Autonomous System Beginners Guide 2023/2024

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

2023-10-18

Contents

Changelog

Section	Version	Change
	1.0	Updated references and links to FS-Rules 2024 v1.0
1.1	1.0	Added further hint that re-runs are only granted for autonomous runs and that an EBS bypass is recommended
6	1.0	Added reference to new rule concerning ASSI visibility
9.7	1.0	Added additional hint concerning rollover protection envelope
14	1.0	Provide additional and updated details on startup procedure

Abstract

This document is intended to give you – as a team – a reference for implementing the Autonomous System (AS) and Autonomous System Brake (ASB) rules. Following this guideline eases the design of your vehicle and helps to review the safety of your design faster. Following this guide does not solely ensure that your design will pass the Autonomous System Form (ASF) review or technical inspection. This guide only provides 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 2024 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 the system to be redundant. In addition, the testability during technical inspection is discussed. As the ASB signals are part of the Autonomous System, they are considered to be System Critical Signals (SCSs), see T14.5.1 and therefore require some additional measures to be taken that are also discussed in this document.

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

1 Remote Emergency System

The Remote Emergency System (RES) is considered the most basic safety feature of the Driverless vehicle. It consists of a remote device that is connected to an on-board receiver unit, which is directly hard-wired into the shutdown circuit, see T14.3.4. Once the shutdown button on the Remote Emergency System (RES) is pressed or a signal loss occurs, the Tractive System (TS) is disabled and the Emergency Brake System (EBS) 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 forwards this signal to 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 5.

1.1 RES-Bypass (T14.3.5)

As re-runs due to a signal loss of the RES can only be granted for autonomous runs, see D2.7.6, and to avoid any other problems during manual driving because the RES is always required to close the Shutdown Circuit (SDC), it is permitted and highly recommended to deactivate the RES in this case. 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. Due to the safety criticality, only safety certified relays with forcibly guided or a mirrored contacts are permitted. This certification ensures that both contacts are never closed at the same time. Solutions relying on software are not allowed.

1.2 Antenna mount

As one of its safety features the RES will also open the SDC, if the signal strength that is received at the receiver unit drops below a certain threshold. Thus, it is strongly recommended to place the RES-antenna away from metal parts and 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 in between the RES remote device and the vehicle may differ from the ones that are present at the test area.

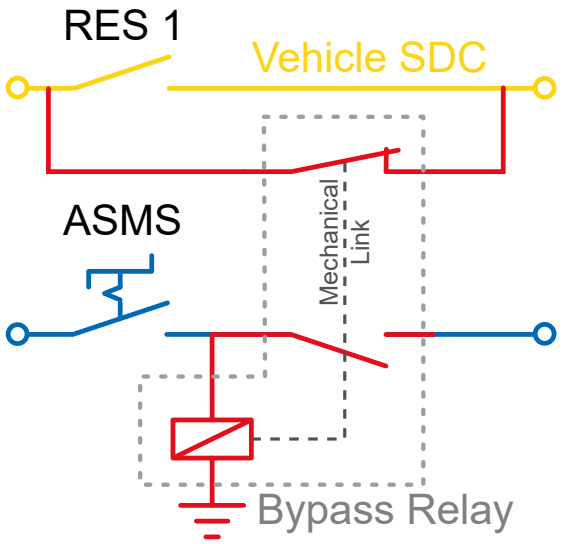

Figure 1: RES bypass circuit

2 Shutdown Circuit

The SDC is the main control line for the TS within the vehicle. For a schematic overview see the figures 21 (CV) and 22 (EV) in the rules. 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 T14.4.1:

Manual Mode: The AS has checked that the Autonomous System Master Switch (ASMS) is switched "Off" and the ASB 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 inside 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 it needs to be ensured that 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
  - [CV ONLY] the fuel supply to the engine and ignition is cut
- EBS is activated 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 6.

3 Autonomous System Master Switch

The Autonomous System Master Switch (ASMS), see T14.6, is an additional master switch, see T11.2, that is a hardwired (non-programmable) solution intended to ensure that all actuators of the AS can be safely deactivated.
Therefore 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 this case, all used components must be rated to the corresponding maximum operating conditions (including current and temperature).
The ASMS shall be kept in the "Off" position whenever possible so that no actuation of the steering or braking system can happen during manual driving (for details see chapter 13), 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.

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 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.

5 Autonomous System Status

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 T14.9. 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 statuses are a part of the overall safety concept.

Definition:
The definition and determination of the current AS Status is described within a flowchart that can be found in Figure 17 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 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 vehicle is only allowed for the ASR and the 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 sent by the RES (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 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 Unsafe 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 T14.9.1. 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 AS has checked that the ASB cannot interact with the brake system.

Implementation:
The definition of the AS statuses does not require any information on 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 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 6 and the data logger, see chapter 15.

Safety delay (5 s):
The safety delay required by T14.9.3 intends to provide a time frame for the ASR and the officials to leave the area nearby the vehicle as soon as it reaches the status "AS Ready". During this time frame the vehicle shall not change its status to "AS Driving" even in case the go signal has been sent by accident.

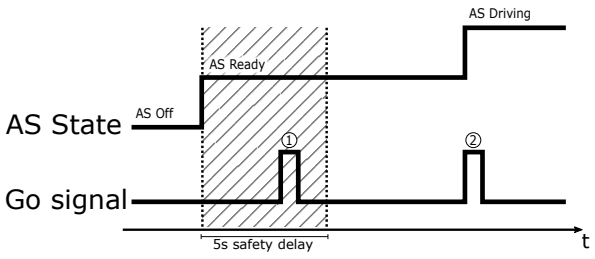

Figure 2: Example timing sequence for the safety delay

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, see ①. To start the selected mission (Status "AS Driv-

ing") a (new) go signal needs to be sent to the vehicle after the time period of the safety delay has elapsed, see ②.

6 Autonomous System Status Indicator

The Autonomous System Status Indicator (ASSI) reflects the current status of the AS and is used by team members and the officials for assessing the current behavior of the vehicle, see chapter 5. It includes three color indicators (usually LED lights) at the vehicle's sides and rear end, see T14.10.2. Additionally a sound generator is required to indicate the status "AS Emergency", see T14.10.5. The ASSI is part of the overall safety concept and will be checked during technical inspection. This includes the correct illumination with respect to the AS status, see T14.10.1, the visibility, see T14.10.3, and the sound level.

7 Autonomous Mission Indicator

As its name already states, the purpose of the Autonomous Mission Indicator (AMI) is to indicate the currently selected autonomous mission as specified in T14.11. It is used by the ASR and the officials to be aware of the autonomous mission which 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 to 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 the dashboard 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.

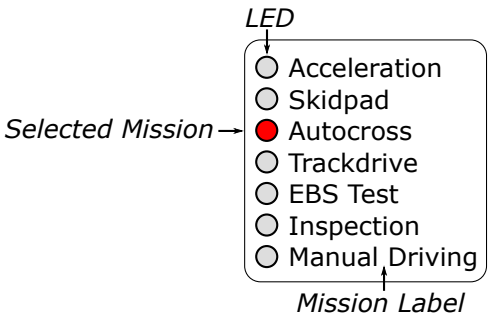

Figure 3: Schematic example of a simple AMI

8 Autonomous System Brake

The term Autonomous System Brake (ASB) covers all aspects that 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).

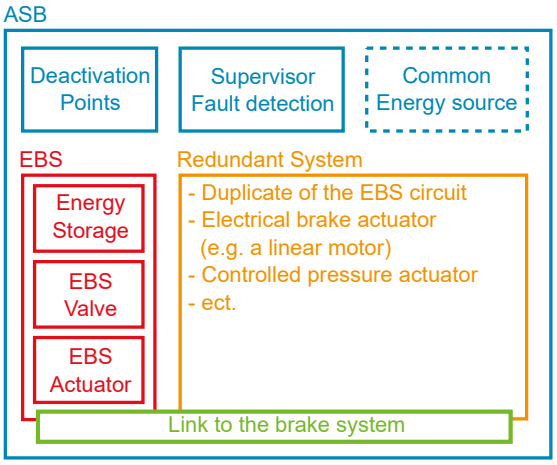

Figure 4: Hierarchical Overview of the ASB

Figure 4 visualizes the structure of the ASB. Requirements like deactivation and failure monitoring are valid for the whole brake system. A major element within the ASB is the

EBS which additionally needs to fulfill T15.2. The other major element is a second, independent system to ensure the functional safety requirements. This system might be a duplicate of the EBS or something completely different 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.

9 Autonomous System Brake reference design

9.1 System Overview

Figure 5 shows a rough overview of a possible ASB implementation. The RES is directly integrated in the SDC (depicted in orange) and the EBS actuator supply (depicted in green) with its relay output, as required by T14.3.4 and T15.2.2.

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 activates the EBS and/or its redundant system (T15.3.3).

SDC logic part: The SDC's logic was previously used to latch the SDC open, but since the 2023 rules, this is not required for the AS anymore. In this example it contains only a HW-Watchdog which is used to open the SDC in case of CPU stalls.

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 an activated EBS (T15.2.1). It may also contain additional actuators 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 the above mentioned parts and some more detailed design aspects regarding the rules will be described.

9.2 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 for 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 that 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.

9.3 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 (T15.3.3).
3. Provides EBS status signals to the Autonomous System.

For this purpose it needs sensors in the mechanical part of the EBS to monitor the status 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.

Supervising the supervisor:
The supervisor is monitoring the system for failures to fulfill T15.3.3. As it is a critical part it becomes also a single point of failure and thus needs monitoring. Common approaches for the supervisor supervision are:

- *External Watchdog (recommended):* A good solution is the use of an external watchdog as in the example. It cannot be deactivated by SW and can easily be checked at startup for proper function.
- *Internal Watchdog:* Using the internal watchdog is not recommended and only

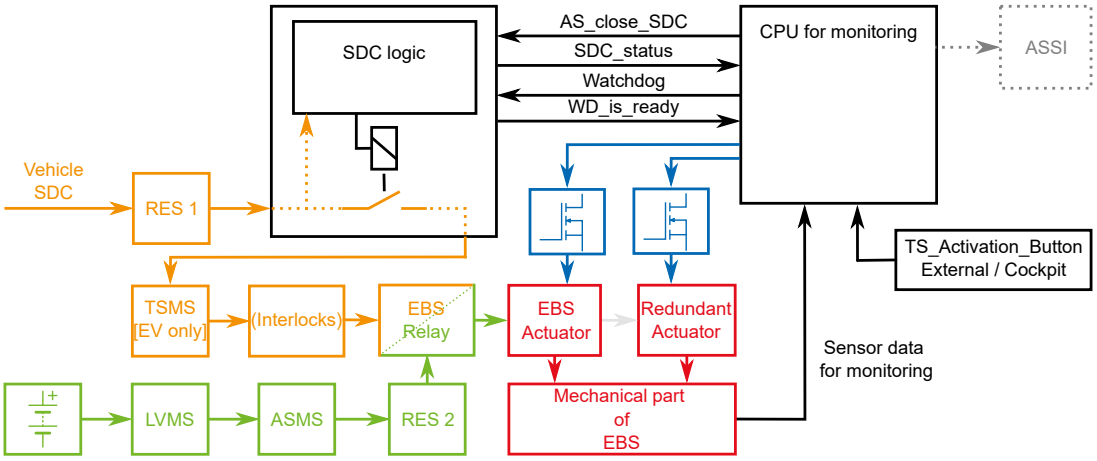

Figure 5: General ASB overview

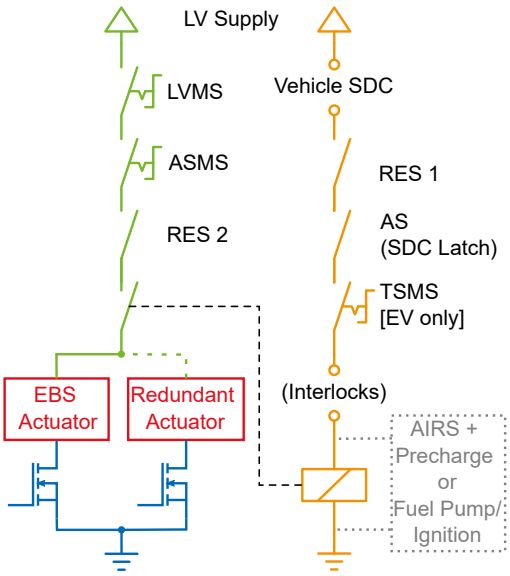

Figure 6: Realization of Rule T15.2.2: EBS supply

possible if a watchdog event will lead to an open SDC. Furthermore, it needs to be ensured in the SW design that it is not deactivated accidentally.

- *Second CPU:* A second CPU in the vehicle can be used, if it can communicate with the supervisor and if it is able to open the SDC independently of the supervisor. In this case a heartbeat is sent between both CPUs. If one fails the other one needs to open the SDC.

Example Signals:

In this reference design the supervisor needs to handle the interface with the SDC logic part. The following signals are used:

- *"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)
- *"WD_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.
- *"SDC_status"* is used to monitor the status of the SDC.

Initial Checkup Sequence:

An initial checkup sequence is necessary (T15.3.2) to determine all kind of failures which could not be detected during operation without applying the brakes. These kind of failures specifically include 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 a initial EBS checkup routine:

1. Start toggling watchdog.

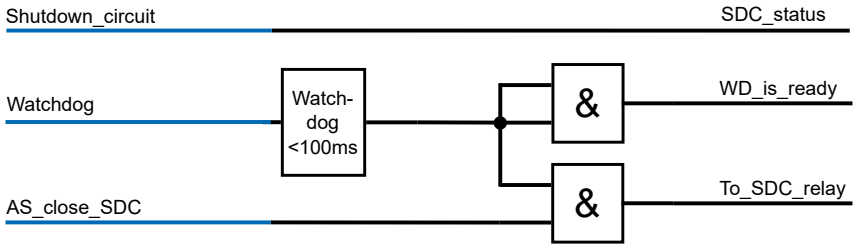

Figure 7: SDC logic diagram

2. Wait for watchdog to respond (*"WD_is_ready"* is high).
3. Stop toggling watchdog.
4. Check *"WD_is_ready"* goes low. Else => failure
5. Start toggling watchdog again.
6. Check that the EBS energy storage is filled.
7. Check that the brake pressure is built 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 built 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 built up correctly.
15. Enable EBS actuator 2 again.
16. Transition to ready state

Continuous Monitoring:
Continuous monitoring is required during operation (T15.3.2) 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 an activated 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 activated 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.

9.4 SDC Logic

Preface: The implementation of the logic here is just an example.

As the Non-programmable Logic was removed in the 2023 rules, there is no logic in the AS required by the rules. The former latching function is also covered in the TS activation rules (EV4.11.4). Nevertheless this reference design still contains some logic around an external watchdog, shown in Figure 7. But as this circuit is trivial, there is only one thing to be mentioned: For reading the status of the watchdog, it should never be connected to the CPU directly because in case of a CPU failure the output of the watchdog might be overdriven by the CPU. To avoid this, either a logic gate or a sufficiently large resistance should be added in between.

9.5 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 (T14.6.5 / T15.1.7). As this storage is a critical part of the EBS, its status must be monitored continuously while driving.

9.6 Redundancy

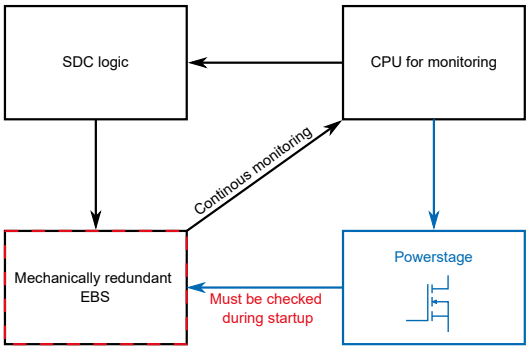

Figure 8: Schematic overview for a fully redundant EBS

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 (T15.3.3). On the electrical side redundancy can be ensured by a second output stage which enables the monitoring CPU to activate the EBS even if the SDC is failing. In case of failure of the monitoring CPU the EBS is activated automatically by the watchdog.

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

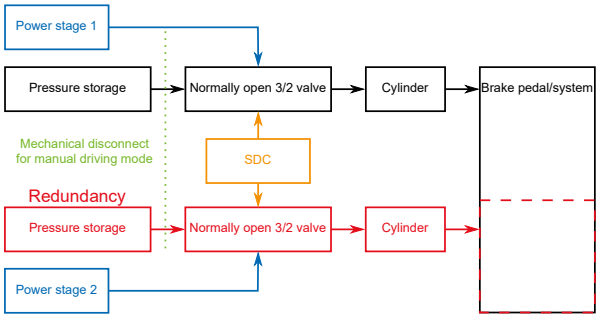

Figure 9: Actively applied braking energy

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.

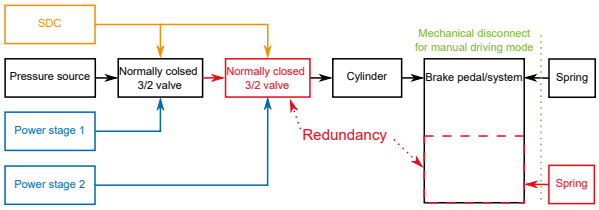

Figure 10: Removal of counterforce, which keeps the brakes opened

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 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 T14.8 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 activate 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.

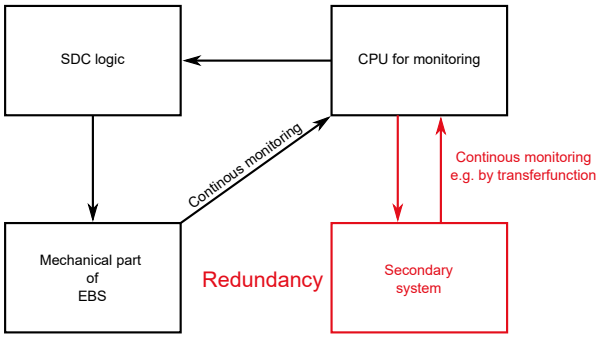

Figure 11: Schematic overview with secondary system as redundancy

9.7 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 will 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 activation:
During the inspection your EBS will be activated 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.

Rollover protection envelope (T1.1.16):
Make sure that your system complies with T15.1.2 since issues concerning this aspect of the rules are typically quite hard to fix.

Overpressure protection (T9):
Typcially a pressure relief valve is used to implement the overpressure protection mechanism. Valves with a non-adjustable (fixed) relief pressure threshold are recommended over valves with an adjustable one. For a fixed threshold checking the datasheet is sufficient. For an adjustable threshold the current value that is set needs to be demonstrated during technical inspection.

9.8 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. It focues 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 orange) including its overpressure protection (FL1, also see T9), 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 available 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 var-

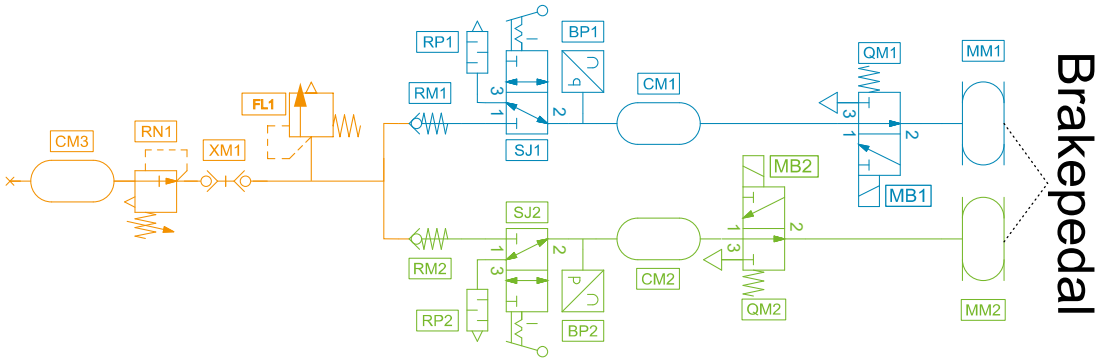

Figure 12: Pneumatic diagram example

ious 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 in 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

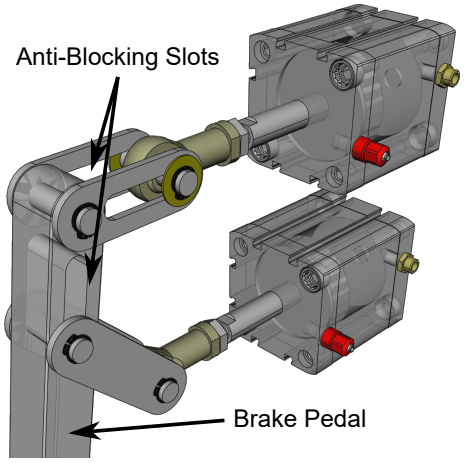

Figure 13: Two ASB actuators directly connected to the brake pedal

or manual braking operation. Thus, mechanisms as the shown anti-blocking slots are highly recommended.

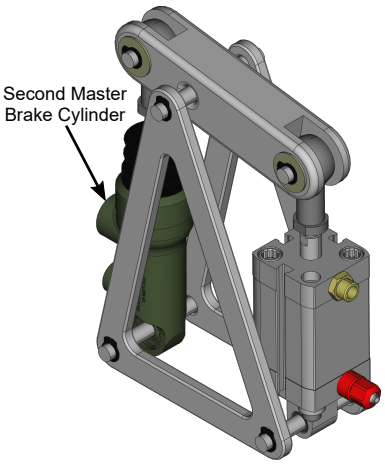

Figure 14: Brake actuation through an additional master cylinder

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 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 be done by an Shuttle(Or)-Valve. In any case it must be ensured, that the manual braking operation is always possible.

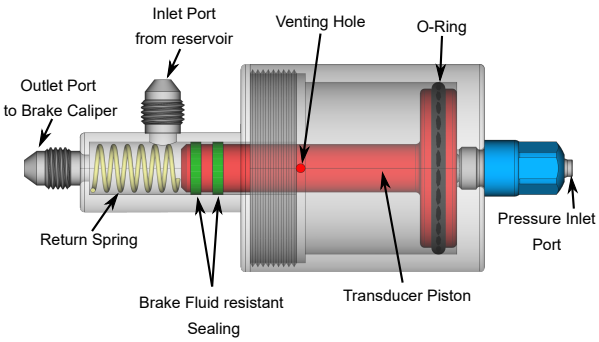

Figure 15: Brake actuation through a pressure transducer

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 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.

10 Steering system

As the steering system is controlled by the AS some safety precautions are required in order to avoid unintended actuation:
The supply of the steering system (or its power stages) needs to be directly controlled by the ASMS, for details see chapter 3. This will especially protect the driver from experiencing an unintended steering actuation by the AS during manual driving.

Additionally the AS shall not perform any actuation of the steering system that would lead to a movement of the steering rack while the vehicle is not R2D, see T14.7.1, so that it is still safe to be around the vehicle while the ASMS is already switched to the "On" position. Nevertheless, once the vehicle is R2D the AS is allowed to actuate the steering system in any manner even though the vehicle might still be in standstill. It needs to be considered that the torque required to move the steering rack will be quite high in that case. Thus, it is strongly recommended to not use steering actuators that need to perform a steering actuation for calibration purposes at startup (e.g. in order to determine a reference angle for straight driving). One exception regarding steering only being allowed while R2D applies during an emergency brake maneuver (EBS is activated) where the vehicle is not R2D anymore due to the open SDC: It is allowed (but not required) to perform a steering actuation until the vehicle reaches standstill, see T14.7.2, 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 13) and in case the vehicle breaks down during the dynamic events and quickly needs to be removed from the track by the officials. Especially in the second case only the ASMS will be switched to the "Off" position prior to moving the vehicle in order to not delay the dynamic events much further.

11 Actuator Decoupling

In order to ease up the design process it is allowed to disconnect the actuators of the AS while driving manually. As manual braking must always be possible, see T15.1.4, this mainly targets the steering actuator in order to enable lower steering forces for manual driving. It must always be ensured that the decoupling adds no additional hazard for the driver. Thus, the steering wheel must always stay connected and it must be avoided

that the decoupling mechanism moves while driving, see T14.8. It should also be considered to implement the mechanism in a way that avoids an unintended actuation by the driver. This is not required by the rules but might cause issues during technical inspection, if there are doubts regarding the driver's safety. In addition it might be beneficial to implement an easy to check indicator that provides a feedback of the current position of the decoupling mechanism (either mechanical or electrical) that can be checked right at the starting line before activating the AS.

Implementation hint: For decoupling the steering system, an electromagnetic clutch supplied by the ASMS might be a simple and robust option.

12 Sensors & Electrical Components Mounting

As per T11.11 sensors and electrical components must be properly mounted and located within a restricted area, see figures 3 and 16 of the rules. The area depicted by both figures combined defines possible positions for all electrical components including the sensors used by the AS. It specifies a maximum design area to prevent exaggerated designs. Exceptions are granted for antennas in order to allow a technically reasonable positioning. To enable a safe operation in manual mode, none of the sensors and electrical components is allowed to come into contact with the drivers helmet to avoid protrusions in case of a crash. This is typically checked with the tallest driver during technical inspection.

13 Manual driving

The manual driving mode intends to avoid injuries caused by any activation of the actuators based on the commands from the AS. By selecting the mission "Manual driving", the system is aware that a driver is seated in the vehicle and shall conduct the appropriate checks. To prevent human errors and to increase overall safety the system needs to ensure that the following conditions are fulfilled:

- The ASMS is switched off (actuators are not supplied). This could easily be evaluated by measuring the supply voltage on the actuator side of the ASMS.
- The ASB cannot interact with the brake system. This needs to be ensured by a check, see T14.4.1, that makes use of appropriate ASB sensor signals.
- Manual actuation of the steering wheel is possible.

All in all, the vehicle should behave comparable to a vehicle that is not equipped with an AS but still conducts some additonal supervision. All parts of the AS that do not interfere with manual driving (especially the processing units and sensors) are allowed to be active.

14 Startup procedure

To run the dynamic events as efficiently as possible, a common 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. Select the autonomous mission to be executed (must be possible without the use of an external device, see T14.11.3).
5. Select the proper RES mode (practice or race) depending on the "e-key" you are planning to use, also see below.
6. Queue and wait to approach the starting line. The LVMS may remain in "On" position.
7. 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)

8. Once the vehicle is properly aligned at the starting line, attach/arm the ASB (e.g. by operating the shut-off valves) after the approval of the officials.
9. Double check that the steering actuator is connected to the steering system.
10. Check that the correct mission (AMI) and RES mode has been selected.
11. Turn on the ASMS and activate the TS after the approval of the officials. (Hint: Shutdown buttons and RES remote device shall be checked in advance.)
12. Leave the area nearby the vehicle and proceed to the area designated for the ASR carrying the RES remote device.
13. Wait for the vehicle to reach "AS Ready" and send the go-signal after the approval of the officials.

15 Data logger

The intention of the data logger is to understand and reproduce the system state in case of failure, e.g. EBS is activated due to range loss of the 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 data logger. To be able to evaluate the recorded data, each team needs to provide a DBC file that includes a definition for all the signals mentioned above. Further hints regarding the data logger can be found in the competition handbook.

16 Autonomous System Form

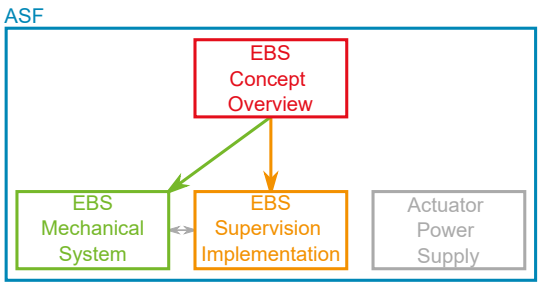

Figure 16: Overview of the ASF

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 focuses on the implementation of the ASB as its implementation is the most complex and prone to failures.
To ensure that all the other parts of the AS, that have not been reviewed, are working as intended, it is always recommended to check all the checklist items of the technical inspection in advance (see Last years Inspection Sheet).
Another purpose of the ASF is to provide a proper documentation in order to identify test cases for the ASB in advance and to ease up technical inspection. To generate this documentation the ASF consists of multiple documents which need to be prepared in a certain format. To generate a common understanding of the documents and to unify the documentation, some rules have to be followed. These rules and some examples are part of the ASF example documents. These can be found throughout the year with a lot of additional information on the ASF at the hands on ASF page.

17 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 the officials. 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. Nevertheless, passing technical inspection does not fully certify the vehicle's rules compliance and therefore further checks during and after the dynamic events may be conducted, see IN 12.1.1. If the vehicle violates any of the rules, it may receive a Disqualified (DQ) or penalty points, also see IN 12.1.4.

The AS related parts of the technical inspection are part of the mechanical and electrical inspection. The former takes care of sensor positions, mechanical ASB design and mountings. The latter checks all other as-

pects of the AS, such as the overall ASB concept, sensor diagnosis or the inspection mission. The inspection mission is used to simulate a fully operational AS 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 e.g. allows to check a correct ASSI functionality and other safety features. The main focus is the ASB where 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 in order to evaluate the system's response.
Details on the procedure can be taken from the inspection sheets which can be downloaded from the FSG website prior to the competition. Throughout the season one might refer to last years inspection sheet as a preliminary source of information.

The final part of the technical inspection concerning the AS is the EBS brake test. It checks that the vehicle delivers the required brake performance, see T15.4.2, under dynamic conditions. The details of the test are described in IN11.2.