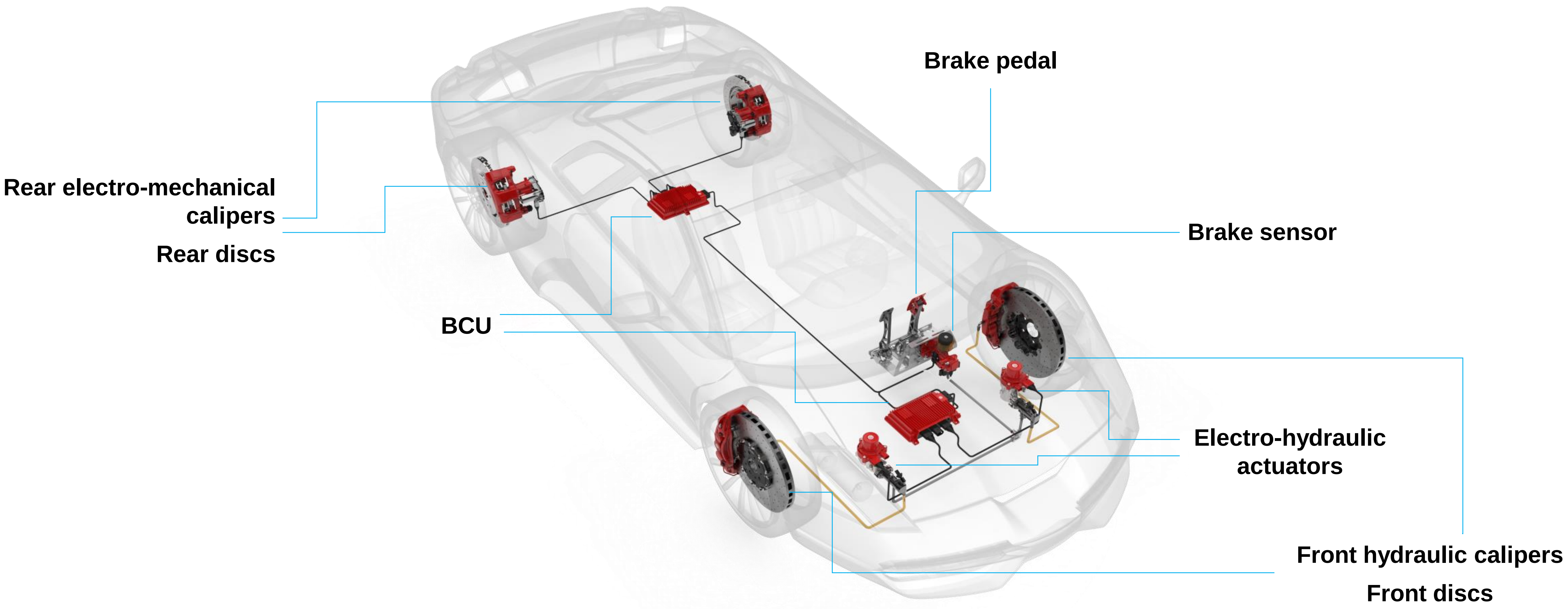
Safety in Automation Systems - Project

System Hazard Analysis of the Brake By Wire system by Brembo

Giovanni Porcellato, Francesco Sacchi

System Architecture



Functioning of the System

- The driver pushes the brake pedal
- The pedal sensor encodes the force exerted on the pedal and sends the related signals to front and rear BCUs
- Front and rear BCUs process the signal received by the pedal and relays an actuation signal to actuators and calipers
- The front electro-hydraulic actuators convert the electronic signal to hydraulic pressure
- At the same time, the rear electro-mechanical calipers convert the electronic signal to clamping force

Advantages of BBW System

1. **Reduction of braking distance**:
   BBW enables a remarking reduction of braking distance thanks to faster response time and integrated braking logics
2. **Tuning of braking torque**:
   The driver can choose between different braking settings
3. **Tuning of pedal feel**:
   The driver can choose between pedal responses according to personal preferences
4. **Reduced load sensitivity**:
   The braking torque automatically adapts to vehicle load, keeping braking distance constant
5. **CO^2 emission reduction**

Details about BCU

The braking torque that each wheel must generate is computed by the two BCUs, that play an important role in braking safely. These control units implement all the automatic control logics needed to get the actuation signal for an optimal braking (ABS, ESC…).

Analyzing these logics one by one would mean to go much deeper in physical braking details, and to specify BCU software architecture, which is unknown. Their failure is still taken into account, though in a general way, as BCU software failures.

Anyway, they cannot be considered as safety functions since they are part of the functioning of the system itself, and not functions activating in case of detection of system faults: their presence is always needed by the BCU's to compute the optimal torque in every condition, not just as a safety measure.

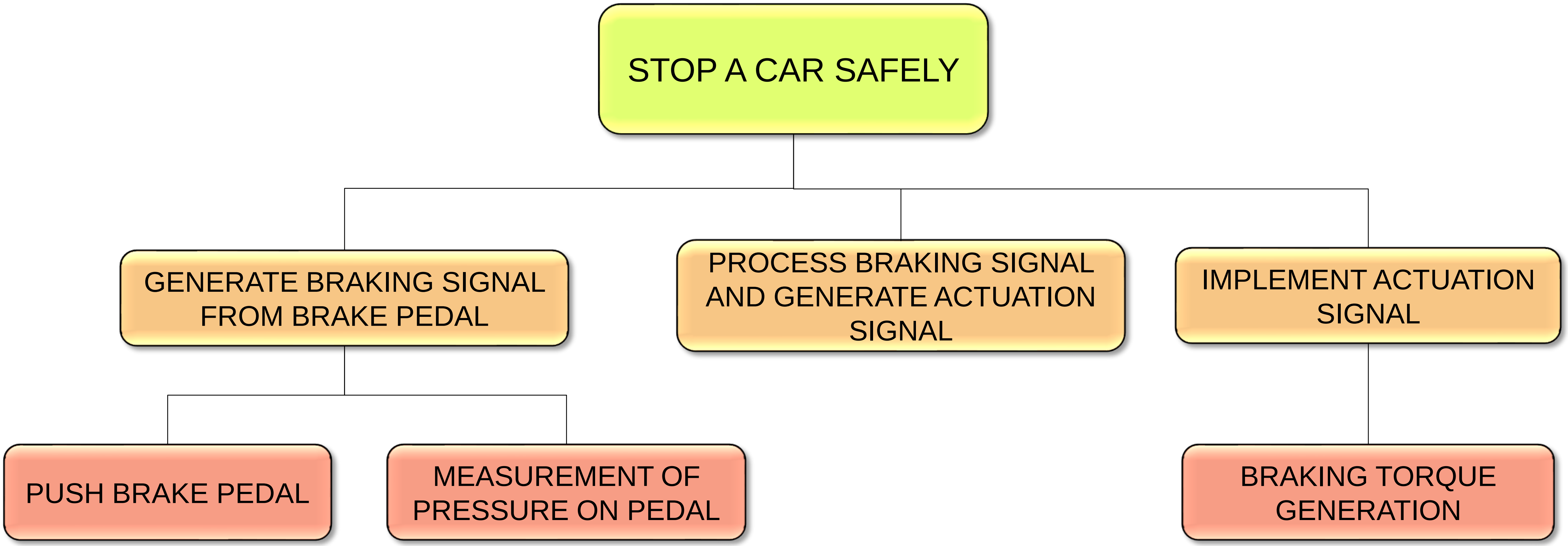
Safety Function

The only safety function is an additional braking system.

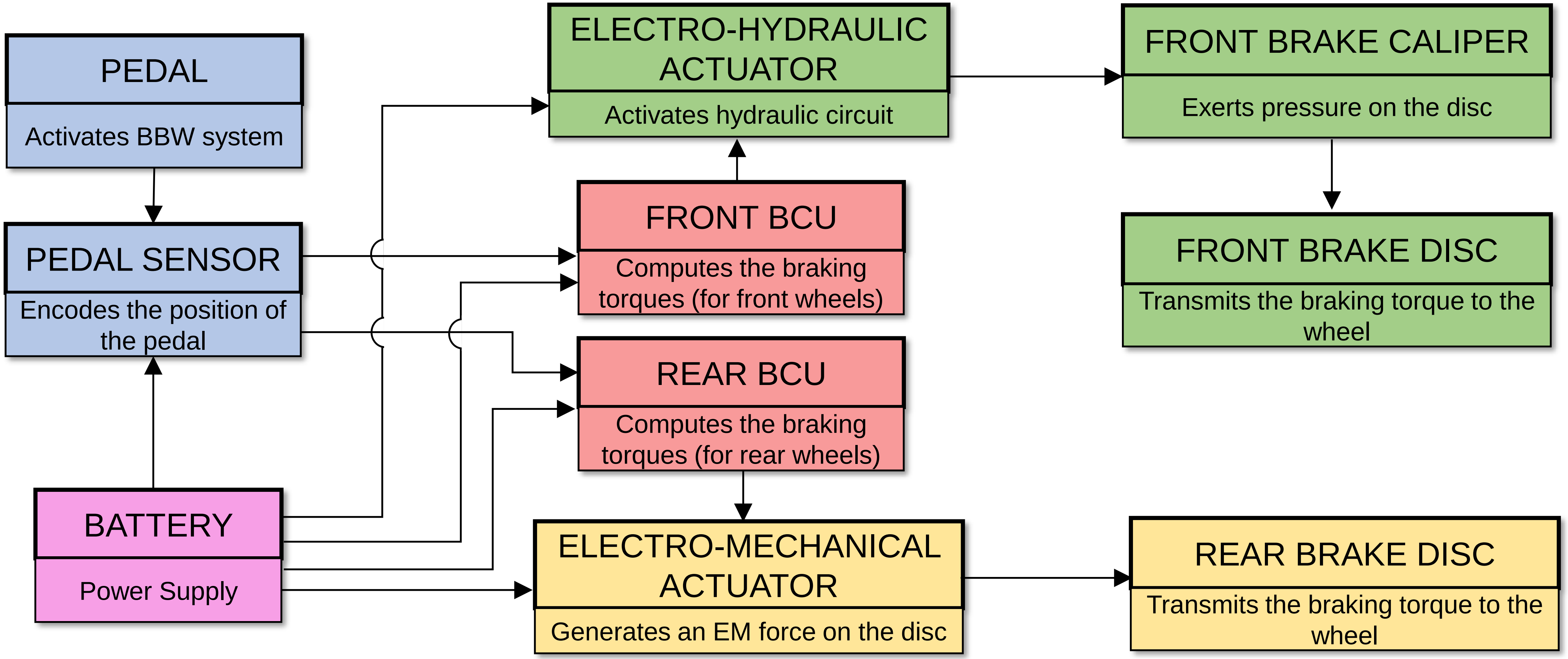
This is a traditional, purely hydraulic braking system activated directly from the brake pedal, if the battery does not work.

In particular, this braking system acts only on the front wheels and uses the same front hydraulic actuators of the BBW.

Functional Analysis



Structural Analysis



Operating Conditions

Operating Condition	Description	Involved Subsystems
BBW not activated	The brake pedal is not pushed, BCU's do not get nor send signals, actuators are idle.	BCU (in idle condition)
Transmission of braking signal	The brake pedal is pushed and the braking signal must be relayed to BCU's and to actuators	Brake pedal and pedal sensor Front and rear BCU's
BBW operating	The brake pedal is pushed, BCU's compute required torques and actuators are working	Brake pedal and pedal sensor Front and rear BCU's Front and rear actuators Front and rear discs and calipers
Release of braking	The brake pedal is released, the actuators stop operating	Brake pedal and pedal sensors Front and rear BCU's Front and rear actuators Front and rear discs and calipers

PHA

Hypothesis

A hypothesis required to apply the PHA method is the removal of all the safety functions. In this case, the hydraulic back-up system, that is the only safety function of the Brembo BBW, is not taken into account.

Targets

- Passengers of the car
- Car
- People outside the vehicle
- Environment (everything surrounding the vehicle)

PHA

Operating condition	Causes	Phenomenon	Effects
Transmission of braking signal	Pedal is stuck in non-braking position; Sensor is not working; Signal transmission wires are not working; Battery failure	Braking signal is not received by the BCU's	Missing deceleration; Harm for the passengers; Damage to the environment and other people; Damage to the car
Transmission of braking signal	Braking signal is not received by the BCU's; Fault of BCU; Signal transmission wires are not working; Battery failure	Actuation signal is not transmitted by the BCU's	Missing deceleration; Harm for the passengers; Damage to the environment and other people; Damage to the car
BBW not activated	Fault of BCU	Braking system activates without braking command	Unintended deceleration; Harm for the passengers; Damage to other people; Damage to the car

PHA

BBW Operating	Actuators pumps fault; Fault of BCU; hydraulic circuit leakage; hydraulic pressure sensor fault; Stuck calipers; Battery failure	Front actuators/calipers do not work properly	Missing/uncontrolled deceleration; Drift; Harm for the passengers; Damage to the environment and other people; Damage to the car
BBW Operating	Actuator EM motor fault; Fault of BCU; Stuck Calipers; Battery failure	Rear actuators do not work properly	Missing/uncontrolled deceleration; Drift; Harm for the passengers; Damage to the environment and other people; Damage to the car
Release of braking	Brake pedal stuck lowered; Sensor mismeasurement; Fault of BCU	BCU’s keep sending signal	Unintended/excessive deceleration; Harm for the passengers; Damage to other people; Damage to the car

PHA

Release of braking	BCU’s keep sending signals; actuators stuck in operating mode	Actuators keep working	Unintended/excessive deceleration; Harm for the passengers; Damage to other people; Damage to the car
BBW operating	Pedal stops working; Sensor mismeasurement; Fault of BCU; Battery failure	Wrong computation of torques	Missing/uncontrolled deceleration; Drift; Harm for the passengers; Damage to the environment and other people; Damage to the car

Risk Assessment Matrices

Time interval: 10 years

Targets: Passengers of the car and people outside the vehicle

	Probability of Mishap					
Severity of consequences	F Impossible	E Improbable	D Remote	C Occasional	B Probable	A Frequent
I. Catastrophic						
II. Critical				3		
III. Marginal			2			
IV. Negligible			1			

Targets: Car and environment

	Probability of Mishap					
Severity of consequences	F Impossible	E Improbable	D Remote	C Occasional	B Probable	A Frequent
I. Catastrophic						
II. Critical					3	
III. Marginal				2		
IV. Negligible				1		

Severity of consequences

Target: Passengers and People outside

I. Catastrophic	Death
II. Critical	Severe injury
III. Marginal	Minor injury
IV. Negligible	No significant harm

Target: Car

I. Catastrophic	Complete destruction
II. Critical	Structural damage
III. Marginal	Secondary damage
IV. Negligible	Superficial damage

Target: Environment

I. Catastrophic	Destruction of the surroundings
II. Critical	Consinstent damage
III. Marginal	Minor damage
IV. Negligible	Negligible effects

PHA

PROBABILITY INTERVAL: 10 YEARS	Risk before					Risk after		
Hazard	Target	Severity	Probability	Risk code	**Description of Countermeasures**	Severity	Probability	Risk code
Braking signal is not received by the BCU’s	P	I	D	3	Design of pedal with reliable material and components; multiple pedal sensors for redundancy; BCU’s stop the car if they do not receive a minimum signal (i.e. when a wire ingoing in BCU is damaged); traditional braking system (backup for battery failure)	II	E	2
	C	I	D	3		II	E	1
	E	II	D	2		III	E	1
Actuation signal is not transmitted by the BCU’s	P	I	D	3	Robust design of BCU hardware and software; actuators stop the car autonomously if they do not receive a minimum signal (i.e. when a wire outgoing from BCU is damaged); traditional braking system (backup for battery failure)	II	E	2
	C	I	D	3		II	E	1
	E	II	D	2		III	E	1

P = people (passenger and people outside); C = car; E = environment

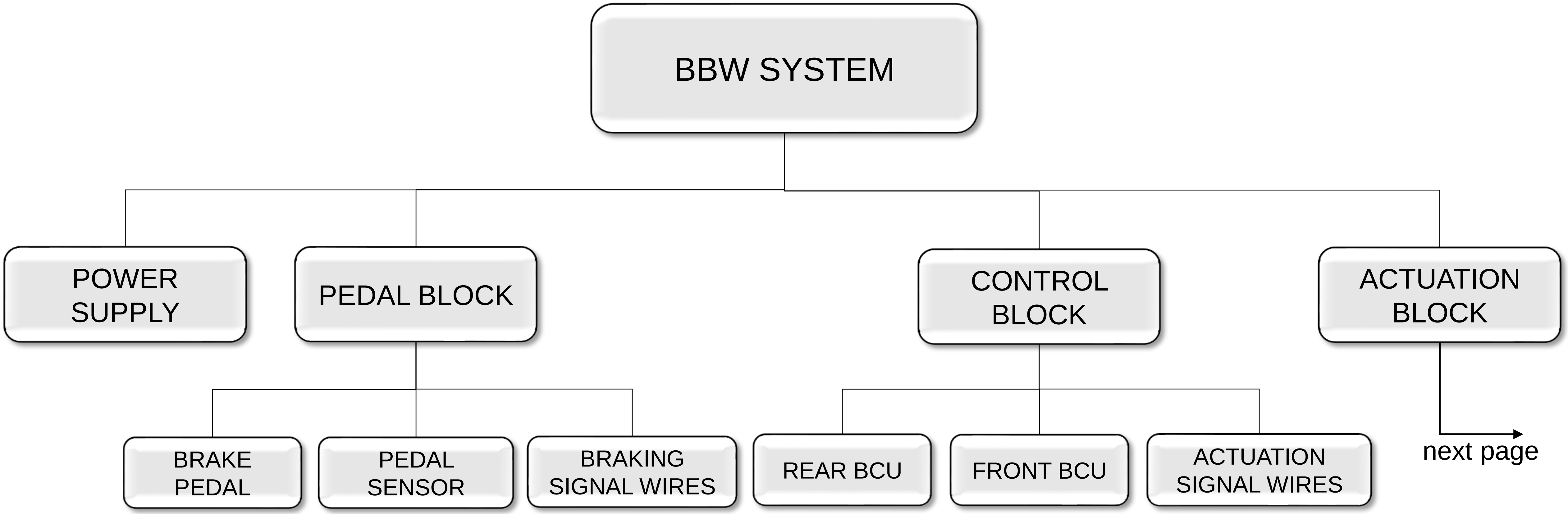
PHA

Hazard	Target	Severity	Probability	Risk code	Description of Countermeasures	Severity	Probability	Risk code
Braking system activates without braking command	P	III	D	2	Robust design of BCU hardware and software	III	E	1
	C	III	D	1		III	E	1
	E	IV	D	1		IV	E	1
Front actuators/calipers do not work properly	P	I	D	3	Periodic maintenance of actuators/calipers components; traditional braking system (backup for battery failure)	I	E	3
	C	I	D	3		I	E	3
	E	II	D	2		II	E	1
Rear actuators do not work properly	P	I	D	3	Periodic maintenance of actuators components	I	E	3
	C	I	D	3		I	E	3
	E	II	D	2		II	E	1

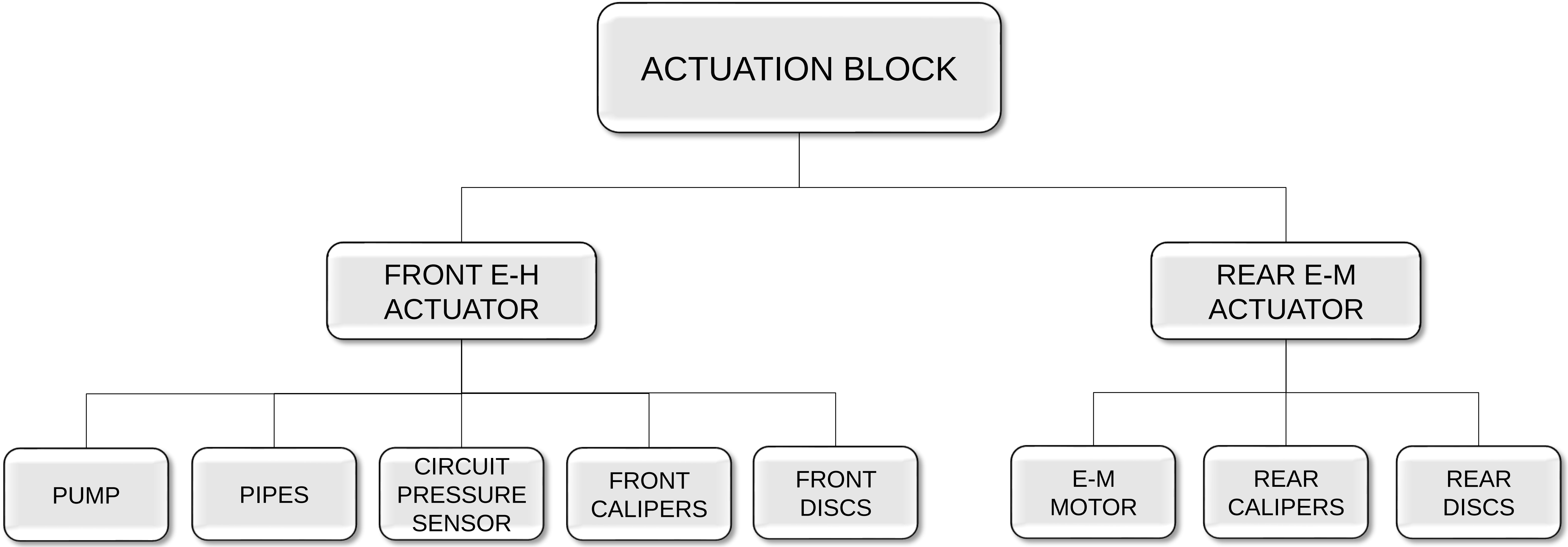
PHA

Hazard	Target	Severity	Probability	Risk code	Description of Countermeasures	Severity	Probability	Risk code
BCU's keep sending signal	P	IV	C	1	Robust design of BCU hardware and software	IV	E	1
	C	III	C	2		III	E	1
	E	IV	C	1		IV	E	1
Actuators keep working	P	IV	C	1	Robust design of actuators; periodic maintenance of actuators	IV	E	1
	C	III	C	2		III	E	1
	E	IV	C	1		IV	E	1
Wrong computation of torques	P	I	D	3	Robust design of BCU's; multiple pedal sensors for redundancy; traditional braking system (backup for battery failure)	I	E	3
	C	I	D	3		I	E	3
	E	II	D	2		II	E	1

FMEA – Components scheme



FMEA – Components scheme



FMEA (Transmission of braking signal)

Component	Failure mode	Failure causes	Failure effects	Seve-rity	Proba-bility	Control Measures
Power supply	Power outage	• Discharged battery • Overheated battery	No output current	I	D	Purely hydraulic backup system Emergency battery
Brake pedal	Stuck non-braking	• Mechanical failure • Physical obstruction	No braking signal generated	I	D	Predictive maintenance; Visual Inspection
Pedal sensor	Wrong measurement	• Wrong Calibration • Structural damage	Wrong braking signal generated	I	E	Use a high quality sensor; Add an auxiliary sensor
	No output signal	• Structural damage	No braking signal generated	I	E	Use a more robust sensor
Braking signal wires	No throughput signal	• Structural damage	No braking signal generated	I	E	Predictive wire maintenance

FMEA (Transmission of braking signal)

Component	Failure mode	Failure causes	Failure effects	Seve-rity	Proba-bility	Control Measures
Rear BCU	No output signal	• Structural damage	No braking signal generated	I	D	Test periodically the integrity of the component
Front BCU	No output signal	• Structural damage	No braking signal generated	I	D	Test periodically the integrity of the component
Actuation Signal Wires	No throughput signal	• Structural Damage	No signal is sent to the actuators	I	E	Predictive wire maintenance
E-M motor	No conversion from signal to clamping force	• Stuck rotor	No braking force generated	I	D	Predictive maintenance of the motor

FMEA (Transmission of braking signal - BBW Operating)

Operating condition: Transmission of braking signal

Component	Failure mode	Failure causes	Failure effects	Seve-rity	Proba-bility	Control Measures
Pump	No conversion from signal to hydraulic pressure	• Stuck rotor • Fluid leakage	No transmission of braking pressure to calipers	I	D	Predictive maintenance of the pump

Operating condition: BBW operating

Component	Failure mode	Failure causes	Failure effects	Seve-rity	Proba-bility	Control Measures
Power supply	Power outage	• Discharged battery • Overheated battery	No output current	I	D	Purely hydraulic backup system Emergency battery
Brake pedal	Pedal is suddenly insensitive to the foot pressure	• The spring linking it to the pedalboard breaks	Braking signal is suddenly very high	III	E	Choice of a more durable spring

FMEA (BBW Operating)

Component	Failure mode	Failure causes	Failure effects	Seve-rity	Proba-bility	Control Measures
Rear BCU	Stops elaborating signals	• BCU software failure	Braking signal is interrupted	I	D	Software update with more robust versions; Periodically test the BCU
	Wrong elaboration of signals	• BCU software failure	Wrong braking signal transmitted	I	D	Software update with more robust versions; Periodically test the BCU
Front BCU	Stops elaborating signals	• BCU software failure	Braking signal is interrupted	I	D	Software update with more robust versions; Periodically test the BCU
	Wrong elaboration of signals	• BCU software failure	Wrong braking signal transmitted	I	D	Software update with more robust versions; Periodically test the BCU

FMEA (BBW Operating)

Component	Failure mode	Failure causes	Failure effects	Seve-rity	Proba-bility	Control Measures
Pedal sensor	Stops measuring properly	• Structural damage	Braking signal is suddenly interrupted or not accurate	I	E	Use a more robust sensor
Pump	Pump breakdown	• Cavitation • Corrosion • Wear	No pressure in hydraulic circuit	I	D	Predictive maintenance; Lubrication
Circuit pressure sensor	Wrong measurement	• Bad calibration	Wrong pressure in hydraulic circuit	II	E	Compare data from pump with sensor output and detects anomalies
E-M motor	Rotor stuck	• Electrical windings damage	No braking torque is generated	I	E	Predictive maintenance

FMEA (Release of braking)

Component	Failure mode	Failure causes	Failure effects	Seve-rity	Proba-bility	Control Measures
Brake pedal	Stuck braking	• Mechanical failure • Physical obstruction	Braking signal is not interrupted	III	D	Predictive maintenance; Visual Inspection
Pedal sensor	Wrong measurement	• Bad calibration	Braking signal is not interrupted	III	E	Use a high quality sensor; Add an auxiliary sensor
Rear BCU	Wrong computation of torques	• BCU software failure	Braking signal is not interrupted	III	D	Software update with more robust versions; Periodically test the BCU
Front BCU	Wrong computation of torques	• BCU software failure	Braking signal is not interrupted	III	D	Software update with more robust versions; Periodically test the BCU
Front calipers	Stuck clamping	• Mechanical failure	Braking torque is not interrupted	III	E	Proper design of the calipers; Predictive maintenance

FMEA (Release of braking - BBW not operating)

Operating condition: Release of braking

Component	Failure mode	Failure causes	Failure effects	Severity	Probability	Control Measures
Rear calipers	Stuck clamping	• Mechanical failure	Braking torque is not interrupted	III	E	Proper design of the calipers; Predictive maintenance

Operating condition: BBW not operating

Component	Failure mode	Failure causes	Failure effects	Severity	Probability	Control Measures
Pedal sensor	Detects non-real pressure on pedal	• Bad calibration	Braking signal is suddenly generated	II	E	Use a high quality sensor; Add auxiliary sensors
Front BCU	BCU requires torque without command	• BCU software failure	Braking torque is suddenly required	II	D	Software update with more robust versions; Periodically test the BCU
Rear BCU	BCU requires torque without command	• BCU software failure	Braking torque is suddenly required	II	D	Software update with more robust versions; Periodically test the BCU

FTA - hypotheses

In the following trees, we proposed three additional safety functions and we considered their implementation together with the one already provided by Brembo, i.e. the purely hydraulic (and purely front) braking system:

- Auxiliary pedal sensors: redundancy on pedal sensor, to decrease hazards probability related to its malfunctioning;
- Emergency battery: an independent battery that works only if the main one is discharged, capable to power the system even just for one braking, with which the car must stop until the main battery is recharged;
- Additive Control Unit (ACU): very simple and robust control unit getting data from pedal sensor, BCU’s output signals and wheels speeds to evaluate the correct functioning of the BCU’s and of the actuation blocks.

FTA - hypotheses

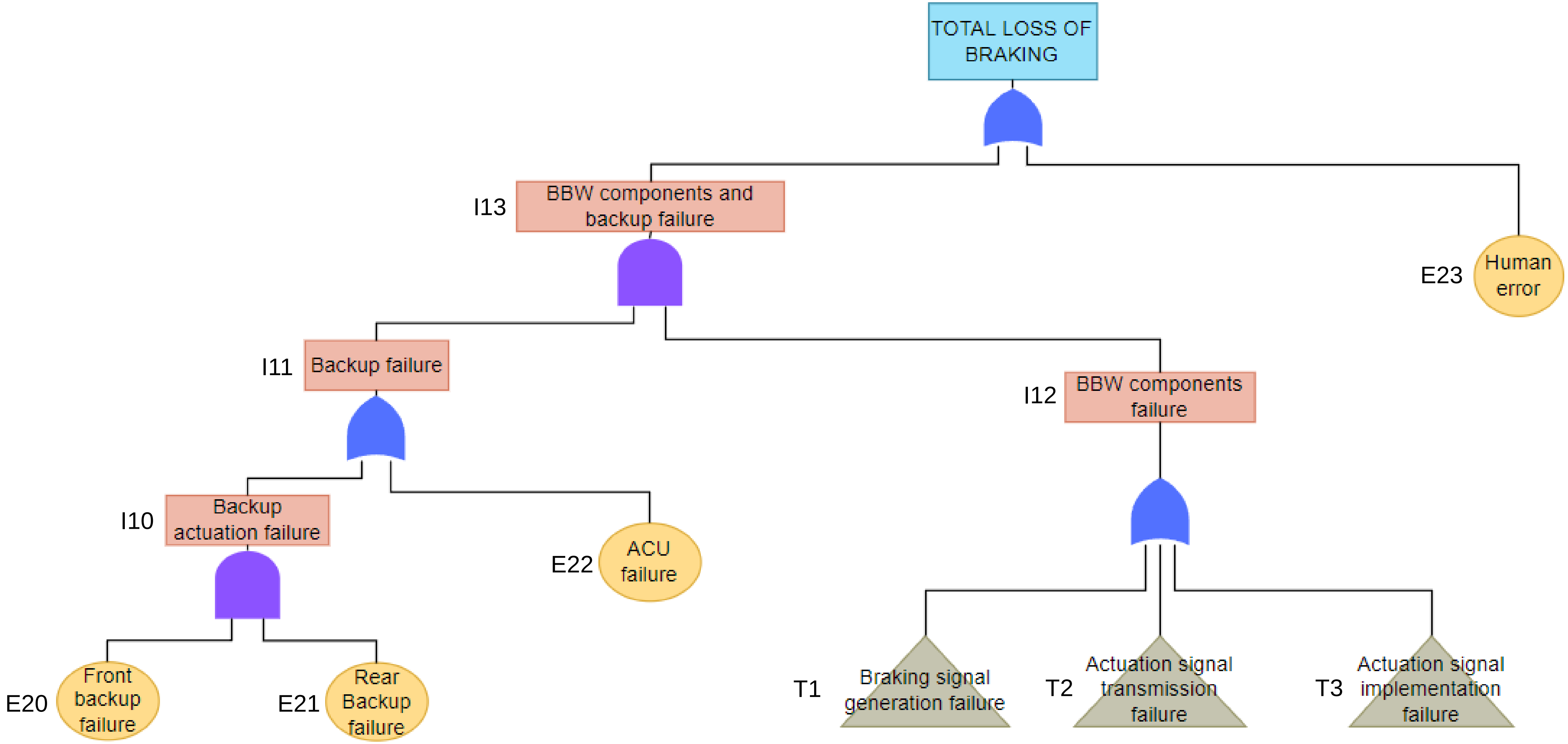
In particular, the ACU should accomplish this tasks:

- compare the received data to detect large errors;
- send an alarm to the driver, warning him to stop and ask for assistance
- activate the standard backup system, or the rear brakes (if the detected error is located in the front hydraulic actuators).

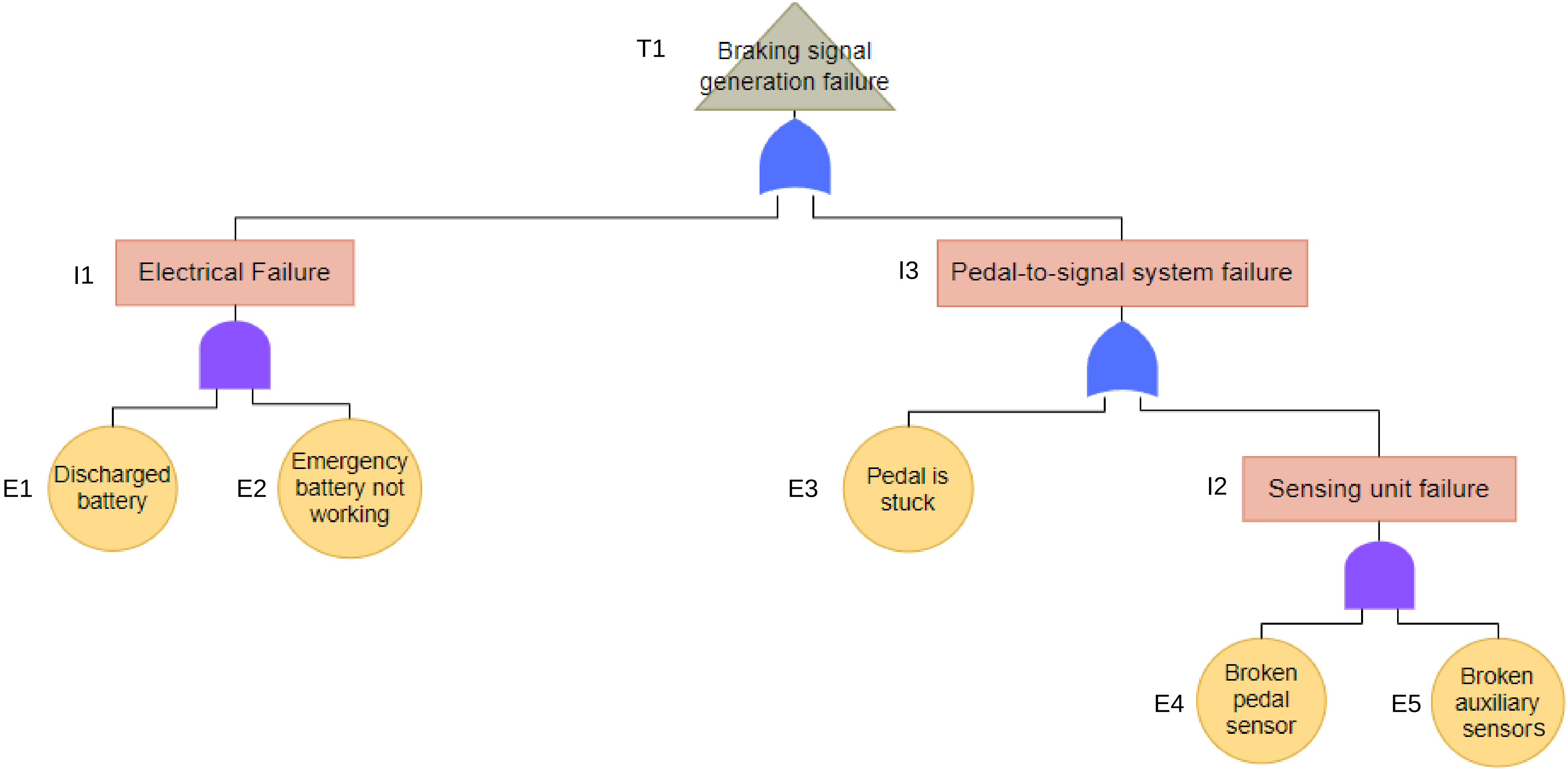
This last detail is important, since the backup system acts on the same hydraulic circuit as the standard front brakes, so it cannot work if those brakes are damaged. Then, rear brakes must be activated.

The ACU should detect only large errors, to have simple software and hardware (so that it is more robust and cheap).

FTA

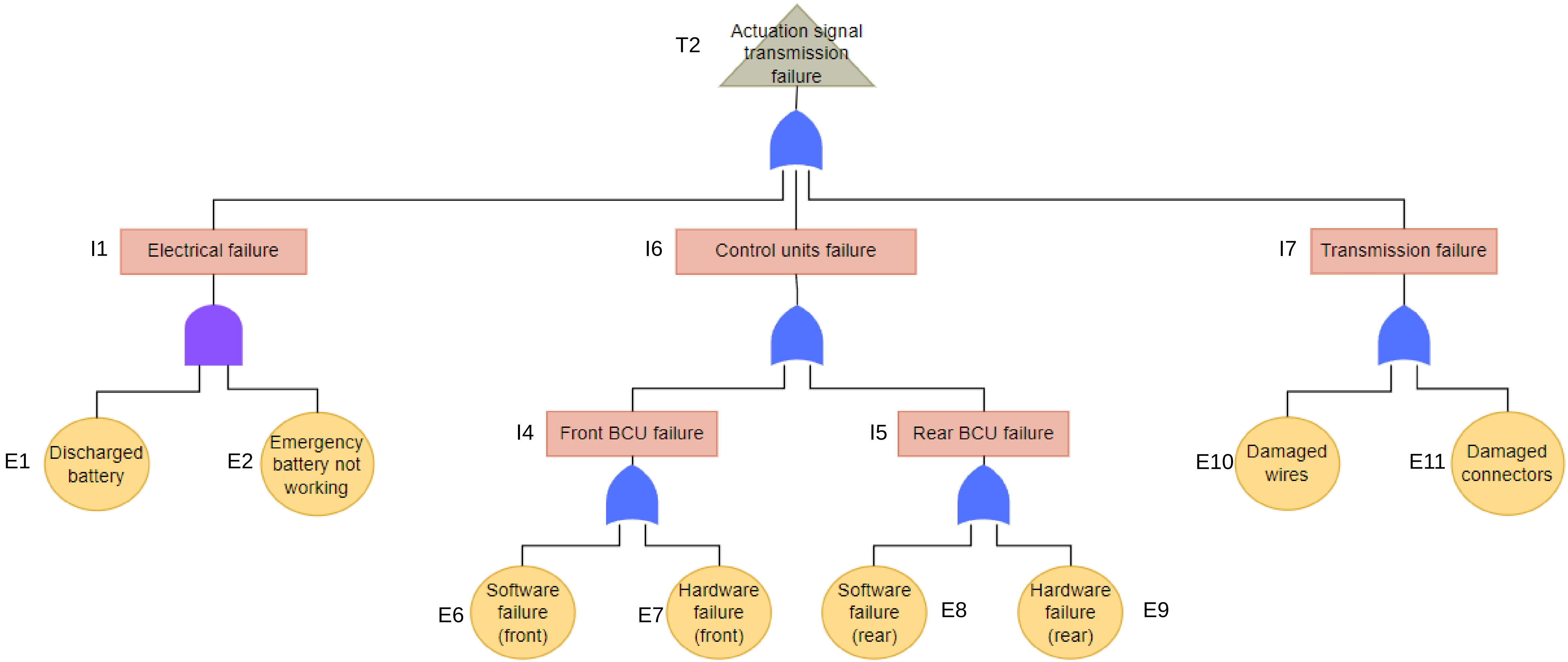

TOTAL LOSS OF BRAKING
I13
BBW components and backup failure
E23
Human error
I11
Backup failure
I12
BBW components failure
I10
Backup actuation failure
E22
ACU failure
E20
Front backup failure
E21
Rear Backup failure
T1
Braking signal generation failure
T2
Actuation signal transmission failure
T3
Actuation signal implementation failure

FTA

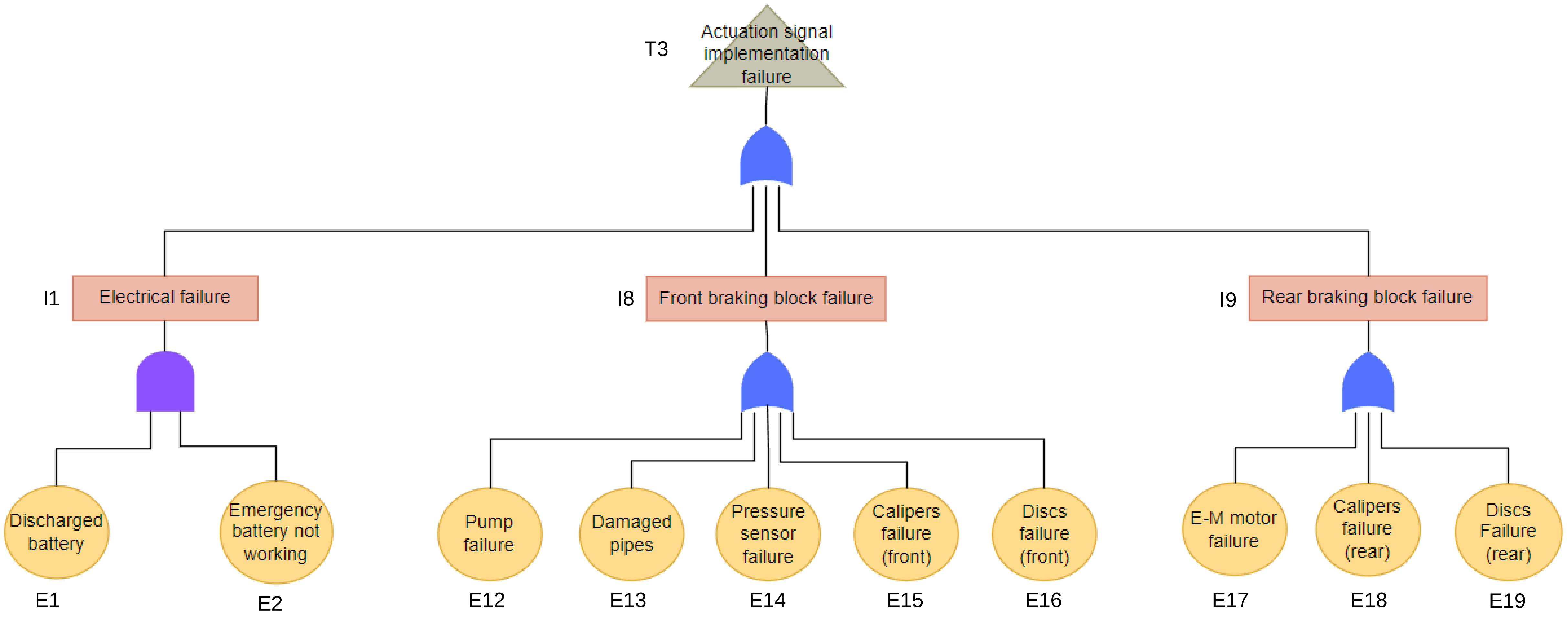


T1
Braking signal generation failure
I1
Electrical Failure
I3
Pedal-to-signal system failure
E1
Discharged battery
E2
Emergency battery not working
E3
Pedal is stuck
I2
Sensing unit failure
E4
Broken pedal sensor
E5
Broken auxiliary sensors

FTA


T2
Actuation signal transmission failure
I1
Electrical failure
I6
Control units failure
I7
Transmission failure
E1
Discharged battery
E2
Emergency battery not working
I4
Front BCU failure
I5
Rear BCU failure
E10
Damaged wires
E11
Damaged connectors
E6
Software failure (front)
E7
Hardware failure (front)
Software failure (rear)
E8
Hardware failure (rear)
E9

FTA



T3
Actuation signal implementation failure
I1
Electrical failure
I8
Front braking block failure
I9
Rear braking block failure
Discharged battery
E1
Emergency battery not working
E2
Pump failure
E12
Damaged pipes
E13
Pressure sensor failure
E14
Calipers failure (front)
E15
Discs failure (front)
E16
E-M motor failure
E17
Calipers failure (rear)
E18
Discs Failure (rear)
E19

FTA - Probability of top event

Event	E1	E2	E3	E4	E5	E6	E7	E8	E9
Probability	0.000005	0.000025	0.000025	0.000005	0.0000025	0.00004	0.00002	0.00004	0.00002

E10	E11	E12	E13	E14	E15	E16	E17	E18	E19
0.000025	0.000005	0.000005	0.0000025	0.0000025	0.0000005	0.0000005	0.0000025	0.0000005	0.0000005

E20	E21	E22	E23	I1	I2	I3	I4	I5	I6
0.000005	0.000004	0.000004	0.001	1.25 e-10	1.25 e-11	0.000025	5.99992 e-5	5.99992 e-5	1.19995 e-4

I7	I8	I9	I10	I11	I12	I13	T1	T2	T3
2.99999 e-5	0.000011	0.0000035	2 e-11	0.000004	1.8949 e-4	7.5976 e-10	0.000025	1.49994 e-4	0.0000145

Probability of the top event: 0.001

Conclusions

As FMEA shows, a key element is the robustness of the BCU’s software, for which constant updates should be performed, in order to avoid fatal errors due to the computation of braking torques.

Looking at the results of the analysis, and in particular considering the single safety function specified by Brembo, some improvements could be applied.

The fault trees highlight that some additional redundancies would decrease the probability of the total loss of braking.

Another notable fact is that the alternative hydraulic braking system provided by Brembo is only acting on front wheels and still relying on the front actuators, that would bring to possible hazards if those actuators are faulty.

The proposed additional safety functions are simple solutions that could be effective in the improvement of the system safety.

References

Brembo developed a tool to show interactively the BBW system:

BBW System by Brembo

For some data relating to probabilities and most common failures, we read:

"The reliability of electronically controlled systems on vehicles" by Knight, Eaton & Whitehead