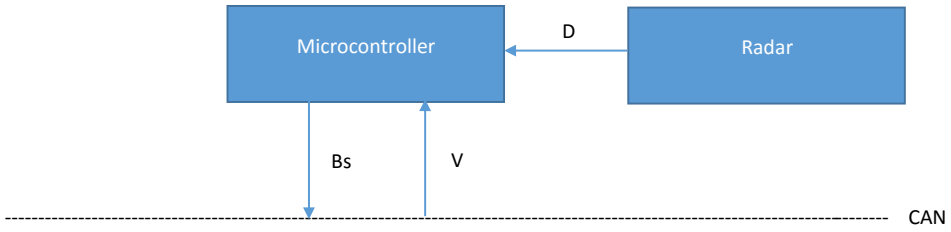
Autonomous Emergency Braking (AEB)

Item definition

Given the current vehicle speed V, and the distance D of the vehicle from the preceding vehicle, if $\frac{V^2}{100} \geq D$, then the AEB activates the brake request and keep braking the vehicle until $\frac{V^2}{100} < D$.
The brake request is either 0 (indicating no brake is needed) or 1 (indicating that bake is needed). The AEB receives the vehicle speed V and the distance D every 100 msec, and decides whether a brake is needed or not.

Graphically:



Where:

- D is the distance of the preceding vehicle
- V is the speed of the vehicle
- Bs is the brake signal

Elements of the item:

Microcontroller (CPU + embedded memory + CAN interface), radar.

Interaction of the items with other items:

The item interacts with the Body Computer through the CAN for receiving the vehicle speed and for providing the brake signal.

Identification of provided functionalities to other items:

The item provides the brake signal to the Body Computer through the CAN.

Identification of required functionalities from other items:

The item requires the vehicle speed from the Body Computer through the CAN.

Identification of hazards:

To identify correctly the hazards, we can firstly perform the FMEA (Failure Mode & Effect Analysis):

- FM1: radar breaks → distance is not correctly measured.
  Note that this failure can lead to different situations: distance measured is smaller than the real one or distance measured is higher than the real one. Anyway the main point is that the measure is not correct anymore due to the failure.
- FM2: microcontroller breaks → break signal is not reliable.

Also for this failure we can have different situations, but the key point is that the microcontroller is not able to correctly perform the algorithm and as a consequence the brake signal is not correct.

- FM3: CAN interface breaks → information is not correctly exchanged with the CAN.

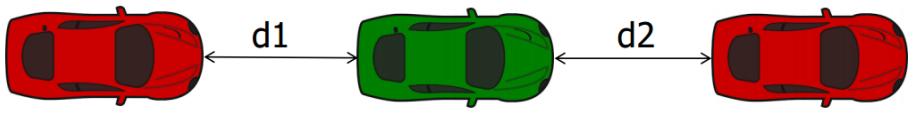
All these failures lead to two main hazards that we have to take into account for the Hazard Analysis and Risk Assessment of the item:

- H1: the item sends the brake signal when is not required (i.e. $\frac{V^2}{100} \geq D$).
- H2: the item does not send the brake signal when is required (i.e. $\frac{V^2}{100} < D$).

Identification of operational situations:

The key point in the identification of the operational situations is that we have to consider also the eventual presence of a following car. Hence we call:

- d1 the distance between the car under analysis and the following one
- d2 the distance between the car under analysis and the preceding one



As a consequence, we can discriminate the operational situations by considering:

- Distance that can be higher or smaller with respect to safety distance (safey distance $= \frac{V^2}{100}$).
- Speed that can be higher or smaller than a threshold value, we will consider 30 km/h as threshold. (the speed will distinguish different degrees of severity).

Therefore, the operational situations are:

- OS1: V < 30 km/h, d1 < safety distance, d2 > safety distance;
- OS2: V > 30 km/h, d1 < safety distance, d2 > safety distance;
- OS3: V < 30 km/h, d1 > safety distance, d2 < safety distance;
- OS4: V > 30 km/h, d1 > safety distance, d2 < safety distance;
- OS5: V < 30 km/h, d1 < safety distance, d2 < safety distance;
- OS6: V > 30 km/h, d1 < safety distance, d2 < safety distance;
- OS7: vehicle moving and a pedestrian or a cycle crosses the road.

Note that it is useless to consider the operational situations in which:

- OS8: V < 30 km/h, d1 > safety distance, d2 > safety distance;
- OS9: V > 30 km/h, d1 > safety distance, d2 > safety distance;

In fact, in both of them, the distance is limit is respected and there is no risk.

ASIL determination:

Operational Situation	H1	ASIL	H2	ASIL	Notes
OS1	S = 1 E = 4 C = 2	A	S E C		H2 cannot take place in OS1 since d2 > safety distance
OS2	S = 2 E = 4 C = 3	C	S E C		H2 cannot take place in OS2 since d2 > safety distance
OS3	S = 1 E = 4 C = 2	A	S = 1 E = 4 C = 1	QM	
OS4	S = 2 E = 4 C = 3	C	S = 2 E = 4 C = 2	B	
OS5	S = 2 E = 4 C = 2	B	S = 2 E = 4 C = 1	A	
OS6	S = 3 E = 4 C = 3	D	S = 3 E = 4 C = 2	C	
OS7	S = 3 E = 3 C = 3	C	S = 3 E = 3 C = 2	B	

Commentato [PL1]: Forse l'exposure va comunque messa a 4

General notes:

- The exposure is always 4 for the OS 1-6, in fact it is a common condition (> 10% of the driving time) to be driving either at low speed (V < 30 km/h) or at high speed (V > 30 km/h).
- The controllability has been set according to the following rules:
  - H1 is considered less controllable than H2 since the driver does not expect that behaviour and he cannot control it by breaking or accelerating. Hence:
    - If V < 30 km/h → C = 2;
    - If V > 30 km/h → C = 3;
  - H2 is considered more controllable than H1 since the driver needs only to brake to avoid dangerous situations. Then:
    - If V < 30 km/h → C = 1;
    - If V > 30 km/h → C = 2;
- The severity has been set according to the following rules:
  - If V < 30 km/h, then:
    - If only one of the two distances is not respected → S = 1;
    - If both the distances are not respected → S = 2;
  - If V > 30 km/h, then:
    - If only one of the two distances is not respected → S = 2;
    - If both the distances are not respected → S = 3;
- For what concerns OS7:
  - The exposure is set to 3 since we consider an urban scenario, then it is medium probable (1% - 10% of driving time) to have a pedestrian or a cycle crossing the road.
  - The severity is always set to 3.
  - The controllability depends on the hazard.

Definition of Safety goals:

The item shall measure correctly the distance of the preceding vehicle and shall send the brake request only if the condition $\frac{V^2}{100} < D$ is verified.

Definition of Functional Safety Concepts:

Since an ASIL D combination came out during the analysis, a lot of resources have to be spent in the functional safety concepts definition.

- FSC1: An ASIL D compatible microprocessor has to be used.
- FSC2: the item shall perform self-test in order to check the correct behaviour of all the components. If any misbehaviour is detected, then the item shall transit to safe state.
- FSC3: redundancy is crucial in case of ASIL D. Hence two radars shall be used to compare the different measurements and eventually two microcontrollers in master-slave configuration.
- FSC4: a bypass circuit which receives V and D and combines them through some logical ports shall be implemented.
- FSC5: an external check of the ECU correct working condition shall be implemented.

Commentato [PL2]: Eventual definition of ASIL D compatible microprocessor

Commentato [AS3R2]: Direi che possiamo risparmiarcela

Commentato [PL4]: Master-slave because is the one we're gonna implement

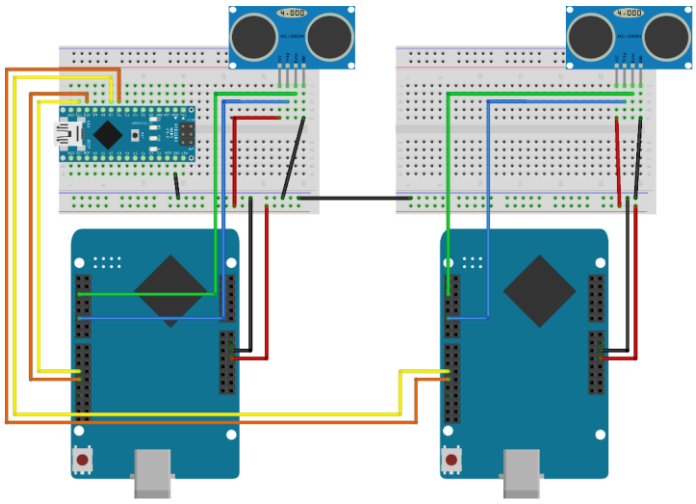
Commentato [PL5]: Ale fai il disegnino con le porte logiche e il comparatore. Forse ce lo possiamo risparmiare A me al momento altri FSCs non vengono in mente, in caso aggiungi qualcosa tu. FATT

Definition of the Safe State:

If only one of the microcontrollers is working, then the other is disabled and the driver is informed.

If both the microcontrollers are not working, the item is disabled and the driver is informed of the malfunction (e.g. through a led in the dashboard).

Implementation of redundancy:



In this configuration two boards work in parallel to measure the distance independently and issue brake request. One board is the master and the other is the slave. Only the master can issue brake request. In case of malfunction of the master the slave becomes able to issue brake requests.