBS), which performs emergency brake maneuvers if its power is cut (T15.1.1). In former rules versions there was an EBS and a service brake but this lead to confusion. Thus both where summed up to one ASB with EBS functionality. Now the whole ASB can be used to guarantee the functional safety requirements.

Figure 4 visualizes this hierarchical approach. Requirements like deactivation and failure monitoring are now valid for the whole brake system. One main part inside the ASB is the EBS which additionally needs to fulfill T15.2. The other main part is a second, independent system to ensure the functional safety requirements. This system might be a duplicate of the EBS or something completely dif-

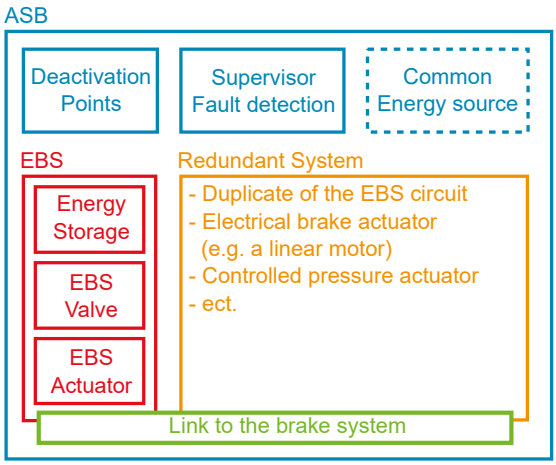

Figure 4: Hierarchical Overview of the ASB

ferent like an electrical linear actuator. This second system does not need to fulfill T15.2 but still needs to be monitored for failures. The following chapter will provide a more detailed look into the implementation of the ASB.

12 ASB reference design

12.1 System Overview

Figure 5 shows a rough overview of a possible ASB implementation. The RES is directly integrated in the SDC (denoted in orange) and the EBS actuator supply (denoted in green) with its relay output, as required by T14.4.4 and T15.2.2. There is also some non-programmable logic integrated into the SDC, to enable the AS to open the Shutdown Circuit. It also latches the SDC by non-programmable logic after reaching the finished state or in case of failure. The non-programmable logic should be placed inside the SDC after the RES, to detect an opened SDC by the RES and latch it (T14.5.1).

The ASB itself consists of the following main parts:

Supervisor: The supervisor monitors the status of the ASB and performs the initial checks for the system. In case of failure the CPU triggers the EBS and/or its redundant system (T15.3.4) and also lights up the EBS failure indicator required by T15.3.3.

SDC Non-programmable logic part: The SDC's non-programmable logic is used to handle the SDC as required by T14.5.1. It also enables the Supervisor to open the SDC in case of failure or in case of CPU stall (Watchdog). It consists of discrete components like logic gates, transistors etc.. It does not include any processors or programmable logic parts.

Mechanical part: The mechanical part of the ASB is defined as the connection between the electrical system and the vehicle's brake system. It stores the energy for emergency brake activation and releases it to the brake system in case of triggered EBS (T15.2.1). It may also contain additional actors to provide dosed braking during operation.
Depending on the system it also must include some sensors for monitoring and the initial check sequence (T15.3.1).

In the following sections, there will be a short description of the above mentioned parts and some more detailed design hints regarding the rules.

12.2 EBS Supply concept

Figure 6 shows the EBS supply concept as required by Rule T15.2.2 (green path). Additionally figure 6 shows how the relay has to be integrated into the SDC (orange path). Important on the SDC implementation is, that the EBS relay must not be delayed when the SDC opens. The system must be designed in a way that ensures the delay mentioned in EV6.1.5 is only applied to the AIRs and not to the EBS relay. Finally the supply concept includes two Powerstages/MOSFETs (blue parts). These additional switches are required to fulfill T15.3 and enable the supervisor to test both actuation paths independently and ensure that the system is working redundantly.

12.3 Supervisor

As previously mentioned, the supervisor:

1. Monitors the system to detect failures.
2. Transitions the system to a safe state in case of a single failure (T15.3.4).
3. Actuates the EBS failure LED (T15.3.3).
4. Provides EBS status signals to the Autonomous System.

For this purpose it needs sensors in the mechanical part of the EBS, to monitor the sta-

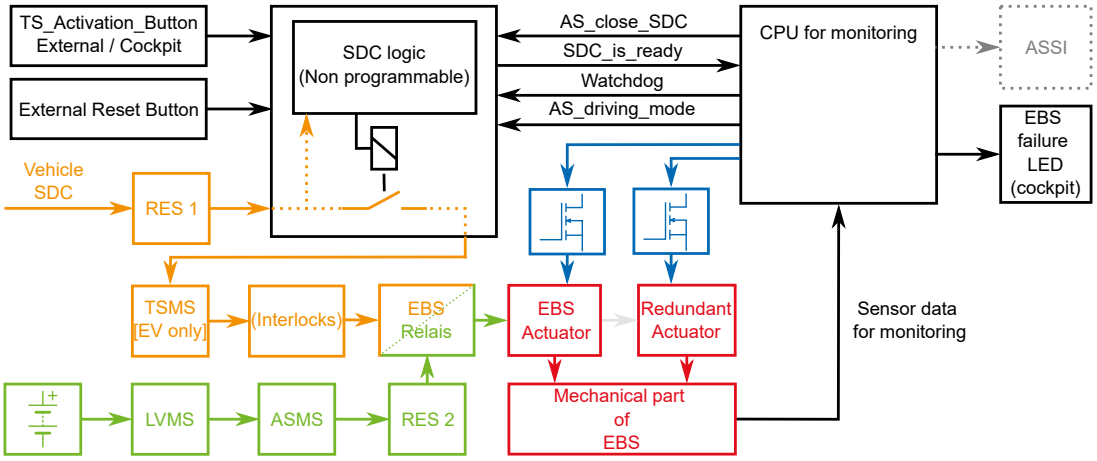

Figure 5: General ASB overview

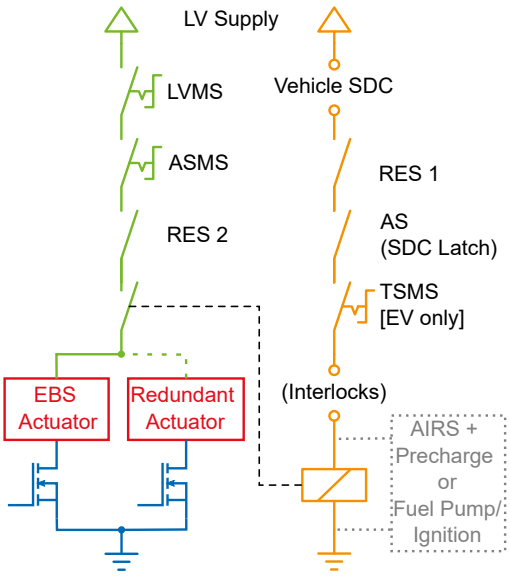

Figure 6: Realization of Rule T15.2.2: EBS supply

tus of the system. Sensor signals could be for example:

- Hydraulic brake line pressure (e.g. for initial checkup)
- Pneumatic tank pressure (e.g. for system continuous monitoring)
- Etc.

The supervisor needs to handle the ASB status and to interface with the non-programmable logic part. The following signals are used by this reference design to interface the non-programmable logic part:

- *"AS_close_SDC"* is used to enable the activation of the TS via the TS activation button, see EV4.11.3, after all system checks are done and the system is ready.
- *"Watchdog"* is mandatory to ensure the supervisor is still alive. This signal must be connected to the CPU and periodically toggled by **software** to maintain a keep alive signal. Otherwise the SDC gets opened. This signal can also be used to open the SDC in case of a detected failure. (e.g. by switching the corresponding CPU output PIN to tristate, or by stop toggling)
- *"AS_driving_mode"* is used to switch the activation buttons between manual and autonomous mode.
- *"SDC_is_ready"* is used to monitor the internal state of the logic and to perform an initial check to ensure that the watchdog is working fine.

Initial Checkup Sequence:

An initial checkup sequence is necessary to determine all kind of failures which could not be detected during operation without applying the brakes. These kinds of failures are especially failures due to wrong assembly e.g. missing connection to the brake pedal. For redundant systems this checkup sequence has to be performed in a way that ensures both systems are working independently. E.g. activate brake through system 1, deactivate brake, activate brake through system 2 and check both for built up brake pressure. The following steps are an short example for an initial EBS checkup routine:

1. Start toggling watchdog.
2. Wait for vehicles SDC to close (*"SDC_is_ready"* is high).
3. Stop toggling watchdog.
4. Check *"SDC_is_ready"* goes low. Else => failure

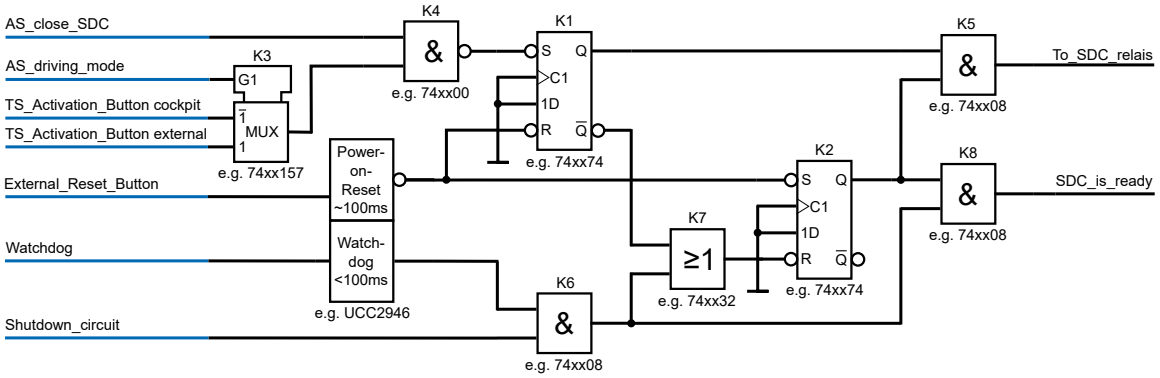

Figure 7: Logic diagram for EBS non-programmable logic part, (blue line = pull-down termination required)

5. Start toggling watchdog again.
6. Check that the EBS energy storage is filled.
7. Check that the brake pressure is build up correctly.
8. Enable TS activation through *"AS_close_SDC"*.
9. Wait for TS being activated.
10. Disable EBS actuator 1 (blue MOSFET figure 6).
11. Check that the brake pressure is still build up correctly.
12. Enable EBS actuator 1 again.
13. Disable EBS actuator 2 (blue MOSFET figure 6).
14. Check that the brake pressure is still build up correctly.
15. Enable EBS actuator 2 again.
16. Transition to ready state

Continuous Monitoring:
Continuous monitoring is required during operation to detect typical failures like cable or pneumatic line ruptures. The typical values for monitoring are the energy storage of the mechanical part and the state of RES. In case of triggered EBS the function of the EBS must be checked as well. If sufficient brake line pressure is not built up, the redundant system must be activated (if the systems are not triggered together, as the example in figure 6).
Example values for continuous monitoring are:

- Monitor the storage of brake energy. e.g. pneumatic tank pressure
- Brake line pressure
- Mechanical state of valves
- Plausibility of sensor signals
- Brake transfer function
- State of the RES via CAN
- etc.

12.4 Non-programmable Logic

Preface: The implementation of the logic here is just an example. It might be implemented in another way as well.

Figure 7 shows a possible implementation of the non-programmable part of the EBS. It is built out of standard 74xx logic gates, which are mentioned in the schematic. This schematic does not include any input/output protection and termination (pull-up/down) circuitry. In addition to the logical gates, see colors in figure 7.

The non-programmable logic part consists of two Flip-Flops which are latching the corresponding states until the next power cycle or reset:
K1: Latches the enabled state of the SDC

K2: Latches the disabled state of the SDC
The initial states of these Flip-Flops are ensured by a power-on-reset chip, which also includes the watchdog functionality. The logical connection is done by standard AND/OR gates.

Additionally, the logic contains a multiplexer (K3), which is used to switch between both activation buttons, depending on the selected driving mode. This is done in hardware here, to ensure that the rule EV4.11.5 is met and the AS cannot activate the SDC by a software fault.

A detailed signal description can be found in the supervisor section above (section 12.3).

Watchdog: The reason for an external watchdog in this design is that at first this HW watchdog cannot be disabled by a programming fault. It gives a second deactivation path additional to the CPU if one whole chip fails. This external watchdog will always be requested during the ASF review, unless you have another solution to handle CPU HW faults.

Alternative Implementation: If your vehicle is already equipped with an SDC latching circuit, you may also use this circuit and incorporate the additional activation button in software. It is also possible to use another ECU inside the vehicle which can communicate with the supervisor, and is also capable of opening the SDC, as watchdog.

12.5 Mechanical Part

The mechanical part must be designed in such a way that the stored brake energy for the EBS is released without the aid of electrical power (T15.2.1), in order to ensure the performance of the EBS in case of a power failure. The energy storage can be realized by e.g. springs, pneumatic pressure or hydraulics.

A good way to activate the EBS is releasing a counter pressure which works against the stored brake energy. For normal operation/brake release, this energy storage must be detachable e.g. by a mechanical disconnect, or deactivatable by pressure release (T14.7.5 / T15.1.6). As this storage is a critical part of the EBS, its status must be monitored continuously while driving.

12.6 Redundancy

Fully-redundant ASB:
A fully redundant EBS means that there are two independent systems fulfilling the EBS requirements in parallel. Thus, the system is still able to come to a safe state, even if a single failure occurs (T15.3.4). On the electrical side redundancy can be ensured by a second output stage which enables the monitoring CPU to trigger the EBS even if the SDC is failing. In case of failure of the monitoring CPU the EBS is triggered automatically by the watchdog.

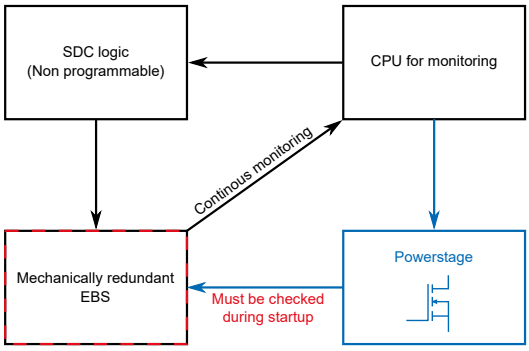

Figure 8: Schematic overview for a fully redundant EBS

On the mechanical side redundancy depends on the chosen system. The following example distinguishes between two scenarios:

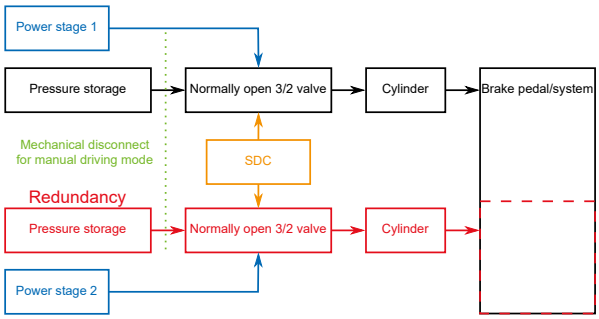

Figure 9: Actively applied braking energy

1. Actively applied braking energy:
Figure 9 shows an ASB with actively applied braking energy. In terms of a pneumatic system, the braking energy is stored in a pressure tank and is released to the brake system via a normally open valve and a cylinder. The brakes are only released if electrical power is applied to the valve. To get into manual driving mode either the pressure has to be removed, or the tank must be mechanically disconnected.

To avoid common cause failures the redundant system consists of two independent but identical systems. The only common part is the connection to the vehicles brake system (brake pedal). This connection must be designed in a way that ensures a sufficient safety factor in all possible cases.

2. Removal of counterforce:
Figure 10 shows an ASB with permanently applied brakes, e.g. by redundant springs. The application of energy is needed to release the brakes. This could be done

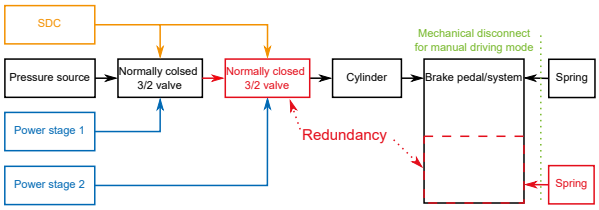

Figure 10: Removal of counterforce, which keeps the brakes opened

by pneumatic or hydraulic pressure. For this system no explicit pressure storage is needed as a loss of pressure results in a safe state. Only the springs and the pressure release valves must be designed redundant. The mechanical connection between the springs and the brake system must be designed in a way that ensures a sufficient safety factor in all possible cases.

To get into manual driving mode the springs must be mechanically detachable or, in case of gas-springs, the pressure must be releasable (keep T14.9 in mind). The state of the springs might be monitored through the brake pressure built up when brakes are engaged. For gas-springs with releasable pressure, the pressure itself must be monitored.

Non EBS actuator as Redundancy:
If the vehicle is equipped with other actuators for dosed braking that do not fulfill the EBS requirements, it is possible to use them as redundancy for the EBS too. As these actuators are part of the ASB, they must be monitored for all failures as well and trigger the EBS in case of malfunction. A sufficient way for continuous monitoring is a transfer function check (brake pressure vs. actuation force), if the actuator is regularly used during operation.

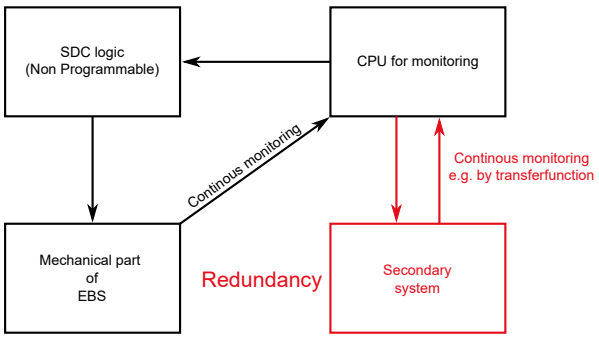

Figure 11: Schematic overview with secondary system as redundancy

12.7 Testability / Technical Inspection

This section should give you some hints how to speed up the technical inspection as there will be limited time for each inspection slot. If it takes too long to sufficiently test the system you'll need to requeue.

SCS:
As all signals of the ASB are considered to be SCS, it must be possible to bypass these signals during technical inspection and manipulate them. This could either be done by using a single connector for each signal or by providing a breakout box for technical inspection if using a multi pin connector.

Accessibility:
All parts of the ASB should be easily accessible without excessively disassembling the vehicle. Especially all mechanical ASB relevant parts and all hydraulic/pneumatic parts beside the vehicles brake system.
All parts must be properly attached to the vehicle. **EBS triggering:**
During the inspection your EBS will be triggered multiple times. To get this tests done as fast as possible, your system should be able to perform multiple EBS tests in a row or you should be able to quickly refill your system.
If for every test a LVMS power cycle is needed (T14.5.1) it might also be helpful to make use of the external reset button, to avoid excessive time loss due to long booting times until the system is ready again. (Since the 2020 rules it is also permitted to have a manual reset button in proximity to the ASMS.)

12.8 Examples

Caution: The renderings in this section have been drawn by an electrical engineer. They are just for visualization purposes and not meant to be a 1:1 blue print for your own constructions.

This section shall give a rough overview on how the implementation of the ASB may look like. Its focus is on the mechanical part as the electrical requirements have already been handled on the past sections.

Pneumatic system:
Figure 12 shows an example implementation of the pneumatic part of the ASB. It consists of the common energy source (denoted in or-

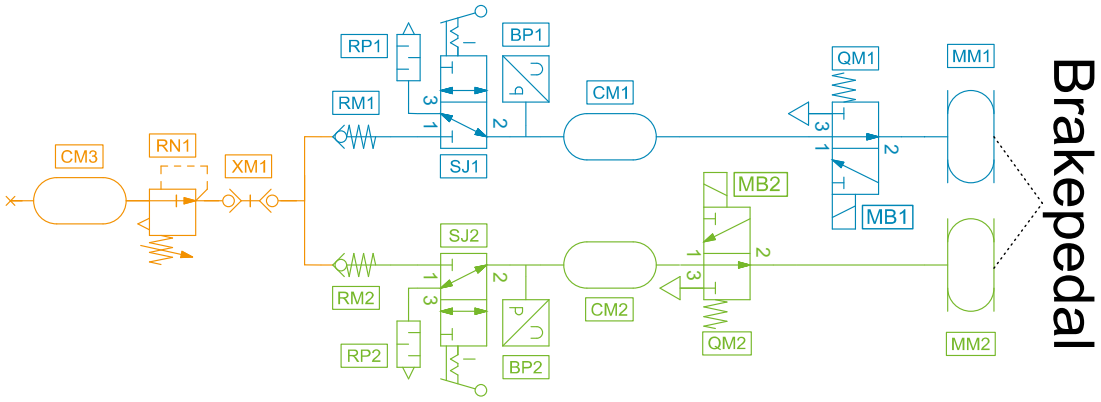

Figure 12: Pneumatic diagram example

ange), the EBS (denoted in blue) and its redundancy (denoted in green). The systems actuates the brake pedal through two fluidic muscles (MM1, MM2). The redundancy is ensured by the two independent pressure tanks CM1 and CM2, which are decoupled by the check valves RM1 and RM2. Each pressure tank must at least contain enough energy to perform an emergency brake maneuver. Using only one tank is not sufficient as a failure to a single tank may also decrease the pressure on the source which may not provide enough energy for the brake maneuver. As both paths have one energy storage, both need a deactivation mechanism. In this case the deactivation is done by a manual valve (SJ1, SJ2) which disconnects the pressure source and vents the tank. Both tanks are equipped with pressure sensors (BP1, BP2) to ensure that sufficient pressure is present to perform the emergency brake maneuvers. If one pressure drops below its limit, the SDC needs to be opened to activate the EBS. This activation will happen by QM1, which fulfills the EBS supply requirements. QM2 may be actuated in parallel to QM1 or may also be actuated separately as it does not need to fulfill the EBS requirements. It could also be a pressure control valve for dosed braking.
For supplying the whole circuit, there are various different options. One common option is, to use high pressure paintball bottles.

Another option is, to fill the pressure tanks by a small compressor inside the vehicle. But here you need to make sure, that the compressor is supplied by the ASMS and that it does not need too much time to fill the tanks, as you only got 1 min.
For the implementation inside the vehicle, it is important to always make sure, that the pneumatic system fulfills T9.

Certification:
In the rules it is required that especially the high pressure equipment and the tanks are certified and labeled accordingly. Therefore you should make sure that the pressure tanks fulfill the legal requirements, are rated properly and are not expired. This will be checked during the competition and may cause you a lot of trouble. Keep also in mind, that it is not allowed to transport filled paintball bottles on public ground in Germany, if they are not "PI" certified.

Connection to the brake system:
On the mechanical interconnection between the pneumatic part and the vehicle's brake system, multiple solutions are possible. This guide shows three possibilities:

a.) Via the brake pedal (Figure 13)
b.) Via a second master cylinder (Figure 14)
c.) Via a direct pressure transducer (Figure 15)

The most obvious and simplest solution is, to connect the ASB actuators directly to the existing brake pedal as shown in (figure 13). The only things which have to be kept im mind are: The mechanical design must be sufficiently strong to guarantee that no failure will arise from it. It must be impossible by design, that the actuators block each other or manual braking operation. Thus, mechanisms as the shown anti-blocking slots are highly recommended.

Another option is to decouple the ASB actuators from the brake pedal, see figure 14. This is quite helpful if there is not much space behind the pedal. In its easiest version the

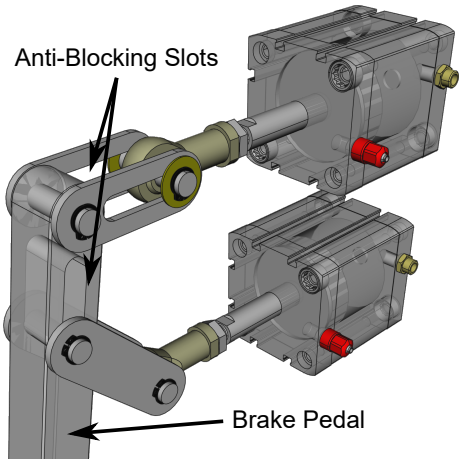

Figure 13: Two ASB actuators directly connected to the brake pedal

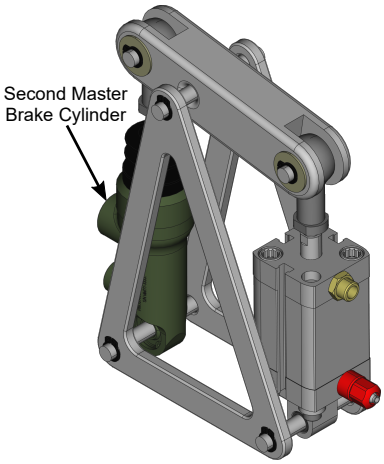

Figure 14: Brake actuation through an additional master cylinder

actuation consists of a pneumatic cylinder which acts on an additional master cylinder. To handle the redundancy and both brake circuits, two master cylinders need to be used. This also allows to actuate both brake circuits with different pressures for optimized braking balance. Special care must be taken on the integration into the brake system. This can usually be done by an Shuttle(Or)-Valve or by connecting the cylinder in series to the existing master cylinder. In any case it must be ensured, that the manual braking operation is always possible.

Taking the previous solution one step further, there is also the possibility to combine the pneumatic and the hydraulic cylinder into a single transducer. As this usually requires a completely self built part, this option should

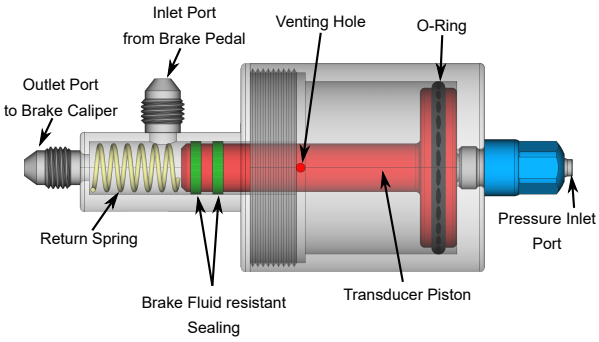

Figure 15: Brake actuation through a pressure transducer

only be taken if you exactly know what you are doing. The potential of getting failures is quite high. Special care must also be taken when choosing the materials, as they need to be brake fluid resistant. Thus, especially the material of the sealing must be stated in the ASF.

13 Sensors & Components

For sensors and components placement, see rules figures 2 and 15, both combined define the allowed positions for all electrical components. It specifies a maximum design area to prevent exaggerated designs as on the aerodynamic devices. Exceptions are granted for antennas, to allow reasonable technical positioning. To enable safe operation in manual mode, none of the electrical components is allowed to come into contact with the drivers helmet, to avoid protrusions in case of a crash. This will be checked with the tallest driver in case of doubt by the technical inspectors. Please also keep the first rule of T2.1 in mind. Even if you are fulfilling the placement rule, you may need to change your design at technical inspection if it exhibits the driver to a potential danger.

14 Autonomous System Form

The ASF is a comprehensive documentation of the AS which has to be uploaded prior to the competition.
Its main purpose is to detect failures which are hard to correct before the competition starts. Thus, the ASF will be focused on the

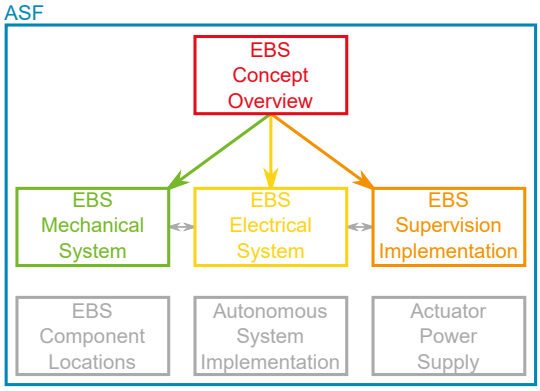

Figure 16: Overview of the ASF

implementation of the ASB, as its implementation is the most complex one and prone to failures. All the other parts of the AS will not be handled by the ASF after 2021. It is now in your responsibility to ensure that e.g. the AS statuses are handled correctly (T14.10) and that all components fulfill the legal requirements(T11.11).
To ensure that all the other parts, which not have been reviewed, are working as intended, it is always a good option to check all the points of tech inspection in advance (Last years Inspection Sheet).
Another purpose of the ASF is to identify test cases for the ASB in advance and to have a proper documentation to ease up the inspection. To generate this documentation, the ASF consists of multiple documents which need to be prepared and must have a certain format. To provide a common understanding of the documents and unify the documentation, some rules have to be followed. These rules and some examples can be derived from the example documents of the ASF. These can be found throughout the year, with many additional information on the ASF at the hands on ASF page.

15 Technical Inspection

The Technical Inspection intends to check the rules compliance of the vehicle. Most of the rules aim at making the competition, but also the whole season, safe and efficient for the team and staff members. Furthermore, the rules ensure that certain features of the vehicle are equivalent to achieve a fair and exciting competition. During the Technical Inspection, most of the safety relevant features will be checked, but bear in mind that passing Technical Inspection is not a proof of rules compliance! Additionally there may also be further checks during and after the dynamic events where rules compliance is checked. If the vehicle violates any of the rules it may receive a Disqualified (DQ) or penalties.

The DV related parts of the Technical Inspection are spread between the mechanical and electrical inspection. The former takes care of sensor positions, ASB design and mountings. The latter checks electrical aspects of the DV system, such as sensor diagnosis, as well as the driverless inspection mission. The inspection mission is used to simulate a fully operational DV vehicle in the Technical Inspection area, while using a minimum set of required inputs such as sensor signals. It should not depend on the availability of all perception sensors or valid GPS signals. This mission allows to check topics like a correct ASSI functionality and safety features. The main focus here is the ASB. Especially the handling of functional safety is checked to avoid critical failures which make the whole ASB unable to work. During this test, several sensors and actuators will be disconnected to see the systems response.
Details upon the procedure can be taken from the inspection sheets which can be downloaded from the FSG website prior to the competition. Throughout the season you might refer to last years inspection sheet as a preliminary source of information.

The final part of the Technical Inspection concerning DV is the EBS brake test. It checks that the vehicle delivers the required brake performance under dynamic conditions. The details of the test are described in IN11.2.

16 Manual driving

The manual driving mode of a DV vehicle intends to avoid injuries caused by movement of any part of the actuators based on the commands from the AS. By selecting the manual mission, the system is aware that a driver is seated in the vehicle and can conduct the appropriate checks. The rules enforce software checks to prevent human error during operation and increase overall

safety under all circumstances. The following conditions need to be fulfilled:

- All actuators are unavailable. It is considered equivalent to check that ASMS is switched off. This could be done easily by measuring the supply voltage on the actuator side of the ASMS. The ASB/EBS energy storages are empty. A startup check of the EBS must validate via its sensor signals that the system is de-energized or fail otherwise, since the manual mission is selected.
- Manual actuation of the steering wheel shall be possible.
- All in all, the vehicle should behave comparable to a standard Electric Vehicle (EV)/Internal Combustion Engine Vehicle (CV), with an additional supervision through the AS. All non-acting parts of the AS are allowed to be active, especially the processing units and sensors.

17 Startup procedure

To run the dynamic events as efficient as possible, a common startup procedure has been defined (D 2.5) which also limits the time to get to "AS Ready". Thus, you as a team should aim at minimizing 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 ASMS and LVMS in "Off" position and ASB detached/decoupled (e.g. by shut-off valves).
3. Turn on the LVMS and check/setup your AS once you are in the preparation area.
4. Queue and wait to approach the staring line. The LVMS may remain in "On" position.
5. Once your vehicle is properly aligned at the starting line, attach/arm your ASB/EBS e.g. by closing the shut-off valves.
6. Double check that your steering actuator is connected to the steering system.
7. Select the correct mission and check on the AMI, if the selection of the mission has succeeded within the AS.
8. Turn on the ASMS and activate the TS on advice of the official. (Hint: Shutdown buttons and RES shall be checked in advance.)
9. Leave the area nearby the vehicle. And proceed to the area designated for the ASRs carrying the RES control.
10. Wait for your vehicle to reach "AS Ready" and give the "Go" signal via the RES control after the approval of the official.