EBS Reference Guide 2020/21

Martin Stollberger / Mathias Gebhardt

November 1, 2020

Abstract

This document is indited to give you a reference for implementing the new Emergency Brake System (EBS) rules. Following this guideline eases the design of your EBS and helps us to faster review the safety of your design. Following this guide does not automatically mean, that you'll pass the Autonomous System Form (ASF) review. This guide only delivers some suggestions for your design. More complex solutions are still welcome. Finally it is still the teams responsibility to ensure a safe design and explain how the safety concept works. Be prepared for critical reviewer questions.

1 Introduction

The references given in this document are mainly based on the Formula Student Rules 2020 Version 1.0. Its main focus is to give some details on the implementation of a non-programmable logic part which is required by DV 1.5.2.

This document also gives a short introduction on failure detection and failure handling during startup and operation (see DV 3.2). Furthermore, DV 3.2 requires some kind of redundancy for the EBS. Some suggestions are made on how to design this system redundant.

The last topic is about the testability during technical inspection. As the EBS signals are part of the autonomous system, they are considered to be System Critical Signal (SCS) (see DV 2.1.1) and there are some points which should kept in mind. This will speed and ease up the Driverless Vehicle (DV) inspection for the teams and the officials.

2 System Overview

Figure 1 shows a rough overview of a possible EBS implementation. The Remote Emergency System (RES) is directly integrated in the Shutdown Circuit (SDC) (denoted in orange) and the EBS actuator supply (denoted in green) with its relay output, as required by DV 1.4.4 and DV 3.1.2. There is also some non-programmable logic integrated into the SDC, to enable the Autonomous System opening 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 must be the last device inside the shutdown circuit directly before the Tractive System Master Switch (TSMS) (EV 6.1.4), to detect an opened SDC and latch it (DV 1.5.2).

The EBS itself consists of the following main parts:

Supervisor: The supervisor monitors the status of the EBS and performs the initial checks for the system. In case of failure the CPU triggers the EBS and/or its redundant system (DV 3.2.1) and also lights up the EBS failure indicator required by DV 3.2.7.

SDC Non-programmable logic part: The SDC's non-programmable logic is used to handle the SDC as required by DV 1.5.2. 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.

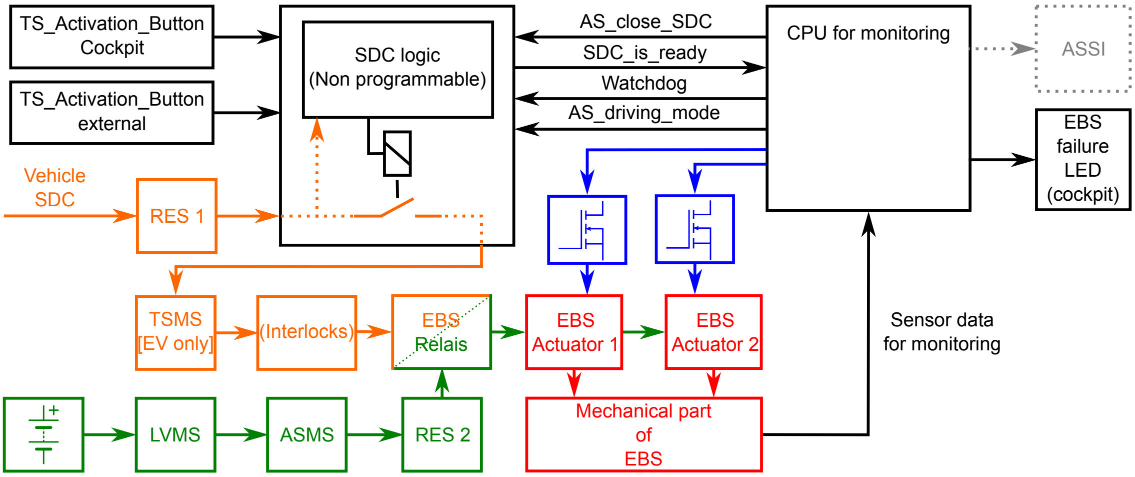

Figure 1: *General EBS overview*

Mechanical part: We will define the mechanical part of the EBS 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 (DV 3.1.3). Depending on the system it also must include some sensors for monitoring and the initial check sequence (DV 3.2.4).

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

3 EBS Supply concept

Figure 2 shows the EBS supply concept as required by Rule DV 3.1.2 (green path). Additionally figure 2 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 EV 6.1.5 is only applied to the Accumulator Isolation Relay (AIR)s and not to the EBS relay. Finally the supply concept includes two Powerstages/MOSFETs (blue parts). These additional switches are required to fulfill DV 3.2 and enable the supervisor to test both actuation paths independently.

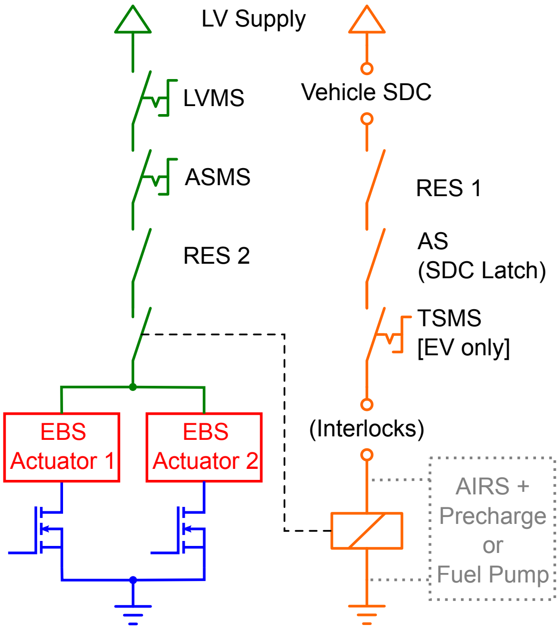

Figure 2: *Realization of Rule DV 3.1.2: EBS supply*

4 Supervisor

As previously mentioned, the supervisor:

1. Monitors the system to detect failures.
2. Brings the system to a safe state in case of a single failure (DV 3.2.1).
3. Services the EBS Failure LED (DV 3.2.7)
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 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.

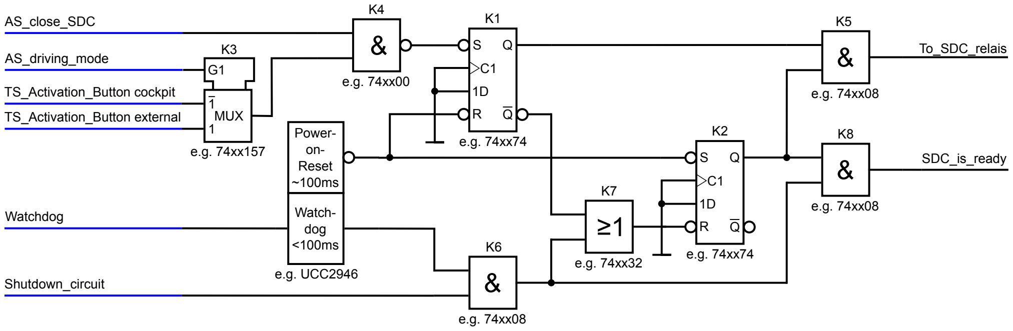

Figure 3: *Logic diagram for EBS non-programmable logic part, (blue line = pull-down termination required)*

The supervisor needs to handle the EBS states 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 Tractive System (TS) via the tractive system activation button (see EV 4.11.2), 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 if working fine.

4.1 Initial Checkup Sequence

An initial checkup sequence is necessary to determine all kind of failures which could not be detected during operation without triggering the EBS. This kind 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 Shutdown Circuit to close (”*SDC_is_ready*” is high).
3. Stop toggling Watchdog.
4. Check ”*SDC_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 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 2).
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 2).
14. Check that the brake pressure is still build up correctly.
15. Enable EBS actuator 2 again.
16. Transit to ready state

4.2 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 EBS 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 2).
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.

5 Non-programmable Logic

Figure 3 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 Fig. 3). As protection circuits are mandatory for safety, there will be some examples in Section A.

The non-programmable logic part consists of two Flip-Flops which are latching the corresponding states until the next power cycle:

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 EV 4.11.4 is met and the Autonomous System (AS) cannot activate the SDC by a software fault.

A detailed signal description can be found in the supervisor section above (Section 4).

6 Mechanical Part

The mechanical part of the EBS must be designed in such a way, that the stored brake energy is released without the aid of electrical power (DV 3.1.3). This is in order to ensure 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 pressure release (DV 2.2.5 / DV 3.1.6). As this storage is a critical part of the EBS, its status must be monitored continuously while driving.

7 Redundancy

7.1 Fully-redundant EBS

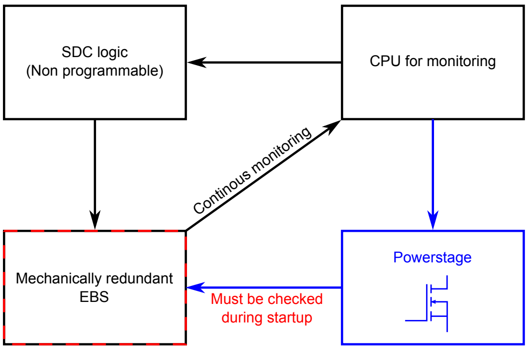

Figure 4: *Schematic overview for a fully redundant EBS*

A fully redundant EBS means, that the system is still able to come to a safe state, even if a single failure occurs (DV 3.2.1). On the electrical side redundancy is 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.

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

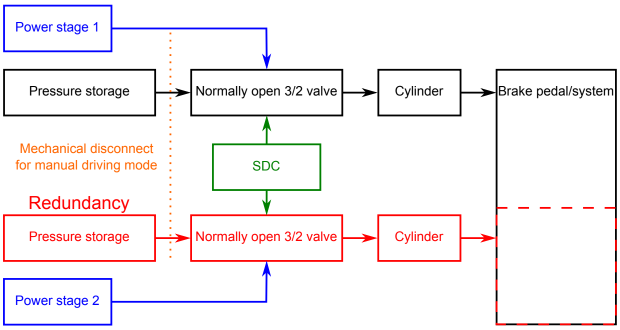

Figure 5: *Actively applied braking energy*

Figure 5 shows an EBS 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 consist 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.

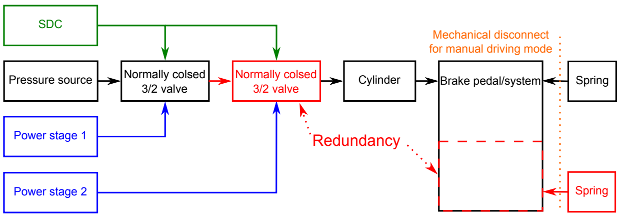
SDC
Pressure source
Normally colsed 3/2 valve
Normally colsed 3/2 valve
Cylinder
Brake pedal/system
Spring
Mechanical disconnect for manual driving mode
Power stage 1
Power stage 2
Redundancy
Spring

Figure 6: *Removal of counterforce, which keeps the brakes opened*

Figure 6 shows an EBS 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. 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.

7.2 Service Brake System as Redundancy

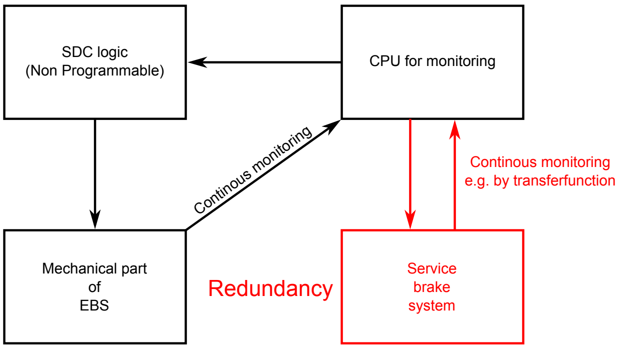

Figure 7: *Schematic overview with service brake system as redundancy*

If the vehicle is equipped with a service brake system for autonomous mode, it is possible to use it as redundancy for the EBS (DV 3.2.6). The only thing that has to be taken into account is, that this system 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, for example.

8 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 to long too sufficiently test the system you'll need to requeue.

8.1 SCS

As all signals of the EBS 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.

8.2 Accessibility

All parts of the EBS should be easily accessible without excessively disassembling the car. Especially all mechanical EBS relevant parts and all hydraulic/ pneumatic parts beside the vehicles brake system.
All parts must be properly attached to the vehicle.

8.3 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 Low Voltage Master Switch (LVMS) power cycle is needed (DV 1.5.2) it might also be helpful if you are able to supply your main CPU externally during tech inspection. This avoids 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 Autonomous System Master Switch (ASMS), which might be the better option.

9 Rule Changes

DV 1.1 Introduced common wording for Electric Vehicle (EV) and Internal Combustion Engine Vehicle (CV):
The wording R2D, TS active and TS activation button is now also being used on combustion vehicles.

DV 1.2.2 Refined wording:
The wording was refined to explicitly state, that the RES is the only device which is allowed to send wireless commands to the vehicle.

DV 1.4.4 Clarified RES integration into the SDC:
Clarified that the RES needs to be integrated directly with one of its relays into the SDC.

DV 1.5.2 (former DV 1.5.3) Manual reset now possible:
For the reset of the non-programmable logic a manual reset button is now allowed additionally to the LVMS power cycle.

DV 1.5.3 (former DV 1.5.4) Refined wording to make the intent more clear.

DV 2.3 Added a new chapter for the steering actuator:
It is now only allowed to move the steering actuator while the vehicle is R2D. Manual steps for deactivating the steering system are forbidden.

DV 2.5 (former DV 2.3) Moved the Autonomous System Status Indicator (ASSI) chapter.

DV 2.5.1 Added the color table.

DV 2.5.4 (former DV 2.4.8) Sound measuring procedure added:
The given sound levels for the ASSI of 80 to 90 dBA need now to be reached in a radius of 2 m around the vehicle.

DV 4 Enhanced the sensors chapter to components as well.

DV 4.1.3 Unified envelope definition:
As sensor and component envelope the surface envelope of T 1.1.16 has now to be used.

DV 4.1.4 Exceptions for antennas and components:
Antennas now may protrude from the envelope up to 100 mm and components placed behind the cockpit may now have 25 % of their bounding box volume outside the envelope.

Appendix

A Electrical Input/Output Protection

This section is not directly related to the Rules but should give some design hints for a proper implementation of the non-programmable logic part, as the protection circuits are mandatory for safety. All considerations in this appendix are based on common practices for input/output protections for digital logic. These protections are always necessary when the logic is connected to external ports which are not part of the common PCB e.g. the vehicles wiring harness.

A.1 Digital Inputs

For inputs common problems are:

- Over voltage (exceeding VCC/GND) due to ESD
- Excessive input currents due to short circuit to higher voltage supply
- Small spikes that cause the logic to change their state

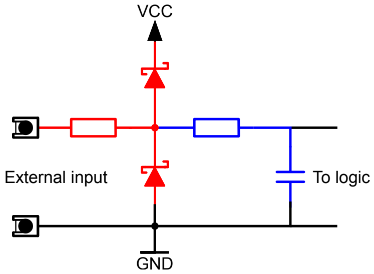

Figure 8: *Digital input scheme, for protection and filtering*

Figure 8 shows a circuitry which deals with this problems. The red part is the over voltage protection and input current limitation. The blue part is a first-order RC filter to suppress small spikes.

The red diodes are fast switching Schottky diodes they clamp the input voltage to approx. $VCC + 0.5\,\text{V}$ and $GND - 0.5\,\text{V}$. The resistor must be suited to limit the clamping current appropriate.

For example: the highest external voltage is your GLVS supply with max. $15\,\text{V}$ and the logic VCC is set to $5\,\text{V}$. A resistor of $100\,\Omega$ limits the continuous clamping current to $100\,\text{mA}$.

Another consideration for this resistor is its thermal capacitance. In case of ESD a lot of energy is dissipated in this resistor. Therefore, a 1206 SMD resistor is much better than a 0603 SMD resistor.

A.2 Digital Outputs

Digital outputs face similar problems as the inputs:

- Over voltage (exceeding VCC/GND) due to ESD
- Excessive reverse currents due to short circuit to higher voltage supply
- Excessive forward currents due to short circuit to GND (chassis)

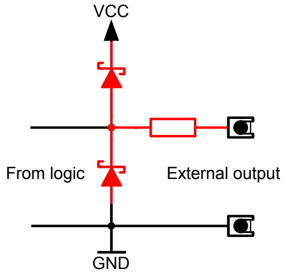

Figure 9: *Digital output scheme, for protection against external voltage*

The red part of Figure 9 is pretty much the same as the red part in Figure 8. On the output the resistor additionally limits the output current to VCC/R.

A.3 Power Outputs

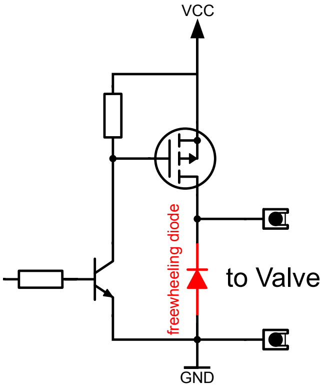

Figure 10: *Power stage output scheme, with protection against fly back voltage of inductive loads*

Special care has to be taken when diving inductive loads with a power stage. As a switched off inductor inducts a huge reverse voltage, a freewheeling diode must be implemented to protect the output transistor against over voltage (see Figure 10 red part).

Changelog

V1.0: Compiled guide against the most recent rules version and updated the rules changes chapter.