System Hazard Analysis of an Adaptive Cruise Control system

AY 2024-2025

Mohebban Joshua (10683856)

Pantella Edoardo (10964011)

HANDS-FREE
DRIVING SYSTEM
FORD BLUE CRUISE

OUTLINE

1. Introduction
2. Preliminary Hazard Analysis
3. Failure Mode and Effective Analysis
4. Fault Tree Analysis
5. Event Tree Analysis

1. INTRODUCTION

Adaptive Cruise Control System Description

In the following safety analysis we will mainly focus on the linear adaptive cruise control subsystem.

Adaptive Cruise Control (ACC) is a level 1 autonomous driving system (according to the SAE definitions) designed to automatically adjust the vehicle's longitudinal dynamics, in order to maintain a safe distance from the car ahead. As per definition, the driver is required to manage the car's lateral dynamics and monitor the driving at all times and is thus legally held accountable for the car's behaviour.

This system operates seamlessly alongside traditional safety systems such as Anti-lock Braking Systems (ABS) and Traction Control (TC), integrating them into its functionalities.

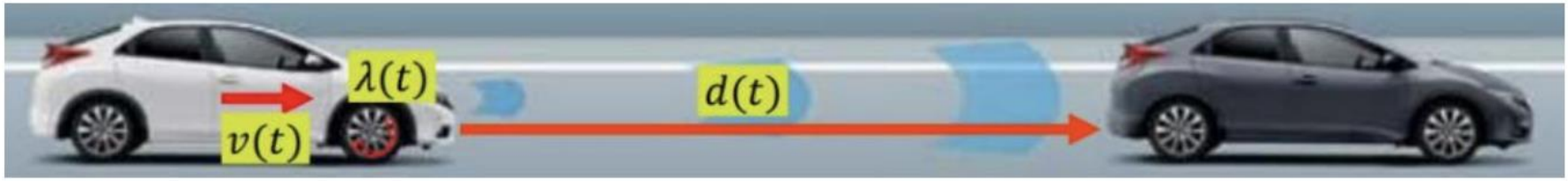
The functionality of ACC relies on various sensors, including radar and camera systems to detect and monitor the surrounding environment. Radar sensors are primarily used to measure the distance to vehicles ahead, while cameras can identify lane markings and traffic signs. Additionally, wheel speed sensors, throttle position sensors and others work together to ensure precise control over braking, stability, and acceleration. ACC also relies on some actuators in order to act upon the vehicle's dynamics, in particular it acts upon the engine's torque through 2 by wire control loops (with electric motors) in order to modify the engine's throttle position and spark timing. Instead, to control the braking torque, it utilizes the build and dump valves of the brake (hypothesis of traditional ABS).

Adaptive Cruise Control System Description

Let's quickly schematize how ACC actually works, from a technical description point of view.

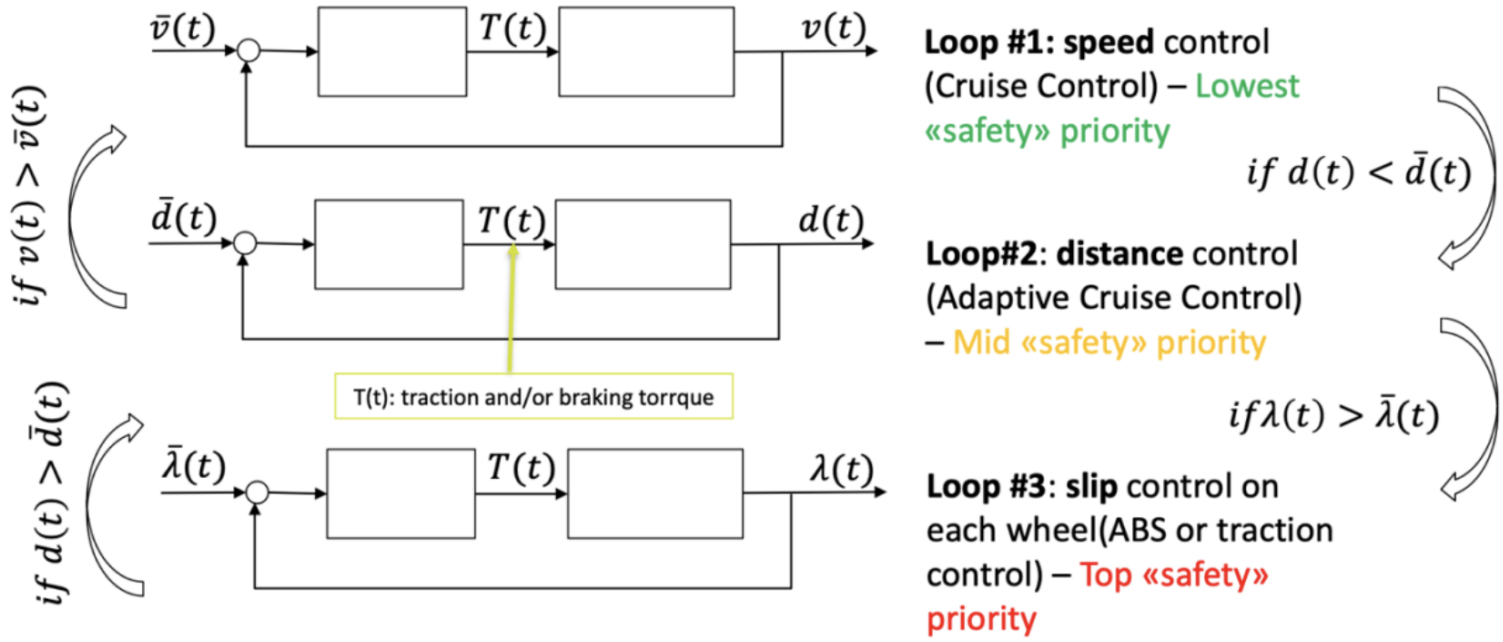
It is made of **three layers of control** that switch to one another when needed:

1. **Velocity control loop** (Cruise Control): it has the lowest safety priority.
2. **Distance control loop** (Adaptive Cruise Control): medium safety priority.
3. **Slip control loop** (ABS or TC): top safety priority.



The white car is called the "ego" vehicle where we have our ACC system, while the grey car is called the "leader vehicle" and represents the obstacle. The three main control variables are the ego vehicle's longitudinal speed $v(t)$, the wheel slip $\lambda(t)$ and the relative distance $d(t)$.

Adaptive Cruise Control System Description



In all three control loops the actuation variable is the **torque at the wheel,** which can be positive in acceleration or negative in braking. We are in the hypothesis of an Internal Combustion Engine (ICE) car with traditional brakes and ABS. In the following we will assume that the positive torque is entirely generated by the ICE while the negative torque is entirely generated by the brakes.

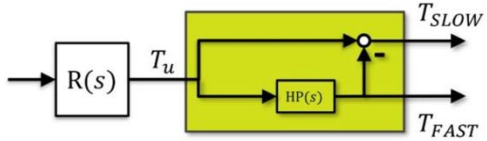
Adaptive Cruise Control System Description

In order to generate the engine's torque we can act on two control variables:

- the **spark timing:** it has an immediate impact on the torque at the cost of a higher environmental impact, because it lowers the engine's energy efficiency.
- the **throttle position:** it has a slower action on the torque but is a cleaner control variable.

Usually a combination of these two control variables is utilized in order to satisfy the torque request through means of an input allocator, in fact the rapid fluctuations of the requested torque are satisfied using the spark timing, while the low frequency content of the request is satisfied using the throttle position. The values of the «spark timing» and of the «throttle position» variables are themselves realized through nested electrically actuated control loops, in fact if we analyze deeply the physical implementation of these two control loops we can see that the torque generation in an engine is realized by a computing unit (**ECU**) to which many components are connected, in particular:

- for the throttle position, a **DC brushless** motor actuates the butterfly valves of the engine, the ECU pilots the DC brushless by taking into account the feedback of many sensors.
- for the spark timing, the ECU drives the **ignition coils** electrically, the correct timing for their sparking is calculated once again thanks to the information brought by many sensors.



Adaptive Cruise Control System Description

In order to further analyze the safety level of ACC we will now make some simplifying assumptions:

- the ECU is an ideal component and thus cannot break, moreover the sub control laws for both the throttle position and spark timing will be considered perfectly tuned.
- the butterfly valves and throttle position sensors are ideal components and thus cannot break.
- the spark timing sensors are ideal components and thus cannot break.
- the ignition coils of the engine will be considered as one single component, meaning that they can either all be functioning or all be malfunctioning.

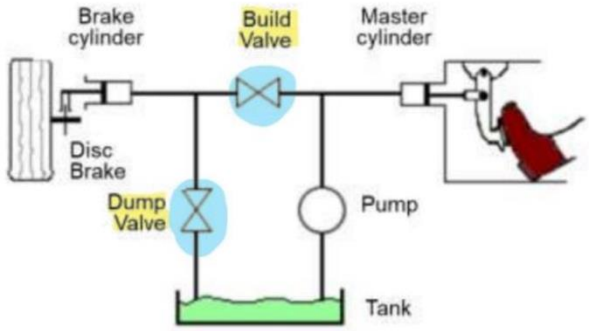
With these hypothesis we will be able to analyze the potential hazards and failures of the system considering the spark timing and throttle position as two decoupled actuators for the ACC system.

In order to generate the braking torque we can act on two on-off switching valves:

- the **build valve**
- the **dump valve**

We have three control actions:

- **Open the build and close the dump**: increase the hydraulic pressure.
- **Close the build and open the dump**: decrease the hydraulic pressure.
- **Close both the build and the dump**: hold the hydraulic pressure.

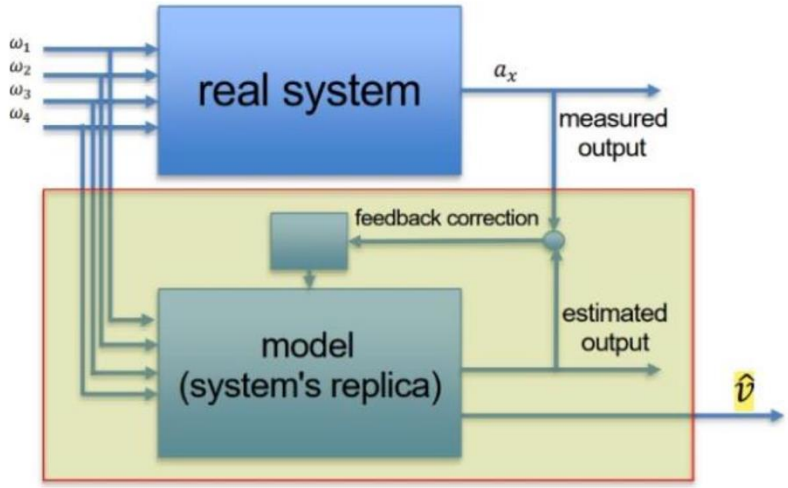


Adaptive Cruise Control System Description

TC, velocity loop and distance loop utilize a PID regulator to realize the engine's torque while ABS, velocity loop and distance loop utilize an hysteresis controller to directly act upon the brake valves.

$d(t)$ is measured with a radar, $v(t)$ and $\lambda(t)$ need to be estimated using a **Kalman filter**.

KF is a model-based software-sensing technique which works in feedback. The idea consists in making a virtual system's replica and to feed it with the same input as the original system. A feedback correction on the measured output (longitudinal acceleration) is used to tune the virtual system's parameters, the closer the error is to 0 the closer is the filter's state to the real system's state.



Adaptive Cruise Control System Description

ACC sensors:

- **1x Radar sensor:** measures the leader car's relative distance and longitudinal speed.
- **4x Wheel encoders:** one for each wheel, needed to measure the angular velocities.
- **1x Longitudinal accelerometer:** needed to improve Kalman estimations.

We have decided to consider all four encoders already present in the system instead of considering the presence of only one single encoder and then showing the need to add three more encoders, one for each wheel, in order to achieve redundancy. This is done because we feel that the presence of four encoders is needed in order to have a more accurate estimation and isn't only employed for safety reasons.

ACC actuators:

- **Spark timing (Ignition coils)**
- **Throttle position (DC brushless)**
- **Build valve**
- **Dump valve**

We will consider a **single centralized computer** on which all the required software runs and a **single power supply unit**.

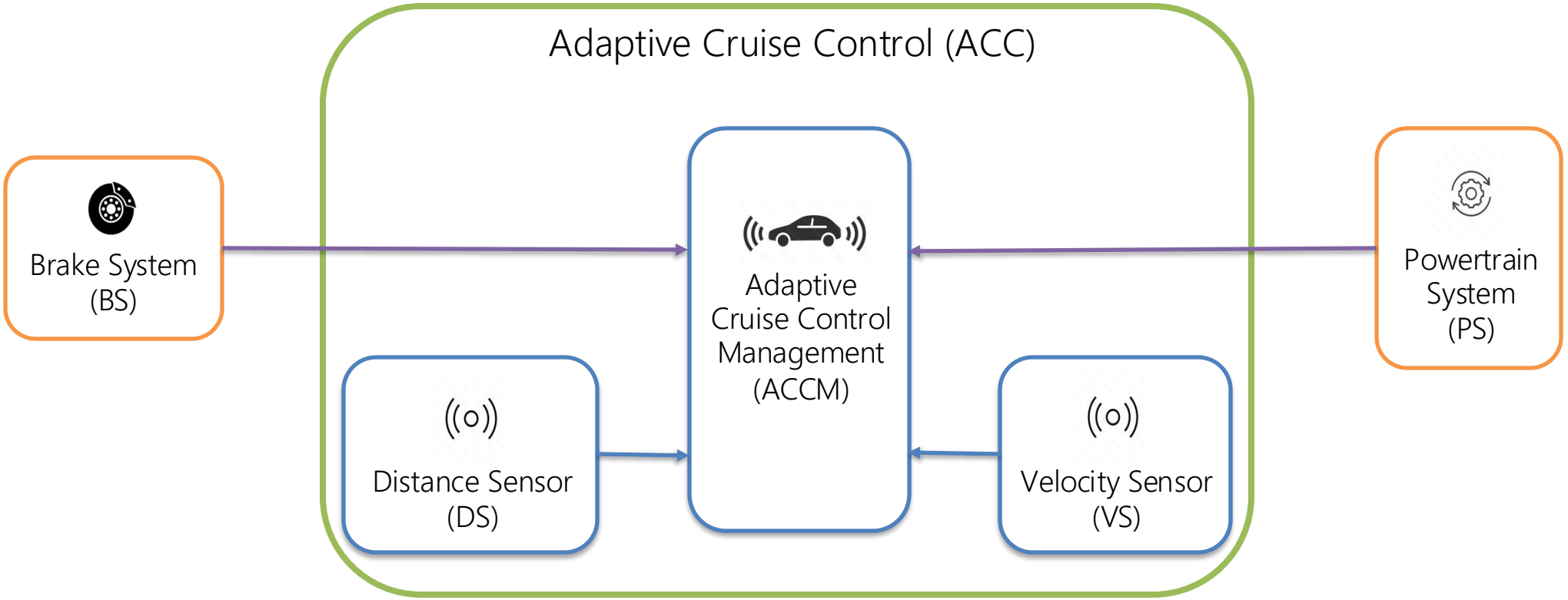
ACC - Hypothesis

For ease of reading we summarize all the hypothesis made, which will be mantained throughout the entire project:

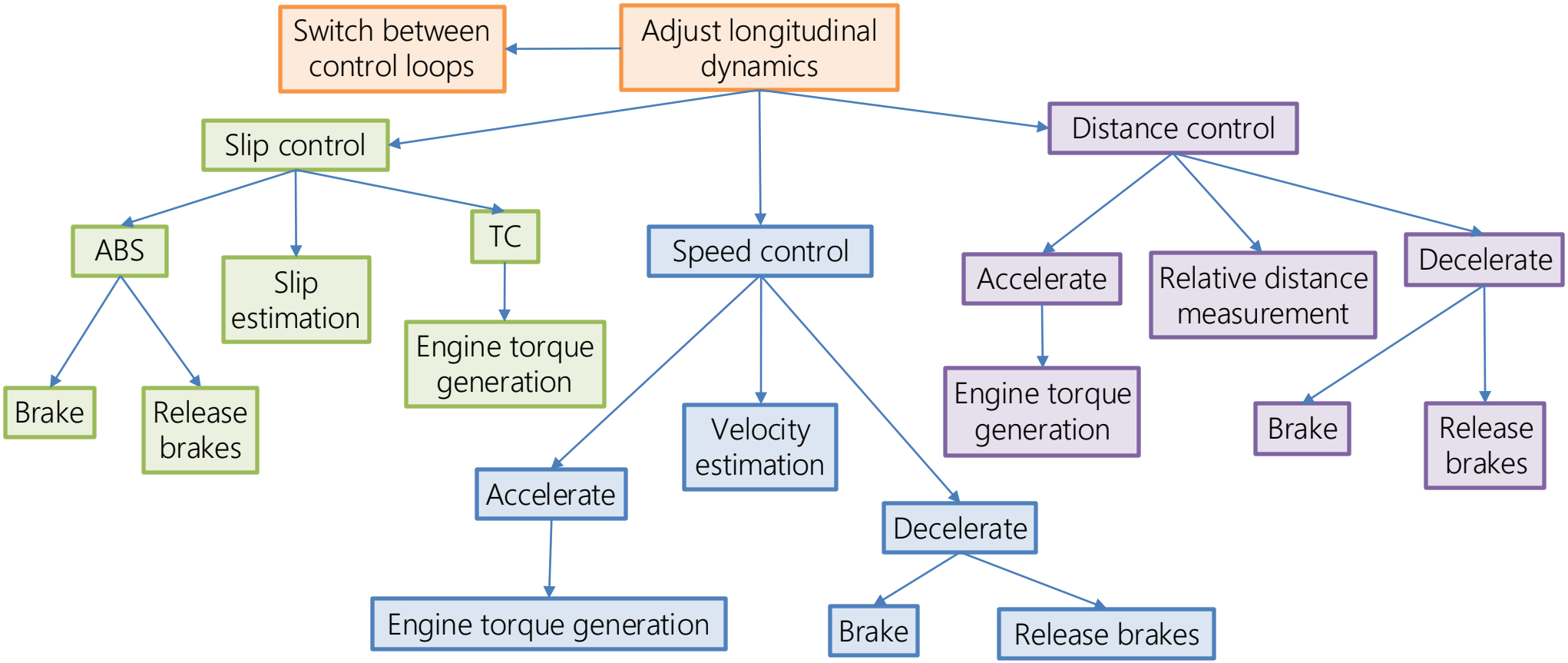
- Traditional brakes and ABS.
- ICE engine.
- Positive torque entirely generated by the engine, negative torque entirely generated by the brakes.
- ECU is an ideal component.
- Sub control laws for throttle position and spark timing are perfectly tuned.
- Butterfly valves of the engine are ideal components.
- Spark timing and throttle position sensors are ideal components.
- Ignition coils are considered as one single component.
- Throttle position and spark timing are decoupled actuators.
- 4 encoders are already present in the system for better precision in estimation.
- If slip estimation works then both ABS and TC are correctly working, we don't consider the presence of a braking torque sensor and of a braking pedal pressure sensor.
- Centralized computer.
- Single power supply.

Functional Analysis

Let's start with a general outline to understand the main parts of the system.

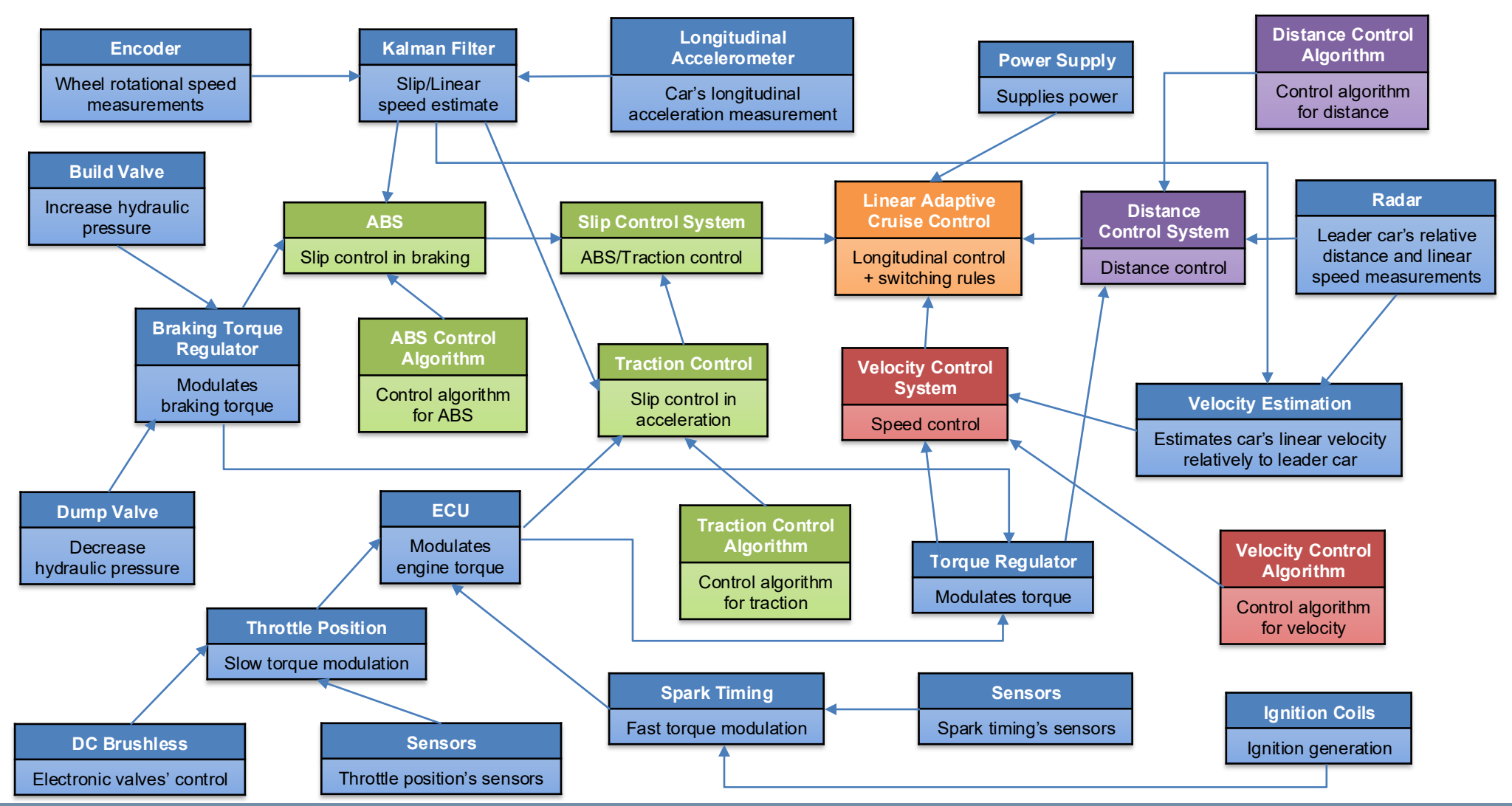


Functional Analysis: scheme



Remark: regarding the slip control, we focus on the slip estimation and we assume that if we are able to correctly estimate it, the ABS and TC subsystems work properly.

Architectural Analysis: scheme



Operating conditions I

OPERATING MODES	DESCRIPTION	INVOLVED SUBSYSTEMS
Velocity Control	ACC switches to velocity control whenever $v(t) > \bar{v}$ and $d(t) > \bar{d}$ hold true. In this mode a kalman filter estimates the car's linear speed using the four wheels encoders and the longitudinal acceleration sensor. The radar outputs the leader car's linear velocity. A PID/hysteresis controller is typically used to track the estimated $v(t)$ to $\bar{v}$. The actuation variable is the torque.	• Power supply • Velocity control algorithm • Kalman filter • Radar • Encoders (4) • Longitudinal acceleration sensor • Build valve • Dump valve • DC brushless (Throttle position) • Ignition Coils (Spark timing)
Distance Control	ACC switches to distance control whenever it holds true that: $d(t) < \bar{d}$ and $\lambda(y) < \bar{\lambda}$ or $d(t) > \bar{d}$ and $v(t) < \bar{v}$. The radar measures the distance from the leader vehicle. A PID/hysteresis controller is usually used to track $d(t)$ to $\bar{d}$. The actuation variable is the torque.	• Power supply • Distance control algorithm • Radar • Build valve • Dump valve • DC brushless (Throttle position) • Ignition Coils (Spark timing)

Operating conditions II

OPERATING MODES	DESCRIPTION	INVOLVED SUBSYSTEMS
Slip Control: ABS	ACC switches to slip control with ABS when $\lambda(y) > \bar{\lambda}$ holds true. A kalman filter estimates the slip value using the four wheels encoders and longitudinal acceleration sensor. For traditional ABS a hysteresis cycle control algorithm is used to keep $\lambda(t)$ near $\bar{\lambda}$. The actuation variable is the braking torque.	• Power supply • ABS control algorithm • Kalman filter • Encoders (4) • Longitudinal acceleration sensor • Build valve • Dump valve
Slip Control: Traction Control	ACC switches to slip control with Traction Control when $\lambda(y) > \bar{\lambda}$ holds true. A kalman filter estimates the slip value using the four wheels encoders and longitudinal acceleration sensor. A PID controller is usually used to track $\lambda(t)$ to $\bar{\lambda}$. The actuation variable is the engine's torque.	• Power supply • Traction control algorithm • Kalman filter • Encoders (4) • Longitudinal acceleration sensor • DC brushless (Throttle position) • Ignition Coils (Spark timing)

2. PRELIMINARY HAZARD ANALYSIS

Assumptions and observations

Assumptions of the case study:

- The vehicle is traveling on a straight highway with a car in front in broad daylight, at a speed of about $100\ km/h$
- There is a single centralized computer that manages the software and a single power supply system
- Analysis of risks and countermeasures is done by trying to maximize system uptime, avoiding shutting down the system whenever possible
- Since the system has a primary safety role in vehicles, it would be already provided with many redundant devices (parallel actuators, parallel wires and sensors and parallel power units), in order to simplify the case study their presence is omitted and the necessity to introduce them as countermeasures is instead shown in the following analysis.
- In order to calculate the risks associated to each hazard the MTBF of some components has been considered, in order to assess the probability of their failure, in particular:
    - Encoder (rotative) MTBF = 100.000 hours
    - Accelerometer (IMU) MTBF = 200.000 hours
    - Radar (LRR) MTBF = 150.000 hours
    - Dump and Build valves (hydraulic valves) MTBF = 10.000 hours
    - For Spark Timing we consider the ignition coils MTBF = 50.000 hours
    - For Throttle Position we consider the DC brushless MTBF = 50.000 hours

Hazard description I

Operating modes	Sources	Phenomena	Effects
Velocity control Slip control	Sensors' problem: 3 or 4 encoders failures	Impossible to estimate or wrong estimation of velocity and slip. Kalman Filter does not work.	• Velocity and slip loops do not work • Driver injuries • People injuries • Collision • Car damage
Velocity control Slip control	Sensors' problem: 2 encoders and 1 accelerometer failures	Impossible to estimate or wrong estimation of velocity and slip. Kalman Filter does not work.	• Velocity and slip loops do not work • Driver injuries • People injuries • Collision • Car damage
Distance control	Sensor's problem: radar failure	Unable to detect the relative distance	• Driver injuries • Distance loop does not work • People injuries • Collision • Car damage
Velocity control Distance control Traction control	Actuators' problem: Ignition coils failure	Unable to generate the torque, total engine failure	• Driver injuries • Loss of vehicle's control • People injuries • Collision • Car damage

Hazard description II

Operating modes	Sources	Phenomena	Effects
Velocity control Distance control Traction control	Actuator's problem: throttle position DC brushless failure	Unable to drive the butterfly valves, total engine failure	• Driver injuries • Loss of vehicle's control • People injuries • Collision • Car damage
Velocity control Distance control ABS control	Actuator's problem: dump valve failure, stuck open	Unable to provide sufficient braking pressure	• Impossible to slow down the vehicle in critical situations • Driver injuries • People injuries • Collision • Car damage
Velocity control Distance control ABS control	Actuator's problem: dump valve failure, stuck closed	Unable to release the brakes	• Loss of vehicle's control • Driver injuries • People injuries • Collision • Car damage
Velocity control Distance control ABS control	Actuator's problem: build valve failure, stuck open	Unable to release the brakes	• Loss of vehicle's control • Driver injuries • People injuries • Collision • Car damage

Hazard description III

Operating modes	Sources	Phenomena	Effects
Velocity control Distance control ABS control	Actuator's problem: build valve failure, stuck closed	Unable to provide sufficient braking pressure	• Impossible to slow down the vehicle in critical situations • Driver injuries • People injuries • Collision • Car damage
Velocity control Distance control ABS control	Actuators' problem: build valve failure AND dump valve failure	Complete loss of braking functionality	• ACC complete loss of functionality • Loss of vehicle's control • Driver injuries • People injuries • Collision • Car damage
Velocity control Distance control Slip control	Power supply failure	Unable to supply and/or damage to the centralized computer and other components	• ACC complete loss of functionality • Driver injuries • People injuries • Collision • Car damage

Targets I

Target	People
SEVERITY OF CONSEQUENCES	
CATASTROPHIC	High-speed collision causing severe injuries or fatalities to passengers or road users.
CRITICAL	Low-speed collision or loss of vehicle control resulting in moderate injuries.
MARGINAL	Anomalous vehicle behavior without physical consequences.
NEGLIGIBLE	Minor discomfort for passengers

Targets II

Target	Vehicle
SEVERITY OF CONSEQUENCES	
CATASTROPHIC	Major structural damage rendering the vehicle unusable.
CRITICAL	Significant damage requiring costly repairs (e.g., airbag deployment, brake system damage).
MARGINAL	Minor damage to external parts or mechanical components.
NEGLIGIBLE	No damage or cosmetic issues (e.g., scratches or dents).

Targets III

Target	Environment
SEVERITY OF CONSEQUENCES	
CATASTROPHIC	Significant destruction of road infrastructure or environmental damage (e.g., loss of control in sensitive areas).
CRITICAL	Moderate damage to infrastructure (e.g., collision with barriers or signage) or localized environmental harm (e.g., minor fuel or fluid leaks).
MARGINAL	Minor damage to infrastructure (e.g., scratches on protective barriers) or negligible environmental impact (e.g., short-term air or noise pollution).
NEGLIGIBLE	No significant damage to the environment or infrastructure.

Risk assessment matrix

Target: **People**

SEVERITY OF CONSEQUENCES	PROBABILITY OF MISHAP(EXPOSURE)				
	E - IMPROBABLE	D - REMOTE	C - OCCASIONAL	B - PROBABLE	A - FREQUENT
I - CATASTROPHIC	3	3	3	3	3
II - CRITICAL	2	2	3	3	3
III – MARGINAL	1	1	1	2	2
IV – NEGLIGIBLE	1	1	1	1	2

Target: **Vehicle**

SEVERITY OF CONSEQUENCES	PROBABILITY OF MISHAP(EXPOSURE)				
	E - IMPROBABLE	D - REMOTE	C - OCCASIONAL	B - PROBABLE	A - FREQUENT
I - CATASTROPHIC	3	3	3	3	3
II - CRITICAL	2	2	2	3	3
III – MARGINAL	1	1	1	2	2
IV – NEGLIGIBLE	1	1	1	1	1

Target: **Environment**

SEVERITY OF CONSEQUENCES	PROBABILITY OF MISHAP(EXPOSURE)				
	E - IMPROBABLE	D - REMOTE	C - OCCASIONAL	B - PROBABLE	A - FREQUENT
I - CATASTROPHIC	3	3	3	3	3
II - CRITICAL	2	2	2	3	3
III – MARGINAL	1	1	1	2	2
IV – NEGLIGIBLE	1	1	1	1	1

PHA I

HAZARD	RISK BEFORE				COUNTERMEASURES	RISK AFTER		
	TARGET	SEVERITY	PROBABILITY	RISK CODE		SEVERITY	PROBABILITY	RISK CODE
Kalman Filter does not work (due to 3+ encoders failure)	P	II	E	2	Disable ACC. Implement a sensor health monitoring system to detect encoders degradation early. Implement alternative sensors like GPS to provide temporary velocity measurements in case of critical failure. In case of critical failure, an alarm notifies the driver who must resume manual driving.	II	E	2
	V	II	E	2		II	E	2
	E	II	E	2		II	E	2
Kalman Filter does not work (due to 2+ encoders and accelerometer failure)	P	II	E	2	Add a backup accelerometer. Implement a diagnostic system to track the accelerometer's health status. In case of critical failure, an alarm notifies the driver and the ACC is disengaged, allowing manual vehicle control.	II	E	2
	V	II	E	2		II	E	2
	E	II	E	2		II	E	2
Failure of the Ignition Coils	P	I	C	3	Switch to ABS control loop to safely brake the car to a halt. Promptly notify the driver of the critical failure with a sound and visual alert. Introduce a real time diagnostic system to track the ignition coils health status. Perform periodic/predictive maintenance.	I	D	3
	V	I	C	3		I	D	3
	E	II	C	2		II	D	2
Failure of the DC brushless (Throttle position)	P	I	C	3	Add a secondary DC brushless motor for actuator redundancy. Insert a mechanical bypass which lets the driver directly control the butterfly valves. Introduce a "fail safe" mode in which the butterfly valves are always slighty open in order to have a low power but functioning engine. Promptly notify the driver of the critical failure with a sound and visual alert. Perform periodic/predictive maintenance.	I	E	3
	V	I	C	3		I	E	3
	E	II	C	2		II	E	2

PHA II

HAZARD	RISK BEFORE				COUNTERMEASURES	RISK AFTER		
	TARGET	SEVERITY	PROBABILITY	RISK CODE		SEVERITY	PROBABILITY	RISK CODE
Unable to detect the relative distance	P	III	D	1	Radar performance is sensitive to environmental conditions. Sensor Fusion, integrating radar with cameras or Lidar, improves reliability and redundancy. Adaptive calibration algorithms can adjust for environmental factors. Add a monitoring system to track sensors' health. Alert the driver in case of critical failure.	III	E	1
	V	III	D	1		III	E	1
	E	IV	D	1		IV	E	1
Unable to provide sufficient braking pressure (due to dump valve stuck open)	P	I	C	3	Installing a redundant dump valve ensures pressure can be released during failure. Implement real-time diagnostic systems to detect anomalies early and alert the driver. Perform periodic/predictive maintenance	I	D	3
	V	I	C	3		I	D	3
	E	I	C	3		I	D	3
Unable to provide sufficient braking pressure (due to build valve stuck closed)	P	I	C	3	A backup pressure system or redundant build valve ensures braking functionality during failure. Implement real-time diagnostic systems to detect anomalies early and alert the driver. Perform periodic/predictive maintenance	I	D	3
	V	I	C	3		I	D	3
	E	I	C	3		I	D	3

PHA III

HAZARD	RISK BEFORE				COUNTERMEASURES	RISK AFTER		
	TARGET	SEVERITY	PROBABILITY	RISK CODE		SEVERITY	PROBABILITY	RISK CODE
Unable to release the brakes (due to dump valve stuck closed)	P	II	C	3	Introduce a redundant dump valve to ensure pressure release functionality even during failure. Implement real-time diagnostic systems to detect anomalies early and alert the driver. Perform predictive/periodic maintenance	II	D	2
	V	II	C	2		II	D	2
	E	II	C	2		II	D	2
Unable to release the brakes (due to build valve stuck open)	P	II	C	3	Introduce a redundant dump valve to ensure pressure release functionality even during failure. Implement real-time diagnostic systems to detect anomalies early and alert the driver. Perform predictive/periodic maintenance	II	D	2
	V	II	C	2		II	D	2
	E	II	C	2		II	D	2
Complete loss of braking functionality	P	I	D	3	Install backup braking systems to provide emergency braking functionality in case of total system failure. Implement real-time diagnostic systems to detect anomalies early and alert the driver. Perform predictive/periodic maintenance	I	E	3
	V	I	D	3		I	E	3
	E	I	D	3		I	E	3
Unable to supply and/or damage to the centralized computer and other components	P	II	C	3	Introduce a backup power system to ensure uninterrupted operation of the centralized computer. Implement overcurrent protections. Implement low-power emergency modes to prioritize critical safety functions, maintaining control over essential vehicle operations even during a power supply failure.	II	E	2
	V	II	C	2		II	E	2
	E	II	C	2		II	E	2

PHA - Observations

Notice that some hazards, like the failure of the kalman filter or the inability to provide braking pressure, are repeated multiple times because they can happen for different reasons which require different countermeasures.

Moreover it is not always possibile to appreciate a visible change in the risk level after the countermeasures are introduced. This is for the following reasons:

- probability is discretized and thus it is not possible to see a change of the value inside the same category.
- some subsystems are inherently redundant (see kalman filter for example) and thus the probability for their failure already belongs to the «E» category even before the introduction of countermeasures.
- we set the risk value, of some given severity levels, to 3 for all the probabilities. This is because we feel that some hazards are extremely critical for the safety of the whole system and thus should always be avoided no matter how unlikely they are.

As we said before, we consider the presence of 4 encoders in the system from the beginning, this is because we think that multiple encoders are necessary for quality of estimation reasons and not just for safety reasons. Considering the presence of just one encoder simply would not make any sense for the slip and velocity estimations.

3. FAILURE MODE AND EFFECTIVE ANALYSIS

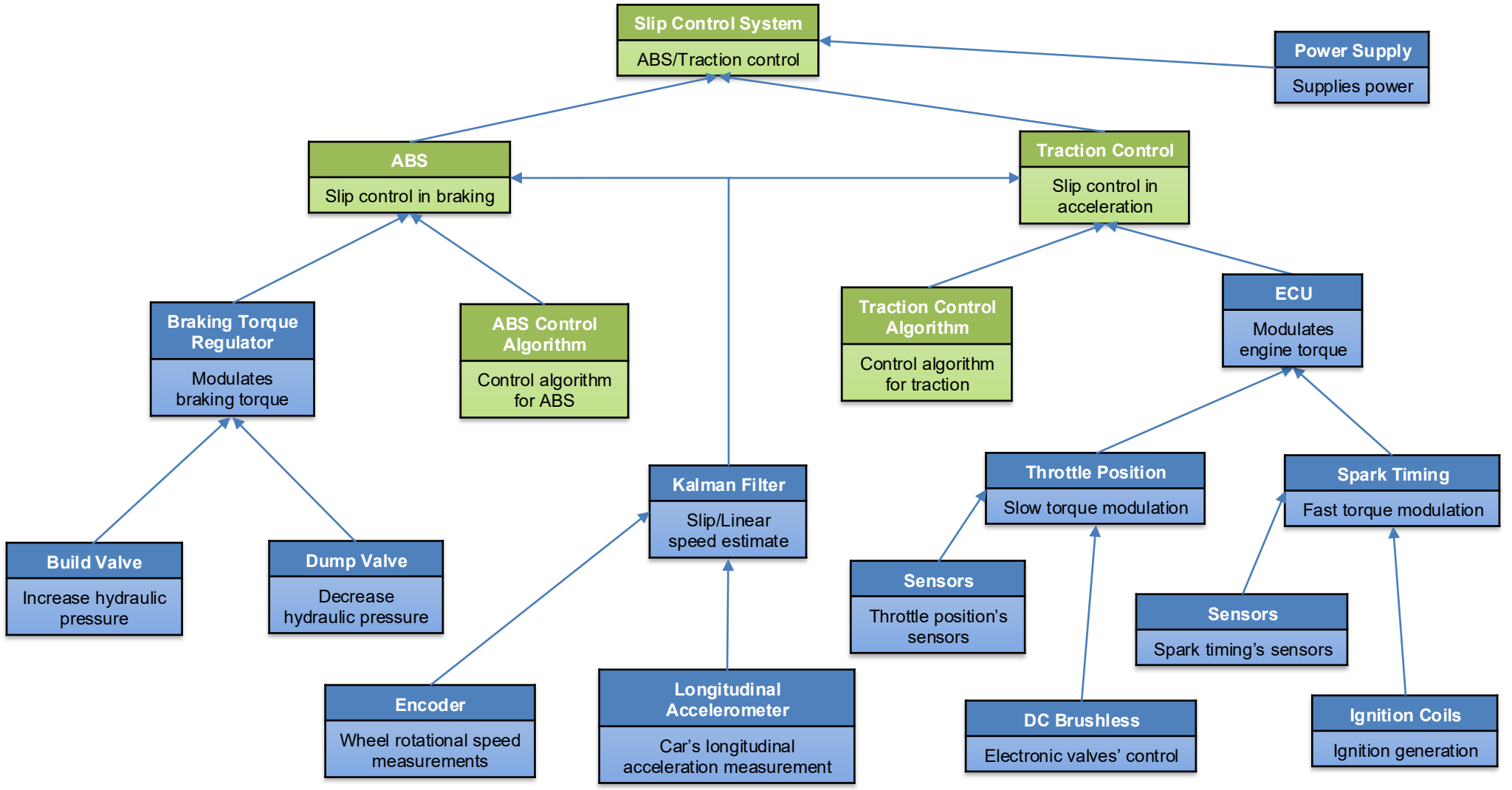
Subsystem and Hypothesis

In the following analysis we will only consider the slip control subsystem because it is the most critical subsystem from a safety point of view. Moreover in order to function it relies on most of the sensors and actuators of the whole ACC system.

In the analysis some assumptions will be made:

- the control algorithms and Kalman Filter are considered perfectly tuned, thus any malfunctioning that would arise in the system is related to single components hardware failures.
- the presence of diagnostic and warning systems like the ones we suggested in pha analysis hasn't been considered but instead we show the need for their presence.
- for the encoder, the effects and subsequent indices have been defined considering the case of 3 or more encoder failures, as the failure of a single encoder would not impact the functionality of the ACC system.
- similarly, for the accelerometer, the scenario of 2 encoder failures combined with an accelerometer failure has been considered.

Subsystem


Slip Control System
ABS/Traction control
Power Supply
Supplies power
ABS
Slip control in braking
Traction Control
Slip control in acceleration
Braking Torque Regulator
Modulates braking torque
ABS Control Algorithm
Control algorithm for ABS
Traction Control Algorithm
Control algorithm for traction
ECU
Modulates engine torque
Kalman Filter
Slip/Linear speed estimate
Throttle Position
Slow torque modulation
Spark Timing
Fast torque modulation
Build Valve
Increase hydraulic pressure
Dump Valve
Decrease hydraulic pressure
Sensors
Throttle position's sensors
Sensors
Spark timing's sensors
Encoder
Wheel rotational speed measurements
Longitudinal Accelerometer
Car's longitudinal acceleration measurement
DC Brushless
Electronic valves' control
Ignition Coils
Ignition generation

Parameters Definition

SEVERITY				
1	2	3	4	5
Inconsequential	Negligible	Marginal	Critical	Catastrophic

PROBABILITY				
1	2	3	4	5
Improbable	Remote	Occasional	Probable	Frequent

DETECTABILITY				
1	2	3	4	5
Always detectable	Easy to detect	Hard to detect	Very hard to detect	Never detectable

Failure Mode and Effect Analysis

Slip Control System I

COMPONENT	FAILURE MODE	CAUSES	EFFECTS	SEV.	PROB.	DETEC.	RPN	RECOMMENDATIONS	SEV.	PROB.	DETEC.	RPN
Encoder	Does not output any signal	Contamination	Slip control does not work (if 3+ encoders do not work)	4	1	3	12	Introduce a diagnostic and warning system in order to track the encoder's health and in order to be able to detect its malfunctioning.	4	1	1	4
		Mechanical wear										
	Wrong reading	Electrical failures										
		Wiring issues										
		Physical damage										
Accelerometer	Does not output any signal	Electrical failures	Slip control does not work (if 2+ encoders and accelerometer do not work)	4	1	3	12	Insert backup sensor. Introduce a diagnostic and warning system in order to track the accelerometer's health and in order to be able to detect its malfunctioning.	4	1	1	4
		Contamination										
	Wrong reading	Physical damage										
		Wiring issues										
		Temperature										
Dump Valve	Stuck open	Mechanical wear	Impossible to brake	5	3	2	30	Install a secondary dump valve. Implement real-time diagnostic system. Perform maintenance	5	2	1	10
		Contamination										
		Electrical failures										
	Stuck close	Internal blockage	Impossible to release brakes	4	3	2	24		4	2	1	8
		Corrosion										

Failure Mode and Effect Analysis

Slip Control System II

COMPONENT	FAILURE MODE	CAUSES	EFFECTS	SEV.	PROB.	DETEC.	RPN	RECOMMENDATIONS	SEV.	PROB.	DETEC.	RPN
Build Valve	Stuck open	Mechanical wear	Impossible to release brakes	4	3	2	24	Install a secondary build valve. Implement real-time diagnostic system. Perform maintenance	4	2	1	8
		Contamination										
	Stuck close	Electrical failures										
		Corrosion	Impossible to brake	5	3	2	30		5	2	1	10
		Internal blockage										
Ignition Coils	Does not work	Wiring issues	Unable to ignite the fuel in the cylinders, no torque generation	5	3	1	15	Add a health monitoring system. Perform periodic/predictive maintenance	5	2	1	10
		Contamination										
		Wear (temperature or vibrations)										
DC Brushless	Does not work	Temperature	Unable to drive the butterfly valves and introduce the fuel inside the cylinders, no torque generation	5	3	1	15	Add a secondary actuator. Add a fail safe mode Introduce an alert system. Periodic/predictive manteinance.	5	1	1	5
		Wiring issues										
		Wear										
Power Supply	Does not work	Overvoltage or voltage spikes	Slip control does not work Damage of other components	4	3	1	12	Insert overcurrent protections. Introduce a backup power system.	4	1	1	4
		Battery wear										
	Overcurrent condition	Wiring issues										
		Electrical failures										
		Temperatures										

Velocity and Distance Control Systems

For the Failure Mode and Effect Analysis of the other two control systems, i.e. the velocity and distance control systems, the analysis of the previous components is the same, since they are engaged in all the three control systems.
In addition, we only have to analyze the failure modes of the radar.

COMPONENT	FAILURE MODE	CAUSES	EFFECTS	SEV.	PROB.	DETEC.	RPN	RECOMMENDATIONS	SEV.	PROB.	DETEC.	RPN
Radar	Does not output any signal	Environmental interference	Distance control does not work	3	2	3	18	Sensor Fusion, integrating radar with cameras or Lidar. Adaptive calibration algorithms. Add a monitoring system.	3	1	2	6
		Hardware failures										
		Wiring issues										
	Wrong reading	Calibration errors										
		Electromagnetic interference										

4. FAULT TREE ANALYSIS

Introduction and Main Hypotheses

The top event considered in this analysis is **the malfunctioning of the Kalman Filter**. This malfunction is selected because it involves both the encoders and the accelerometer, which are two key sensors of the ACC. Additionally, this failure leads to the malfunctioning of both the slip and the velocity control loops, requiring thus the disengagement of ACC.

In line with the previous hypothesis, the ACC system already naturally incorporates redundancy for the encoders. Therefore, the countermeasures addressed in this analysis focus solely on the power supply subsystem and the accelerometer sensor.

To simplify the process, we first calculate the probabilities of failure for a single **encoder** and for the **accelerometer**. Finally, these probabilities are combined to determine the likelihood of the top event occurring.

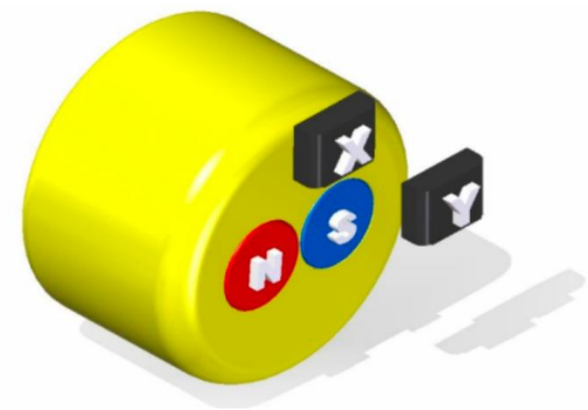
All the probabilities of the basic events are not taken from real data. They have been made up only for the scope of this project.

A previously considered countermeasure to obtain the vehicle's speed and, consequently, the slip was to use of a GPS sensor. However, this is not included in the current analysis, as the focus is on the malfunction of the speed and slip estimation, whereas GPS provides a direct measurement without requiring any estimation.

Encoder Functioning and Physical Structure

Rotary magnetic hall effect encoders are often employed in automotive applications, in order to construct the Fault Tree of this component it is necessary to briefly overview how it is physically made and how it works:

Figure 1: Two Hall effect sensors in quadrature and a pair of magnets.

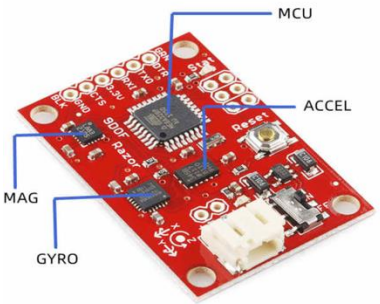


It is composed of a rotor and of a stator, on the rotor a permanent magnet is mounted. On the stator two hall effect sensors are mounted in quadrature so that they can measure independently the variation of the magnetic field and output a voltage signal each. A circuit board, equipped with a microcontroller and containing the encoder's algorithm, is also mounted on the stator. A protective casing encapsulates all the delicate hardware.

The rotor is mounted rigidly to the inner ring of the bearing, which rotates together with the wheel's hub. The stator is mounted rigidly to the outer ring of the bearing, which is fixed to the knuckle (stationary part of the suspension). A precise air gap exists between the rotor and the stator, it is carefully designed in order ensure adequate signal quality and must never change.

Accelerometer Functioning and Physical Structure

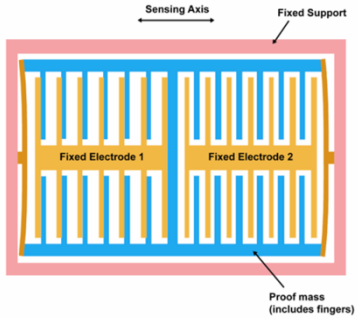
IMUs are often employed in automotive applications, once again in order to construct its fault tree a brief overview of its physical implementation and of how it works is necessary.



IMUs are electronic devices composed of a printed circuit board (PCB) encapsulated in a protective casing. Onto the PCB various sensors (MEMS) are mounted, in particular we are interested in the functioning of the longitudinal accelerometer.

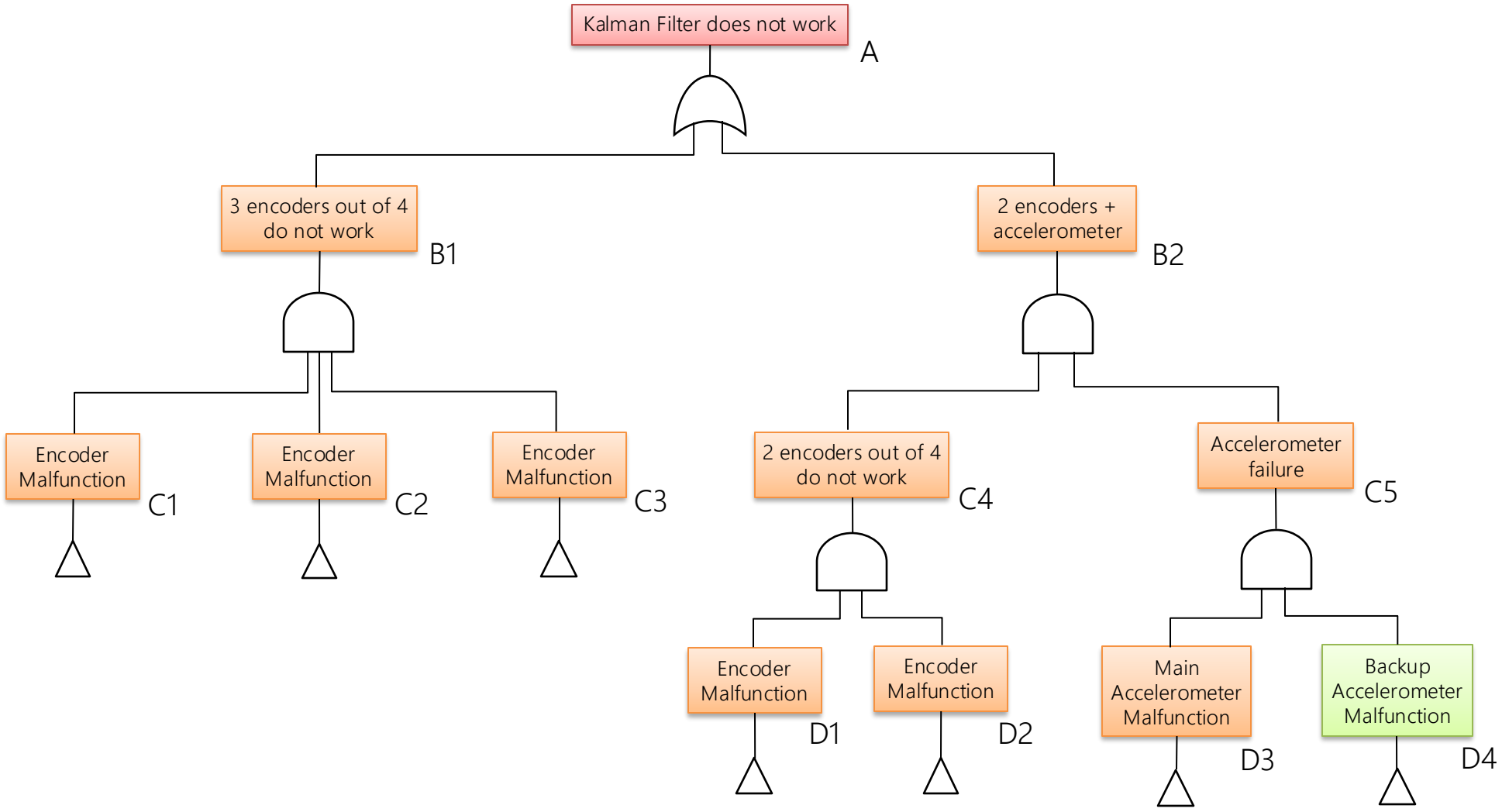
The accelerometer consists of a proof mass attached to its reference frame by mechanical springs.

The springs allow movement of the proof mass along what is known as the sensitivity axis. Measuring the displacement of the proof mass allows computation of the applied acceleration. The sensitivity axis must be aligned with the longitudinal axis of the vehicle.



Measurement of the displacement is performed through electrical capacitance. The sensor will have several differential capacitors. These are electrodes that are fixed in place either side of the proof mass. The proof mass will have extension arms that protrude into the space between the differential capacitor electrodes. At a standstill, the fingers are centered between the electrodes and a known capacitance is produced to represent zero acceleration. During an acceleration event, the proof mass moves – this is because it is sprung and so will accelerate at a different rate to the rest of the sensor (the reference frame). As a result, the fingers move closer to one electrode, creating a change in capacitance from which acceleration can be derived.

Kalman Filter Malfunction I



Kalman Filter Malfunction II

Event Code	D1	D2	D3	D4
Probability (%)	12.70	12.70	10.91	10.91

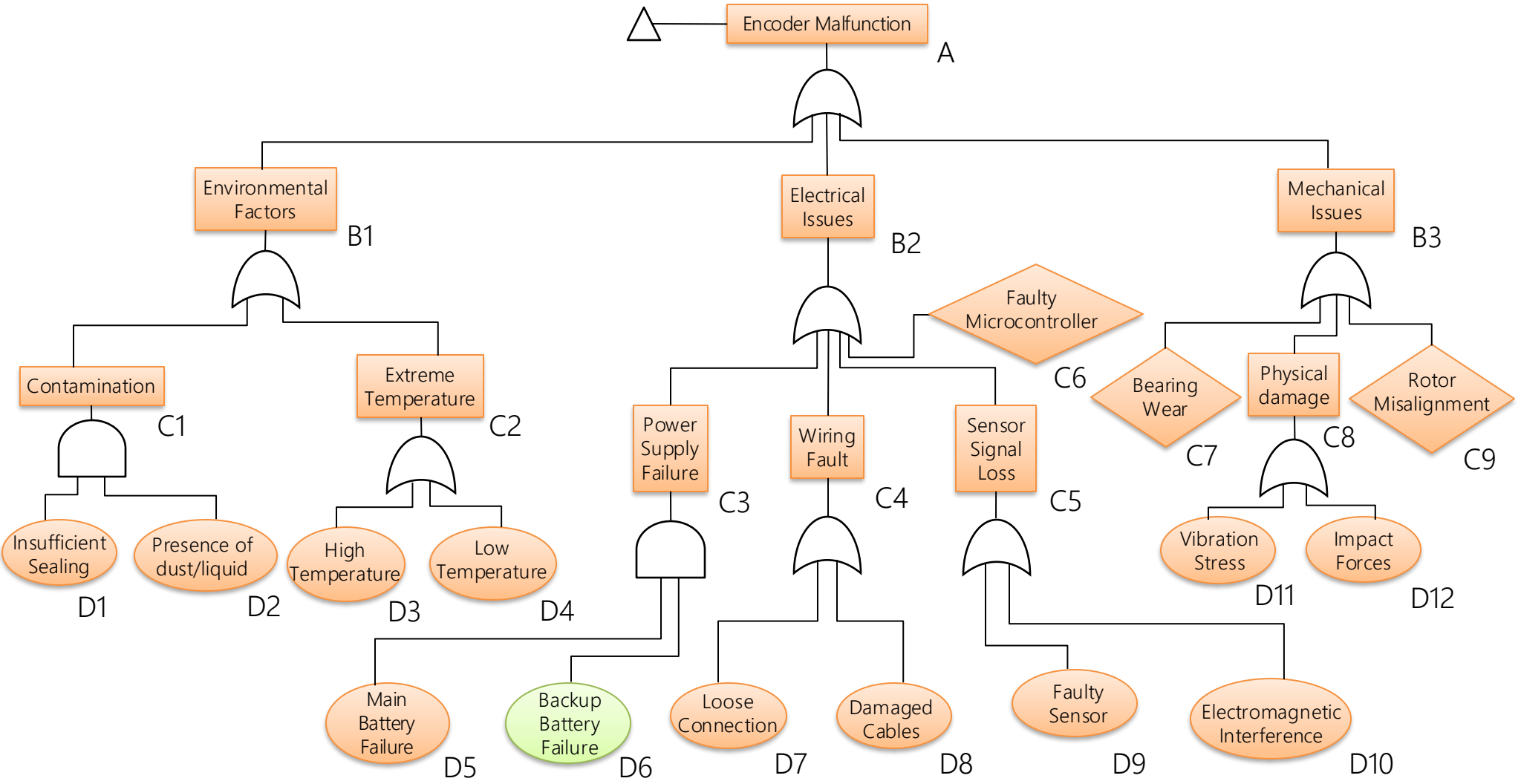
Event Code	C1	C2	C3	C4	C5
Probability (%)	12.70	12.70	12.70	1.61	1.19

Event Code	B1	B2	A
Probability (%)	0.20	0.02	0.22

Remark: notice that, before the introduction of the safety measures, a single base event (power supply failure) would have lead to the top event.

The probability of an encoder and accelerometer malfunction has been determined using specific fault trees for each component. These fault trees are presented in the following slides.

Encoder Malfunction I



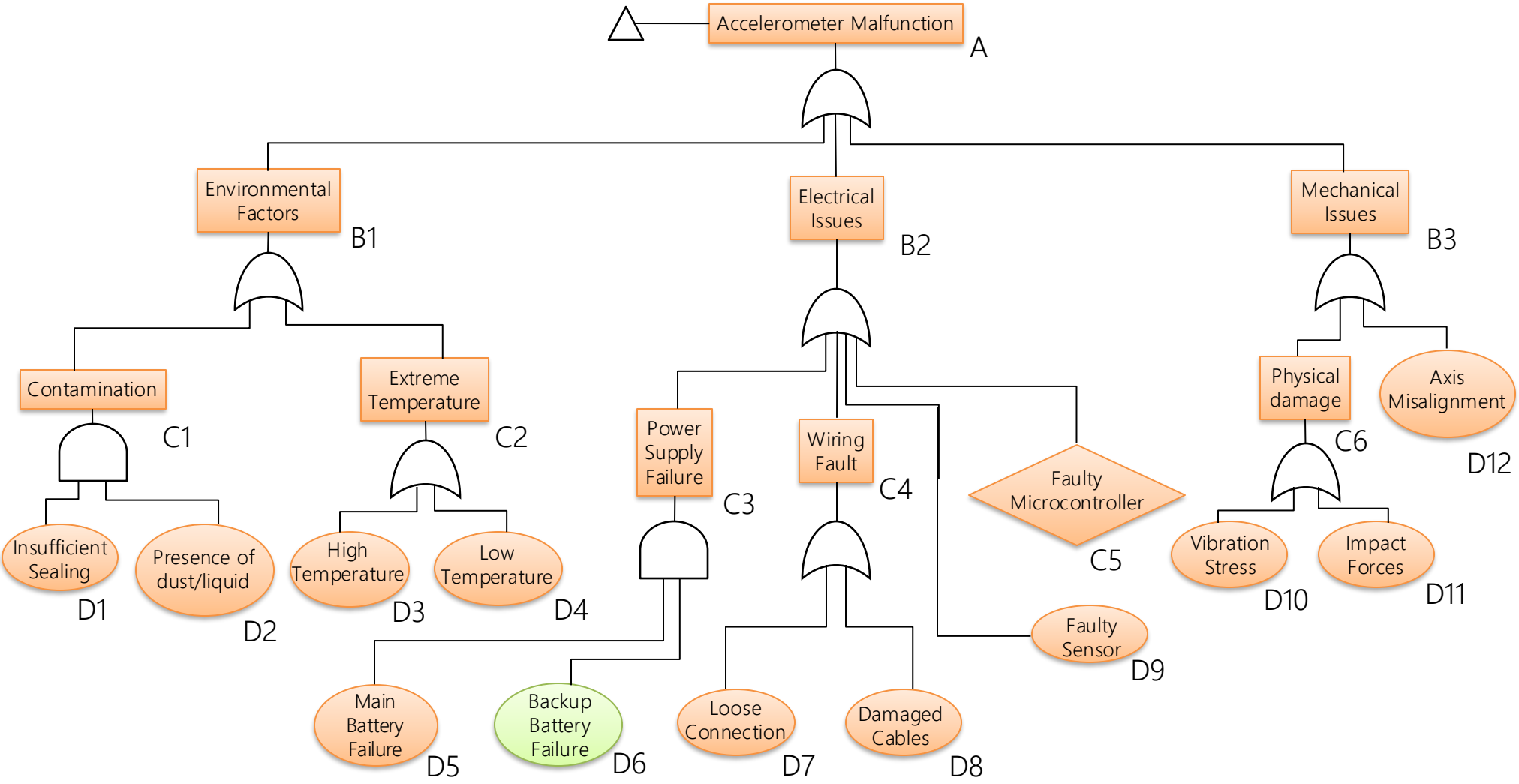
Encoder Malfunction II

Event Code	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12
Probability (%)	0.80	1.00	0.50	0.30	0.08	0.08	0.10	0.20	0.03	0.01	5.00	3.00

Event Code	C1	C2	C3	C4	C5	C6	C7	C8	C9
Probability (%)	0.008	0.80	0.16	0.30	0.04	0.05	2.00	7.85	2.00

Event Code	B1	B2	B3	A
Probability (%)	0.81	0.55	11.50	12.70

Accelerometer Malfunction I



Accelerometer Malfunction II

Event Code	D1	D2	D3	D4	D5	D6	D7	D8	D9	D10	D11	D12
Probability (%)	0.80	1.00	0.50	0.30	0.08	0.08	0.10	0.20	0.03	5.00	3.00	2.00

Event Code	C1	C2	C3	C4	C5	C6
Probability (%)	0.008	0.80	0.16	0.30	0.05	7.85

Event Code	B1	B2	B3	A
Probability (%)	0.81	0.54	9.69	10.91

Kalman Filter Malfunction at higher level I

The fault tree for the Kalman Filter malfunction can be analyzed at a higher level, treating encoder and accelerometer malfunctions as basic events.

As previously discussed, the malfunction of the Kalman Filter can result from either the failure of 3 or more encoders or the failure of 2 or more encoders combined with the accelerometer.

A high-level analysis is valuable for understanding the probabilities of these two distinct causes and, consequently, determining which is more critical.

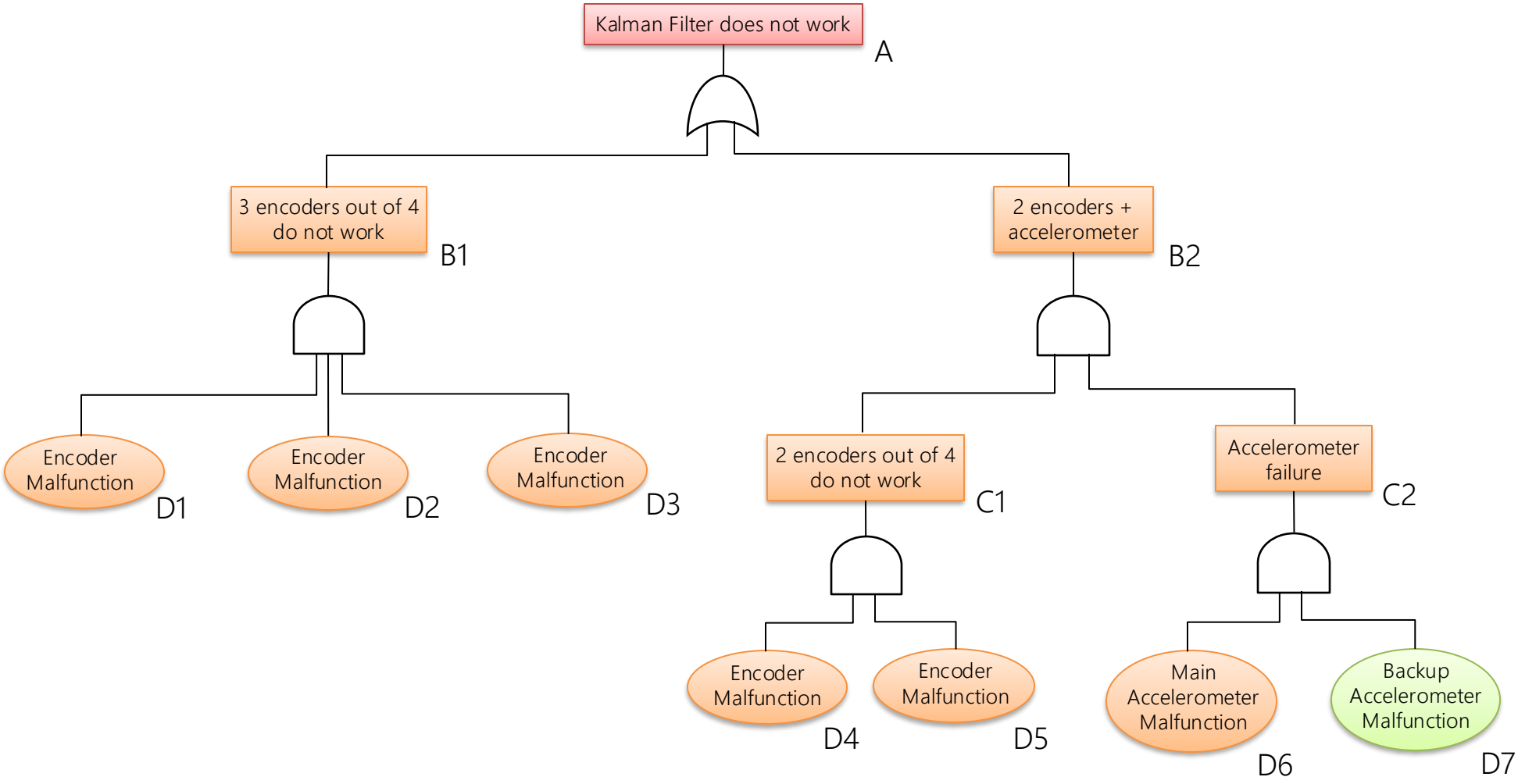
In this analysis, the probabilities of the basic events are not based on real-world data but are estimated using the MTBF (Mean Time Between Failures) of the encoder and accelerometer:

- encoder (rotative) MTBF = 100.000 hours
- accelerometer (IMU) MTBF = 200.000 hours

Based on this data, we have assumed that the probability of an encoder failure is higher than that of an accelerometer.

Therefore, it is expected that the probability of 3 or more encoder failures is slightly higher than the probability of 2 or more encoder failures combined with an accelerometer failure.

Kalman Filter Malfunction at higher level II



Kalman Filter Malfunction at higher level III

Event Code	D1	D2	D3	D4	D5	D6	D7
Probability (%)	13.00	13.00	13.00	13.00	13.00	8.00	8.00

Event Code	C1	C2
Probability (%)	1.69	0,64

Event Code	B1	B2	A
Probability (%)	0,22	0.01	0.23

Observations:

- The probability of an accelerometer failure (event C2) is significantly lower than the initial probability (events D6 and D7) due to the implementation of a backup accelerometer as a countermeasure.
- As expected, it can be observed that the failure of 3 encoders (event B1) is more likely and thus more critical than the failure of 2 encoders and an accelerometer (event B2).
- The difference between these two probabilities is more significant than initially anticipated, as a backup accelerometer was added while no changes were made to the number of encoders, which were already redundant.

5. EVENT TREE ANALYSIS

Introduction

We analyze the event tree of the throttle position actuator, in particular the initiating event is taken as the **malfunction of the DC Brushless** in order to see how it affects the functioning of the engine and therefore of the ACC system.

The presence of a backup **DC brushless**, of a **mechanical bypass** and of the **fail safe mode** is considered.

Thanks to the presence of a suitable sensor (assumed ideal) in case of failure of both the primary and the auxiliary DC brushless, the system is switched to the mechanical backup mode, allowing the driver to manually control the butterfly valves of the engine.

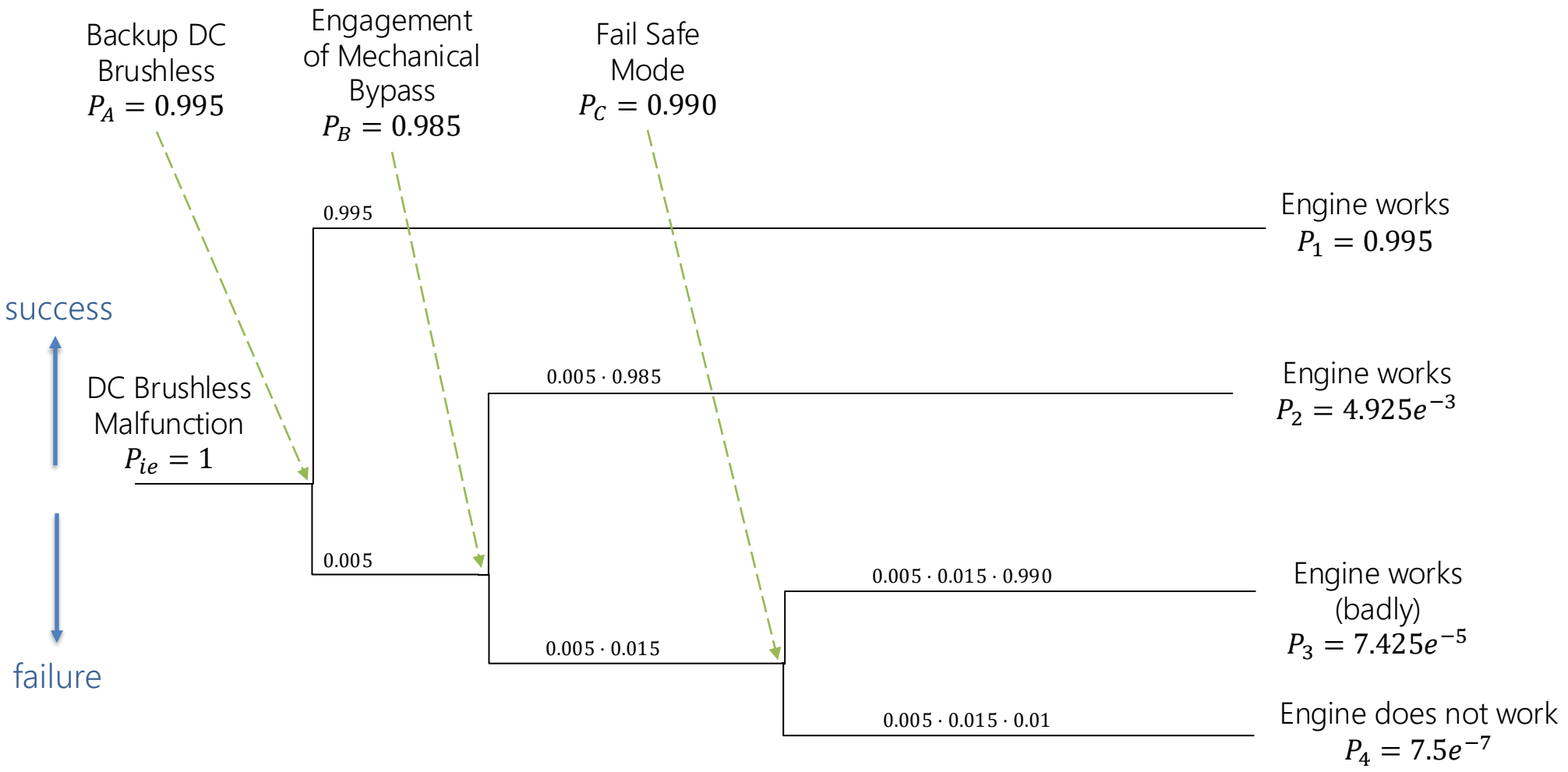
In case of failure of the mechanical bypass, a fail safe mode known as "**limp mode**" is engaged.
The fail safe mode is completely mechanical and consists in a spring, for each butterfly valve, which keeps the valve always slighty open, allowing the engine to work at low power, giving the time to the driver to safely halt the vehicle.

The events considered are reasonably independent, therefore $P\ (A \cap B) = P\ (A) \cdot P(B)$
The probabilities are arbitrarily chosen and are not taken from real data. They have been made up only for the scope of this project.
In particular:

- P_A, P_B and P_C are the probabilities that the corresponding countermeasure works.
- P_1, P_2, P_3 and P_4 are the probabilities that the engine works or does not work.

As expected, after the three countermeasures considered, the probability that the engine does not work is very low.

Scheme


Backup DC Brushless
$P_A = 0.995$
Engagement of Mechanical Bypass
$P_B = 0.985$
Fail Safe Mode
$P_C = 0.990$
success
failure
DC Brushless Malfunction
$P_{ie} = 1$
0.995
0.005
$0.005 \cdot 0.985$
$0.005 \cdot 0.015$
$0.005 \cdot 0.015 \cdot 0.990$
$0.005 \cdot 0.015 \cdot 0.01$
Engine works
$P_1 = 0.995$
Engine works
$P_2 = 4.925e^{-3}$
Engine works (badly)
$P_3 = 7.425e^{-5}$
Engine does not work
$P_4 = 7.5e^{-7}$

6. CONCLUSIONS

Conclusions

The hazard analysis of the Adaptive Cruise Control (ACC) system has demonstrated its inherent safety and reliability, thanks to its inherently redundant design.

However, critical components, such as the accelerometer sensor, actuators, and the single power supply, remain areas of vulnerability that require careful consideration.

Through the introduction of targeted countermeasures, such as a backup power supply, sensor health monitoring systems, and redundant actuation mechanisms, the overall safety of the system can be significantly enhanced.

These improvements ensure that the ACC can maintain its functionality even in the presence of certain failures, thus reducing the risk of accidents and system shutdowns.

Lastly, while the system already exhibits high reliability in presence of the countermeasures, auxiliary measures such as regular/predictive maintenance schedules and driver alerts play a crucial role in further increasing safety.

Once all countermeasures have been introduced, the ACC system can achieve optimal performance and ensure driver and passenger safety in all operating conditions.

References

- "Automation and Control in Vehicles" – Lecture notes
- "Safety in Automation Systems" – Lecture notes
- www.heidenhain.it for encoder MTBF
- www.analog.com for accelerometer MTBF
- www.bosch-mobility.com for radar MTBF
- www.fuchenglhd.com for hydraulic valve MTBF
- W. A. Lopez-Contreras and J. D. Rairan-Antolines. Design of a magnetic encoder using the Hall effect, 2019.
- www.jouav.com/blog/inertial-measurement-unit.html
- www.advancednavigation.com/tech-articles/inertial-measurement-unit-imu-an-introduction

THANK YOU!

POLITECNICO
MILANO 1863