System hazard analysis of a high speed/high capacity railway

A.Y. 2019-2020
Safety in Automation Systems
Prof. Riccardo Scattolini

Alex Franco, 928019
David Luna, 913300
Matteo Savino, 920028

Index

Glossary

In describing the system we will often come across anagrams abbreviating some names of the system's parts. In this slide a brief chart is provided with the meaning of the most important ones.

Anagram	Meaning
BTS	Base Transreceiver Station
DMI	Driver Machine Interface
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EVC	European Vital Computer
FSM	Full Supervision Mode
GSS	Ground SubSystem
GSM-R	Global System Mobile - Railway
HS/HC	High Speed/High Capacity
MA	Motion Authority
OBSS	On-Board SubSystem
PCS	Posto Centrale di Stazione
PPF	Posto Periferico Fisso
PSM	Partial Supervision Mode
RBC	Radio Block Center

POLITECNICO MILANO 1863

System hazard analysis of a high speed/high capacity railway

INTRODUCTION and ASSUMPTIONS

A Brief Introduction on High Speed Railways in Europe

In Europe, since the late 1990s, train control systems have been standardised to allow interoperability, mainly on the upcoming new high speed railways network along all the continent.

The system chosen is the ERTMS. The first tests were held by the French and Spanish railway companies in the early 2000s, with the application of the Level 1 ETCS.

The Roma-Napoli segment, opened in 2005, was the first line in Europe to operate the Level 2 ETCS.

For the purpose of our project we are studying the Roma-Napoli segment of the italian HS/HC railway indeed, where only high speed ERTMS-equipped passenger trains are allowed to travel, although it recently opened to some high speed cargo trains.

The Roma-Napoli Segment and some Assumptions for Conciseness

The Roma-Napoli HP/HC railway is a 205 km long railway connecting the two stations of Roma Termini and Napoli Centrale in 1h 10min, with a commercial speed of 300 km/h, an average distance between consecutive trains of 25km.

It is a two-rail segment which always allows the contemporary passage of two trains with opposite direction, with a maximum slope of 21‰ and a minimum corner radius of 5450m. Traction is electric in AC, with 2 x 25kV tension at 50Hz. There are no railroad crossings along the entire line.

For conciseness purposes and to reduce the system to a more suitable one for our analysis, we are neglecting some aspects of the whole process as, for example:

- *Priority policies* regarding the two operating companies;
- *Departure and arrival* peculiar operations*;*
- *Environmental related issues* such as all the itinerary interruptions not due to another train's presence;
- The *components* only employed when the train travels on *traditional railways* (ETCS - level 0);
- *Cargo trains presence* on the line;
- *Shunting manoeuvres* and the related operating modes;
- Any *power supply failure;*
- Any *failure of the communication system (GSM-R)*, except for a few (not explored) in the FTA;
- All *train managing issues* which do not affect the train running, i.e. doors not opening/closing;

POLITECNICO
MILANO 1863

System hazard analysis of a high speed/high capacity railway

SYSTEM DESCRIPTION

The European Rail Traffic Management System (ERTMS)

The **ERTMS** is the systems of standards for management and interoperation of signalling for railways by the European Union.

Its main target is to promote interoperability of trains in EU, replacing former national signalling equipment and procedures with a single European standard for control and command systems.

The separately managed parts are:

- ➢ Communication (*GSM-R*)
- ➢ Signalling (*ETCS*)
- ➢ Payload management (*ETML*)

The European Train Control System (ETCS)

The **ETCS** is the signalling and control component of the **ERTMS.**

ETCS is implemented with standard trackside equipment and unified controlling equipment within the train cab. In its advanced form, all lineside information is passed to the driver wireless inside the cab, removing the need for lineside signals watched by the driver.

The main topic of the system is basically to accomplish two main functions:

- *Automatic Train Protection* (ATP), to ensure the correct distance exists between two trains on the same line. The entire line is divided into sections: when a **Motion Authority** is granted for a section, the train has the right to move up until the end of that section, if the **MA** is not granted for the incoming section, the train is given with a braking point calculated in order to stop by the end of the free section.
- *Automatic Train Control* (ATC), to operate emergency braking. The train driver controls traction and braking operations according to the information received on his DMI, but the emergency brake intervenes in case of train driver faults (i.e. the braking point is passed and no action from the driver).

The European Train Control System (ETCS)

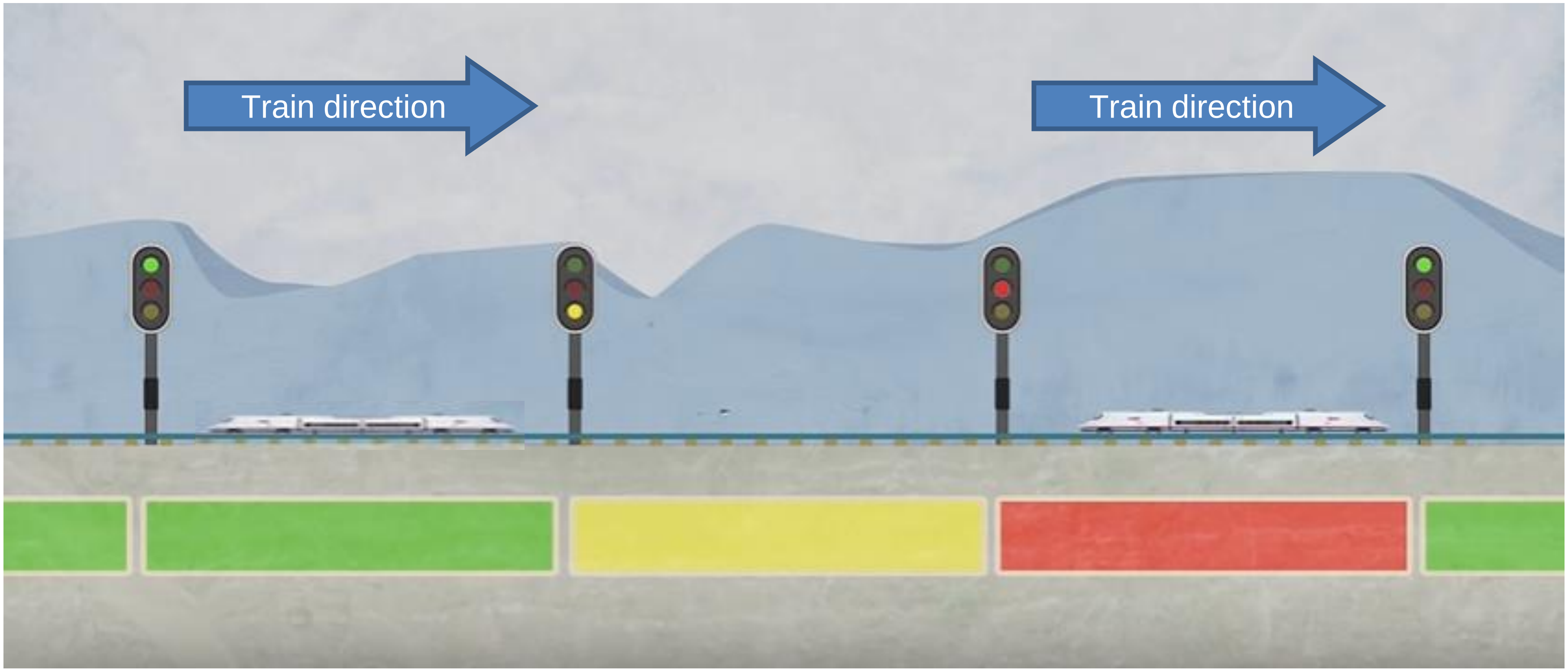


fig. 1 – Motion Authority operational logic. In case of «yellow» section, a braking point is given by the MA for the following train in order to stop before entering the «red» occupied section

The European Train Control System (ETCS)

- **ETCS - Level 0**

  When a ETCS equipped convoy travels on a non-ETCS railway, it is considered at level 0 and will operate as a traditional train, observing ground signage.

- **ETCS - Level 1**

  It is the most suitable to be integrated with the traditional signalling system: while traditionally-equipped convoys use the classic ground signals, ETCS-operating trains use “*Eurobalises*” transponders, with a double function:

  1. Receive information from the train about position and train integrity and status, and from the line-fixed signals about line status
  2. Depending on the information received, sends the **Motion Authority (MA)** to the train on-board **EVC**, which can now calculate max. speed and braking curves.

     Transmissions are operated via radio or via induction at train passage.

The European Train Control System (ETCS)

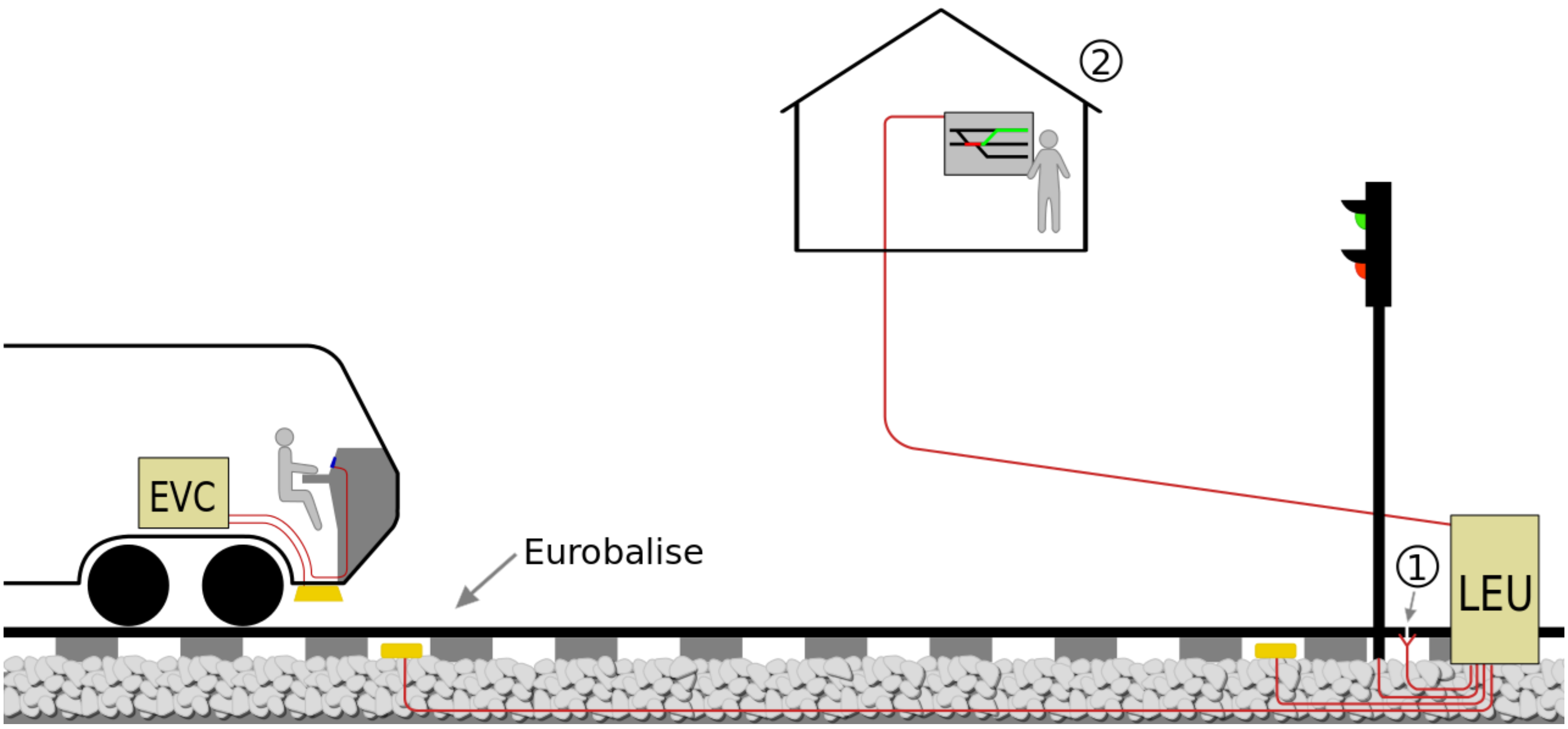


fig. 2 - ETCS - Level 1 functioning scheme

The European Train Control System (ETCS)

- **ETCS - Level 2**

  This is the actual standard operating on the Roma-Napoli railway section.

  1. A Radio Block Center (RBC) receives information on trains positions, integrity and status, elaborated and monitorated by ground operators, situated in Roma Termini PCS (Posto Centrale di Stazione).
  2. The RBC sends **MA** and route information continuously, together with max. speed available and braking points.

  Eurobalises transponders, which can be found at the beginning and at the end of each line section, just work as position detectors to readjust the train odometers. Transmissions are operated via radio and optical fiber by **GSM-R**, while Eurobalises use induction.

  Only Level 2 ETCS and GSM-R equipped rolling stocks are allowed to circulate on Level 2 railways.

- **ETCS - Level 3**

  ETCS Level 3 is based on *dynamical line sections* that **continuously** provide the trains with the correct braking points in order to stop behind the preceding convoy. The first studies have been undertaken In the late 2010s by an european public company but they are still at their early stages.

The European Train Control System (ETCS)

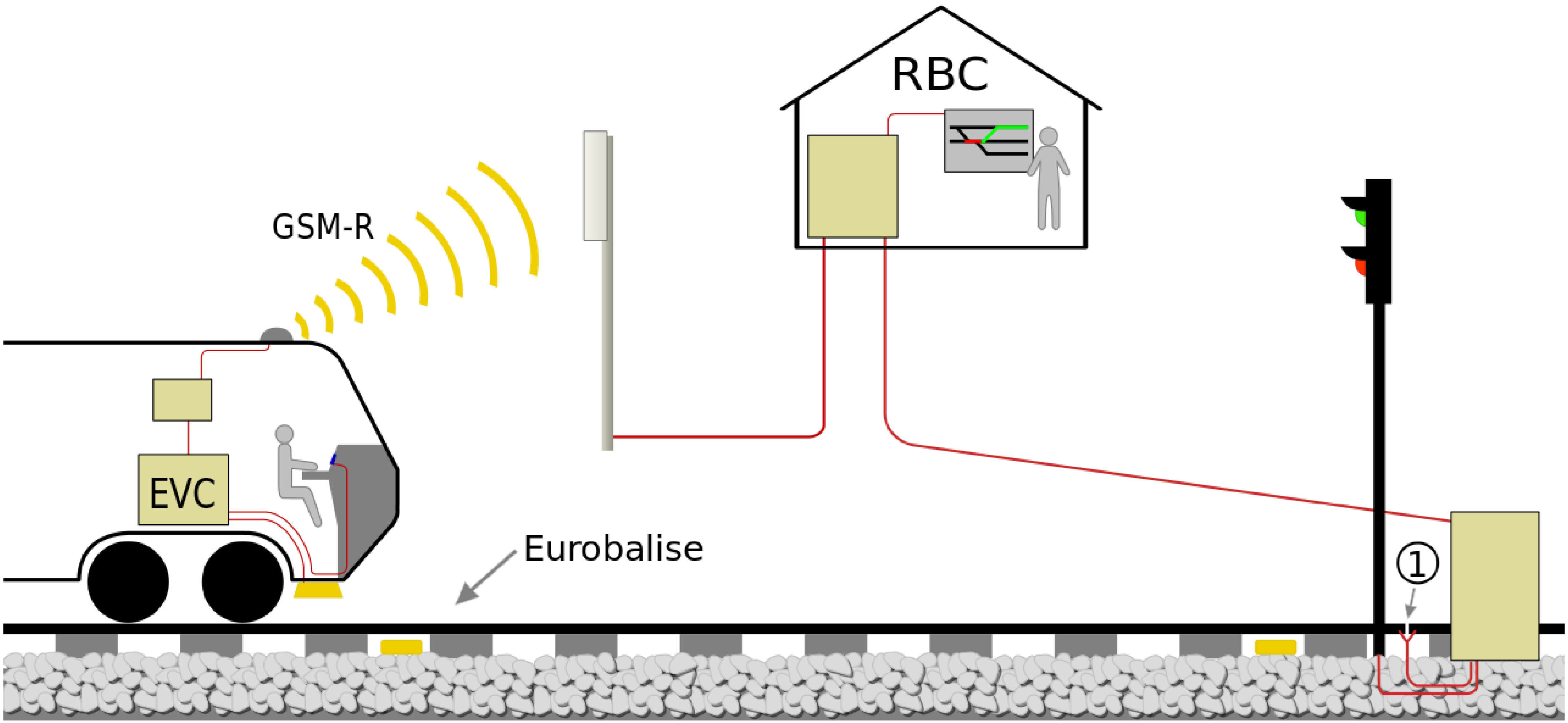


fig. 3 - ETCS - Level 2 functioning scheme

The Global System Mobile - Railway (GSM-R) Network

The **GSM-R** is the current standard for continuous railways radio-signalling.

It is designed to operate on dedicated frequencies, transmitting control and emergency messages between its two main levels:

- **Central level**

  The PCS (Posto Centrale di Sistema) located in Roma Termini that contains the three RBCs (Radio Block Center), each of them controlling an average of 70 km on the line.

  Their topic is to calculate the distance between trains and to send the **MAs** which allow the trains to continue its journey.

- **Peripheral level**

  PPF (Posto Periferico Fisso), located each 12 km, and BTS (Base Transreceiver Station), located each 3 km.

  The firsts gather information about rails status and is connected to the RBC, which send its **MAs** to the train **EVC** through the BTS located along the route.

The fixed components communicate through a long distance optical fiber telecommunication system, while BTSs and trains communicate via radio.

On-Board and Ground Subsystems

The GSM-R's ultimate purpose is therefore to connect a «moving» and a ground-fixed system.

In fact, the two subsystems clearly develop different and complementary functions.

- **Ground subsystem**

  The **GSS** generates the informations needed by the train e transmits via GSM-R the MAs. Among these informations, there are speed profiles, slowing downs, slopes, etc. All of them are generated by the RBC and the PCS through the elaboration of the informations received by the other components of the GSS like the rail status from the PFF, or the train status sent by each train EVC via the BTSs. The various components are connected via optical fiber.

- **On-Board subsystem**

  The **OBSS** goal is to provide a continuous control of the trains speed and a protection against the overcoming of the limits of the MAs. To acheive the goal, all the components of the OBSS carry out a specific task: the odometer identifies the train position thanks to the information received by the Eurobalises via induction through the balise reader, the EVC selects the most suitable speed and braking profiles among the different received from the RBC according to the train's features, and shows the train driver the speed limits and the target speed through the DMI.

The GSM-R Network and the Main Subsystems

fig. 4 - GSM-R functioning scheme

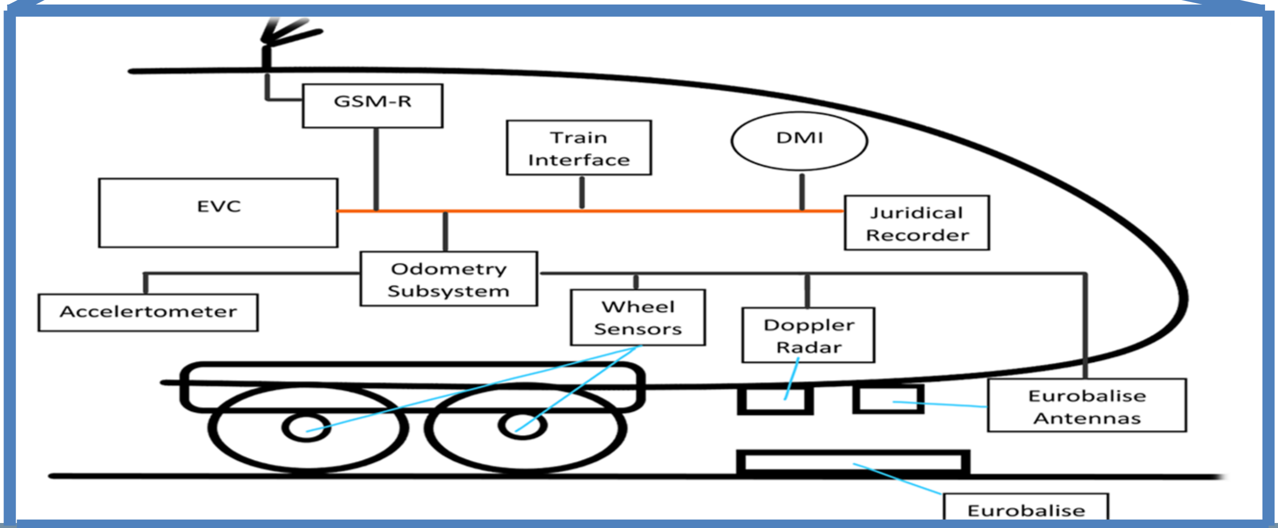


fig. 5 – Diagram of the On-Board subsystem components

Operating Modes

On the railway in question, operating modes are mainly the three described below, divided into *Full Supervision* modes and *Partial Supervision* modes. We will just consider the difference between **FSM** and **PSM** throughout our PHA.

- **Full Supervision Mode**

  ETCS has all required information. Full speed is permitted (300 km/h).

- **Partial Supervision Modes**

  In these scenarios, the train driver is free to enter a line segment when the related MA is not granted (*However in this case of studio, we will assume the passage from **FSM** to **PSM** is not related to any kind of failure*).

  - **Staff Responsible**

    Under written or verbal recorded prescription, can be used to overcome a radio-connection failure until the signal is recovered under driver responsability. Max. speed: 30-50 km/h.

  - **On-sight ride**

    Available when the condition “free” is not verified in the next line section. Max. speed: 30 km/h.

Driver Machine Interface (DMI)

Since on Level 2 - ETCS equipped railways there is no ground signage (apart from some particular cases, later specified), all information such as **MAs**, track conditions and speed limits to respect are provided to the driver on the Driver Machine Interface (**DMI**).

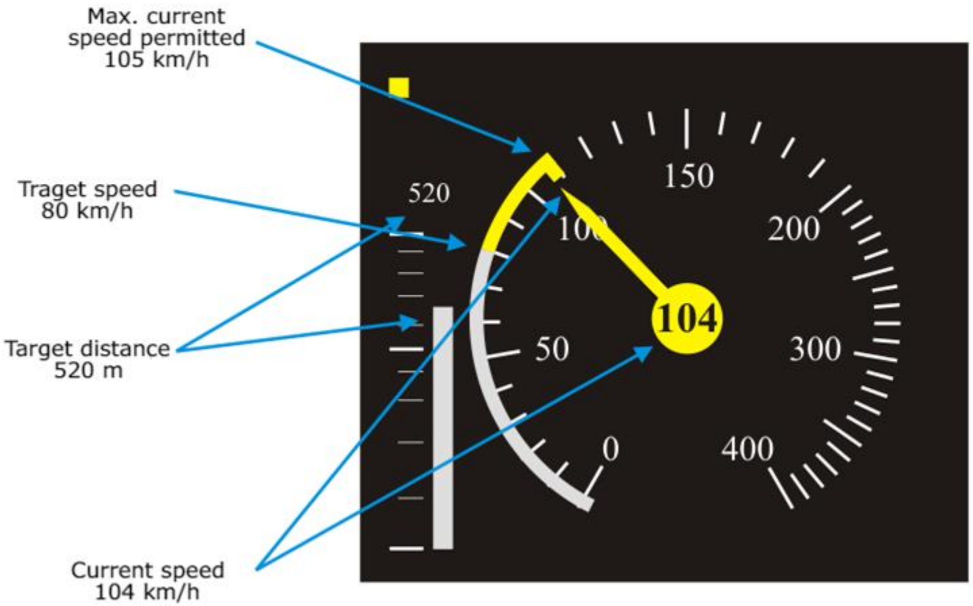


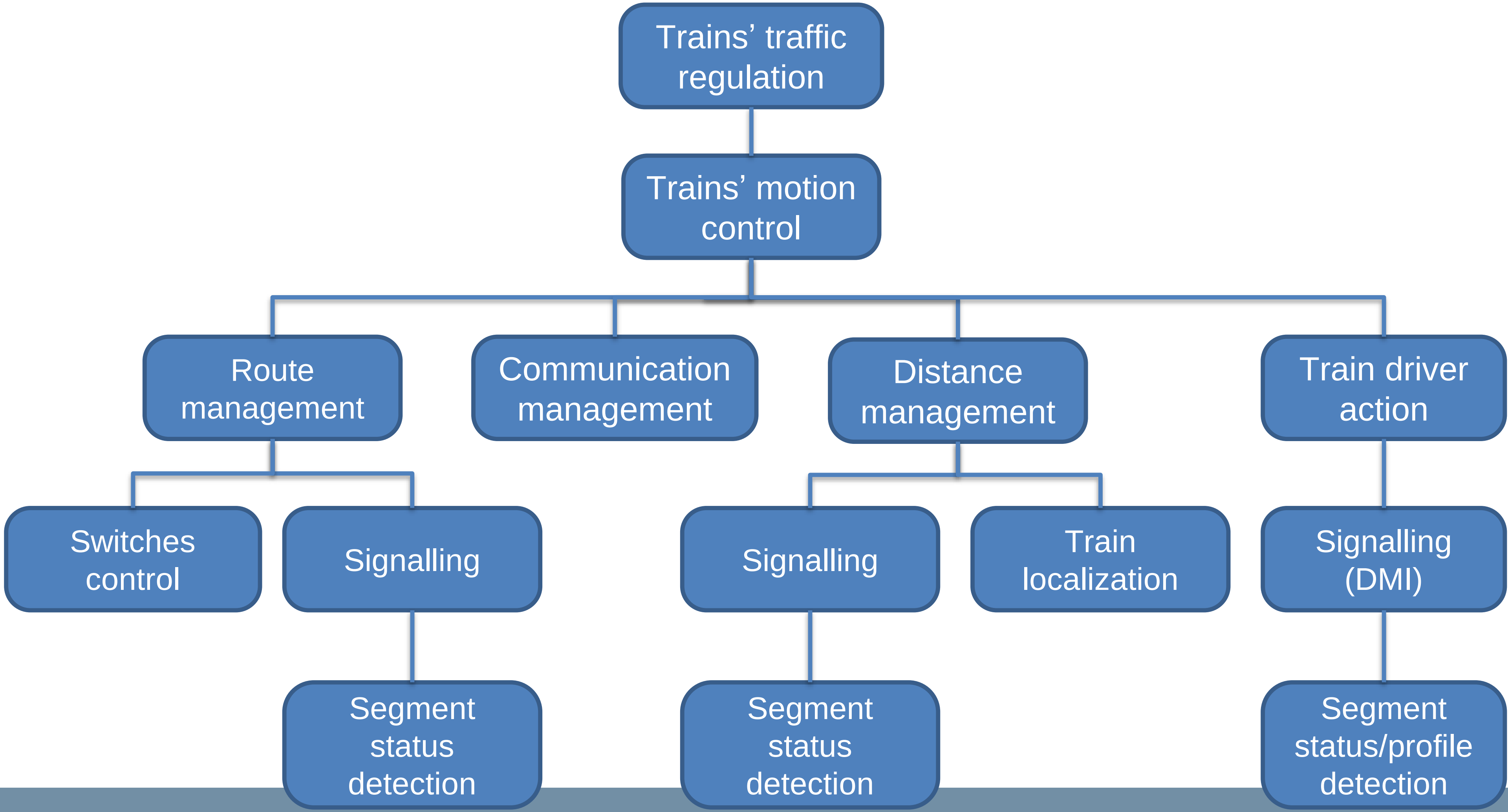
fig. 6 - ETCS DMI

POLITECNICO
MILANO 1863

System hazard analysis of a high speed/high capacity railway

FUNCTIONAL ANALYSIS

Functional Analysis

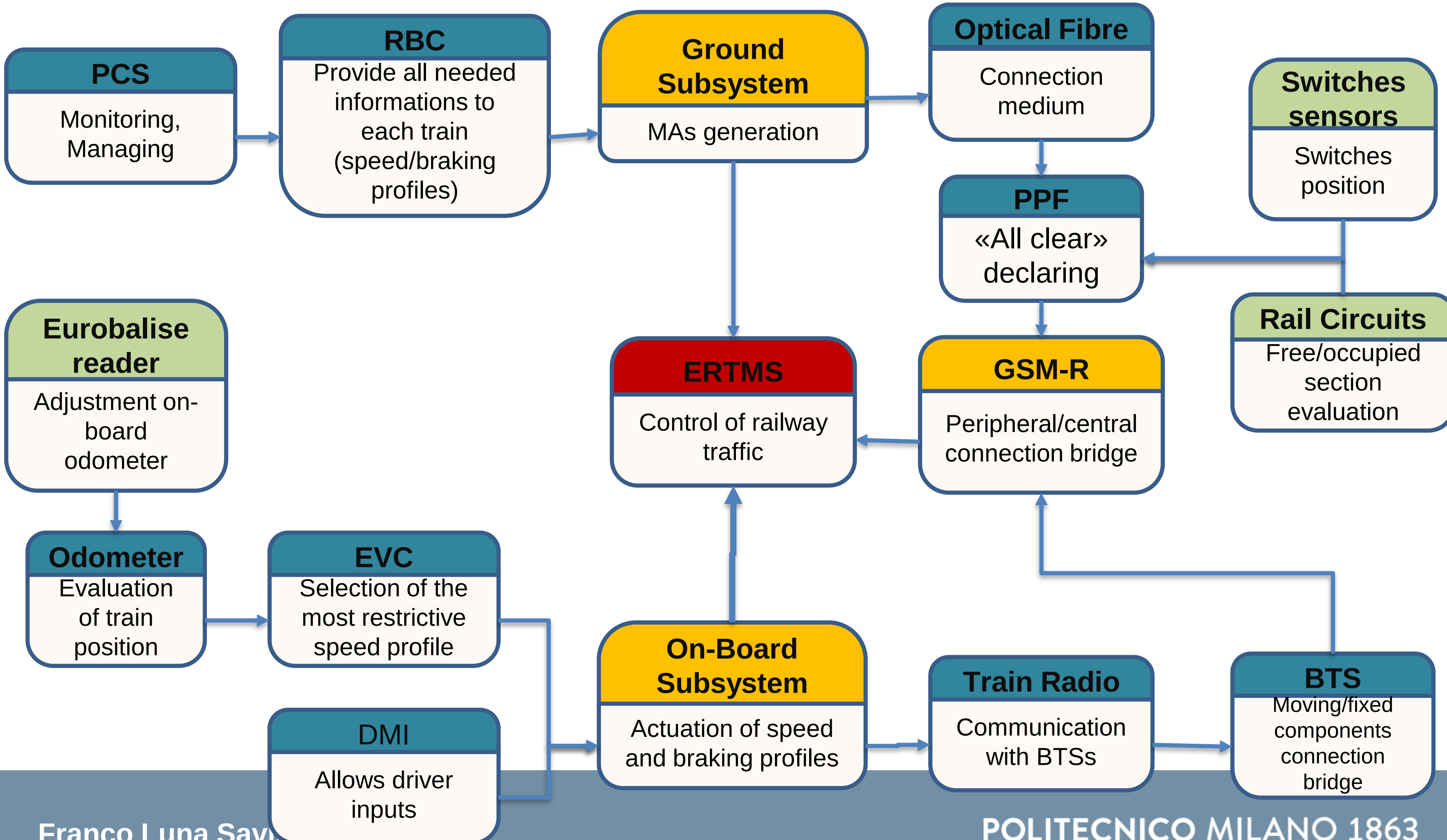


POLITECNICO MILANO 1863

System hazard analysis of a high speed/high capacity railway

ARCHITECTURAL ANALYSIS

Architectural Analysis



POLITECNICO MILANO 1863

System hazard analysis of a high speed/high capacity railway

PRELIMINARY HAZARD ANALYSIS

PHA: Hazard Description (I)

Operating Mode	Hazard		
	Source	Phenomenon	Effect
Full supervision Partial supervision	• EVC failure • Balise reader failure • Odometry failure • Braking system failure • Driver ignoring DMI	Train does not stop at designed point and ends in an occupied section	• Injuries or death to people • Damage to the train and its infrastructure
Full supervision	• RBC failure • Interlocking (Rail circuits) malfunction • Odometry malfunction • Wrong speed profile • Braking system failure	Instantaneous deceleration	• Injuries to people • Possible delays • Excessive wearing to the train
Full supervision Partial supervision	• Communication failure (Internal and external) • Switch sensors failure	Wrong rail selection on terminals	• Delays • Wrong routing • Possible crash with another train • Injuries or death to people

PHA: Hazard Description (II)

Operating Mode	Hazard		
	Source	Phenomenon	Effect
Full supervision Partial supervision	• Unsuitable variables displayed on the DMI • Inappropriate control input (HMI) • Ignoring DMI danger alerts	Biased motion of the train	• Wrong information related to the train-to-train distance and stopping distance
Full supervision	• RBC not noticing another train incoming • Wrong speed profile	Air effect between two trains facing opposite directions	• Damages in the train body and aerodynamics
Full supervision	• Switch sensors/actuators failure • Odometry malfunction • Wrong speed profile • Local communication failure	Derailment due to too high speed	• Injuries or death to people • Damage to the train
Full supervision Partial Supervision	• Failed or delayed activation of the braking system	Railway section block	• Delays • Wrong position information • Damage to the train

PHA: Targets

The targets at risk which would be affected by the consequences of an accident are the **train** (**T**), the **infrastructures** (rails, power supply structures, rails sensors, …) (**I**), and the **passengers** (including the company staff on-board) (**P**).

Target	Train (T)
Severity of consequences	
CATASTROPHIC	Total train destruction
CRITICAL	Limited irreparable damages
MARGINAL	Reparable damages
NEGLIGIBLE	Secondary damages

Target	Infrastructures (I)
Severity of consequences	
CATASTROPHIC	Total loss of railway portion
CRITICAL	Partial losses
MARGINAL	Reparable damages
NEGLIGIBLE	Secondary damages

Target	Passengers (P)
Severity of consequences	
CATASTROPHIC	Deaths
CRITICAL	Severe injuries
MARGINAL	Minor wounds
NEGLIGIBLE	Complaints and delays

TARGET: TRAIN (T)

Severity of Consequences	Probability of Mishap				
	E – IMPROBABLE	D - REMOTE	C - OCCASIONAL	B - PROBABLE	A - FREQUENT
I – CATASTROPHIC	2	2	3	3	3
II – CRITICAL	1	2	2	3	3
III – MARGINAL	1	1	1	2	3
IV - NEGLIGIBLE	1	1	1	1	2

Note: Probabilities estimated using a time interval of 10 years

TARGET: INFRASTRUCTURES (I)

Severity of Consequences	Probability of Mishap				
	E – IMPROBABLE	D - REMOTE	C - OCCASIONAL	B - PROBABLE	A - FREQUENT
I – CATASTROPHIC	1	2	3	3	3
II – CRITICAL	1	1	2	3	3
III – MARGINAL	1	1	1	2	2
IV - NEGLIGIBLE	1	1	1	1	1

Note: Probabilities estimated using a time interval of 10 years

PHA: Risk Assessment Matrices

TARGET: PASSENGERS (P)

Severity of Consequences	Probability of Mishap				
	E – IMPROBABLE	D - REMOTE	C - OCCASIONAL	B - PROBABLE	A - FREQUENT
I – CATASTROPHIC	2	3	3	3	3
II – CRITICAL	2	2	3	3	3
III – MARGINAL	1	1	2	2	3
IV - NEGLIGIBLE	1	1	1	1	2

Note: Probabilities estimated using a time interval of 10 years

PHA: Possible Countermeasures

Probability Interval: 10 years	Risk BEFORE					Risk AFTER		
HAZARD	Target	Severity	Probability	Risk Code	COUNTERMEASURES	Severity	Probability	Risk Code
Train does not stop at designed point and ends in an occupied section	T I	II III	E E	1 1	- Acoustic alarms that ring in the cabin in case of danger, to recall driver attention; - Safety belts for passengers - Emergency braking sub-system	II III	E E	1 1
Instantaneous deceleration	T P	IV III	B B	1 2	- Safety belts for passengers - Invite the passengers not to get up during the travel - Double-check algorithm to determine the sutiable decelartion profile for a given desired distance.	IV IV	B B	1 1
Wrong rail selection on terminals	T I P	II I I	C C C	2 2 3	- Implementation of a logic which never puts the train on an occupied rail - Periodic mantainance on the switching system	II I I	E E E	1 1 2

PHA: Possible Countermeasures

Probability Interval: 10 years	Risk BEFORE					Risk AFTER		
HAZARD	Target	Severity	Probability	Risk Code	COUNTERMEASURES	Severity	Probability	Risk Code
Biased motion of the train	T P	II II I	C C C	2 2 3	- Error message notification on the DMI; - HMI improvement; - Additional alarm systems for warning - Comparison between data from the odometry system and the balises and the wireless connection	II II I	D D D	2 1 2
Air effect between two trains facing opposite directions	T P	III IV	A A	3 2	- Safety belts for passengers - Double-check of the chosen speed profile - Balise triggered deceleration	III IV	B B B	2 1
Derailment due to too high speed	T I P	I I I	D D D	2 2 1	- Redundancy of speed and odometry sensors - Preventive maintenance of switch sensor actuactors - Ultrasonic defect detection, radar, spectroscopy,	I I I	E E E	2 1 2

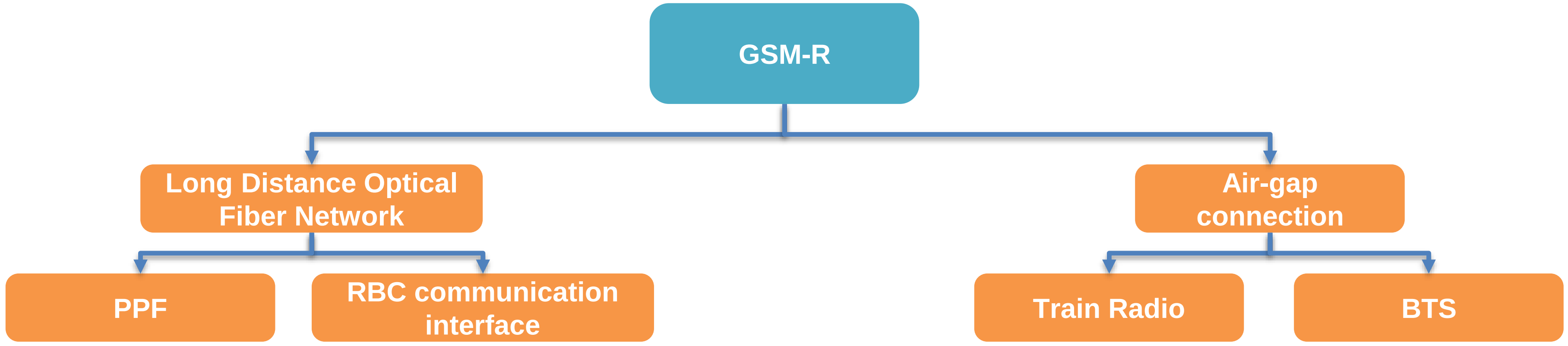
POLITECNICO MILANO 1863

System hazard analysis of a high speed/high capacity railway

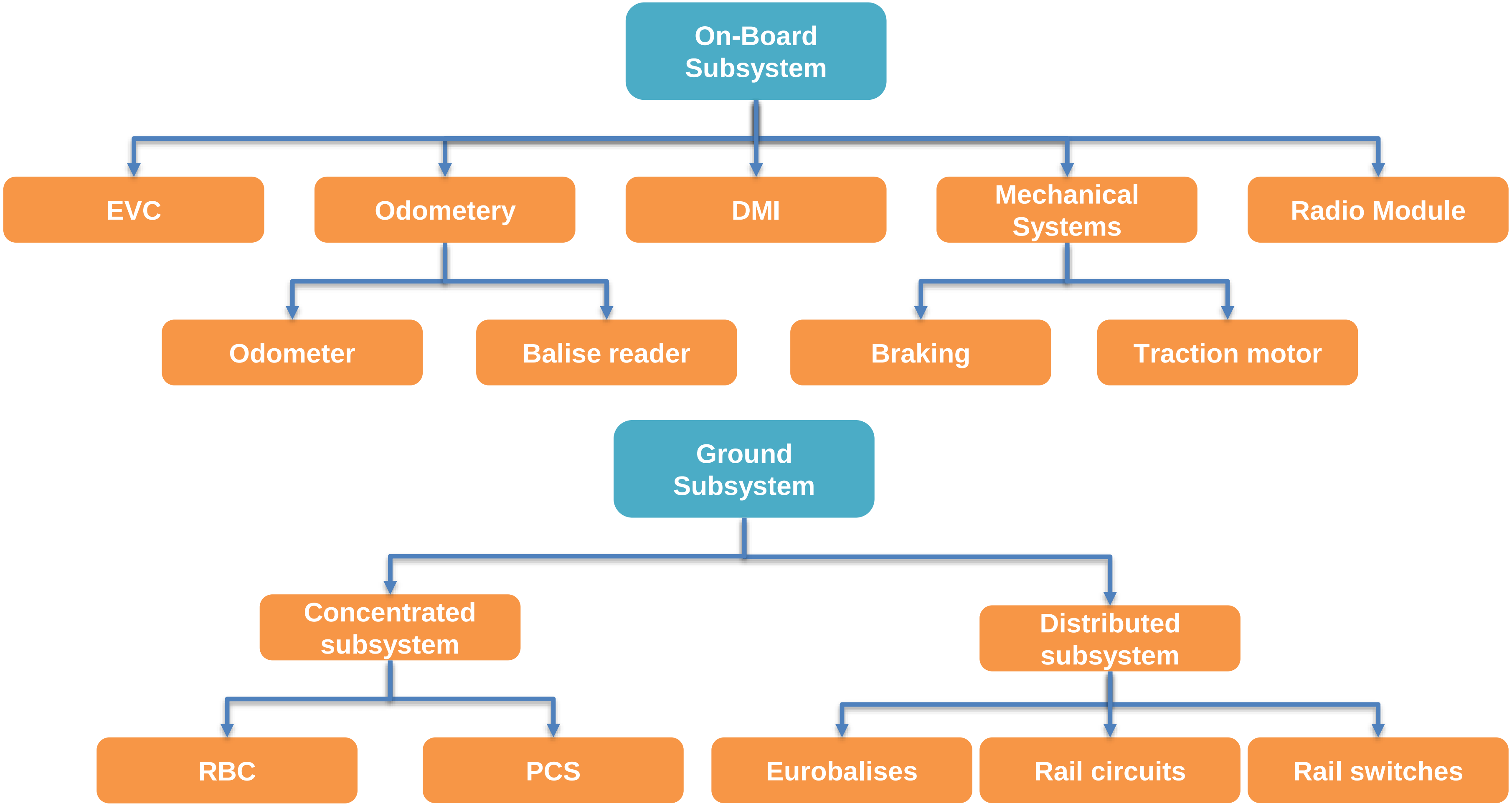
FAILURE MODES and EFFECT ANALYSIS

FMEA: System Structures (I)

As you can easily imagine, the system structure is gargantuan and focusing on each component of the whole system would led us to a huge amount of elements to treat.
We have consequently decided to deal only with the elements concerning the *line managing system*, neglecting the train's mechanical systems specifically (here reduced to *traction* and *braking* for conciseness) and the power supply network as already mentioned in the introduction slides.
Moreover, only a structural scheme of the GSM-R subsystem is provided below, although it will not be treated in the FMEA because we assumed there are no communication issues or failures in our system.



FMEA: System Structures (II)



FMEA: Full Supervision Mode

Component	Failure Mode	Failure Causes	Failure Effects	Severity T	Severity P	Severity I	Probability	Control Measures/ Remarks
EVC	Malfunctioning	Lack of electrical power	On-board subsystem does not work	II	II	II	D	• Emergency power generator
		Connection problems	Wrong interconnection between actuactors and ensors	II	II	II	D	• Periodical inspection • Automatic switch to Partial Supervision Mode
Odometer	Malfunctioning	Internal electronic problems	Impossibility or difficulties to perform a measurement	I	-	I	C	• Maintenance • Check operating conditions
	Wrong Indication	• Missed calibration • Bad weather conditions	• Inaccurate measurement • misleading interpretation	I	-	I	C	• Automatic switch to Partial Supervision Mode

FMEA: Full Supervision Mode

Component	Failure Mode	Failure Causes	Failure Effects	Severity			Probability	Control Measures/ Remarks
				T	P	I		
DMI	Wrong Indication	Wrong computation of speed profile	Incorrect distance and speed maintained among rail convoys	II	I	II	B	• Acoustic alarms ring in the cabin in case of danger, to recall driver attention • Emergency brakin gsystem
BALISE READER	Uncertain measurements	Balise transmission module fault(or radio frequency interference)	Inaccurate or missing location information of train	III	-	III	B	Adoption of protection systems for radio frequency interference
TRACTION MOTOR	Lack of electric power	Motor power supply failure	Train in stuck	II	-	II	D	• Maintenance • Periodical inspection
	Over current	Overload	Explosion,insufficient torque ,overheating and premature wear of components	I	I	I	D	Overload relay connected to the motor starter
	Over braking Over acceleration	• Speed profile not suitable for the track side • Wrong action from the controller	• Wrong planned position and motion of rail convoy • Possible collision • Derailments	I	I	I	D	• Check the controller programming • protection systems for correcting maneuvers

FMEA: Partial Supervision Mode

Component	Failure Mode	Failure Causes	Failure Effects	Severity T	Severity P	Severity I	Probability	Control Measures /Remarks
EVC	Malfunctioning	Crash of system	Ground subsystem disconnected by EVC	II	II	II	D	Train driver assume full control of the rail convoy (with speed limitations)in absence of MA
DMI	No input signal(Speed profile or braking curves)	EVC malfunctioning	Non-acceptance With the directives imposed by RBC	II	II	II	D	Maintain a radio/message communication channel between driver and PCS

FMEA: Full Supervision Mode & Partial Supervision Mode

<table>
<tr><th rowspan="2">Component</th><th rowspan="2">Failure Mode</th><th rowspan="2">Failure Causes</th><th rowspan="2">Failure Effects</th><th colspan="3">Severity</th><th rowspan="2">Probability</th><th rowspan="2">Control Measures/Remarks</th></tr>
<tr><th>T</th><th>P</th><th>I</th></tr>
<tr><td rowspan="5">RAIL CIRCUITS</td><td rowspan="3">Malfunctioning</td><td>Relay damage</td><td rowspan="3">Lack of information for optimal distance between trains</td><td rowspan="3">-</td><td rowspan="3">IV</td><td rowspan="3">III</td><td rowspan="3">C</td><td rowspan="3">• Backup electrical generator
• Maintainance
• Periodical inspection</td></tr>
<tr><td>Defective wires</td></tr>
<tr><td>Lack of electrical power</td></tr>
<tr><td rowspan="2">Unwanted operation</td><td>Shunting problems</td><td rowspan="2">Inadequate inputs for RBC Interlocking problems</td><td rowspan="2">II</td><td rowspan="2">I</td><td rowspan="2">II</td><td rowspan="2">B</td><td rowspan="2">• Periodic sensing on the circuit capabilities</td></tr>
<tr><td>Inverted relay output</td></tr>
<tr><td rowspan="6">RAIL SWITCHES</td><td rowspan="5">Stuck rail</td><td>Weather conditions (Snow)</td><td rowspan="3">Excessive rail wear Derailments</td><td rowspan="3">I</td><td rowspan="3">I</td><td rowspan="3">II</td><td rowspan="3">D</td><td rowspan="3">• Maintainance
• Periodical inspection</td></tr>
<tr><td>Structural damage</td></tr>
<tr><td>Mechanical damage on the switch</td></tr>
<tr><td>Lack of electrical power</td><td rowspan="3">Wrong trayectory</td><td rowspan="3">-</td><td rowspan="3">IV</td><td rowspan="3">III</td><td rowspan="3">C</td><td rowspan="3">• Online sensing on switch position</td></tr>
<tr><td>Absence of input signals</td></tr>
<tr><td>Wrong configuration</td><td>Path planning</td></tr>
</table>

FMEA: Full Supervision Mode & Partial Supervision Mode

Component	Failure Mode	Failure Causes	Failure Effects	Severity T	Severity P	Severity I	Probability	Control Measures/Remarks
EuroBalises	Transmission errors	Wayside failures Air-Gap Programming	• Erroneous calibration of odometry to the reference point	II	I	II	B	• Placement distance of the eurobalises • Locking algorithms while the eurobalise is in use
	Undetectability	Structural damage Erroneously reports detection of a balise in presence of a EuroBalise	• Loss of trackability redundancy	III	III	II	D	• Maintainance • Periodical inspection • Better coding diferentiation between all the technologies
PCS	Wrong data	RBC	• Unsupervised train motion	II	I	II	B	• Redundancy and minimization of error sources from sensing
	Undesired Planning	Missing information on the schedule Human error	• Delays • System colapse	-	IV	III	C	• Implementation of robust planning programs
RBC	Inadequate I/O signals	Odometry readings Balise readings Transmission	• Wrong commands of MAs • Problems setting the distance between trains	II	I	II	B	• Redundancy of different methods and sensors • Tracking algorithm from the GSM-R communication

POLITECNICO MILANO 1863

System hazard analysis of a high speed/high capacity railway

FAULT TREE ANALYSIS

FTA: Assumptions

For the purpose of better understanding the following Fault Tree Analysis of the described system, we provide here some assumptions and observations we took in consideration drawing it up.

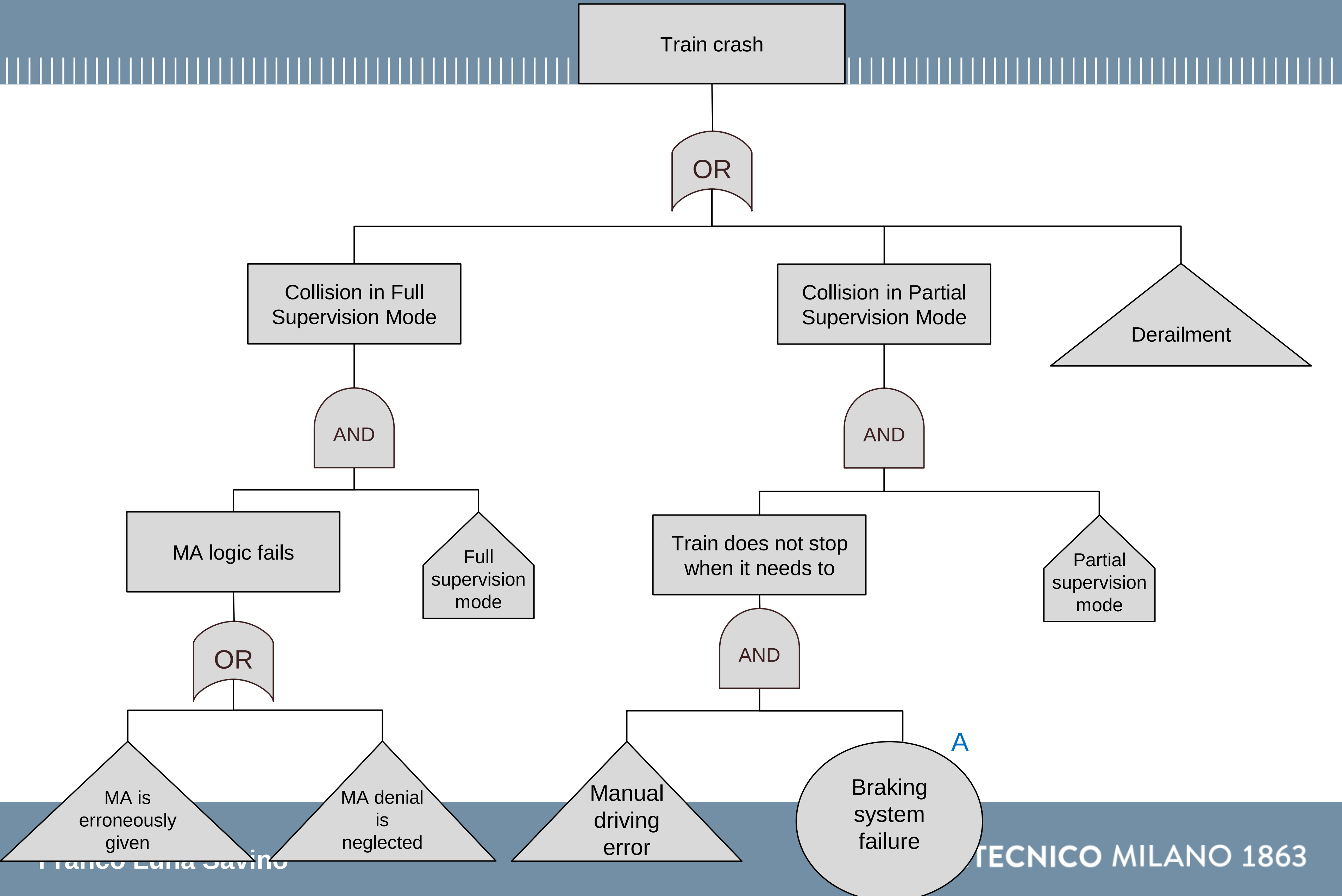
First of all, we only considered the main Top Event we are interested in, that is the *train crash*, forasmuch as it represents the most dangerous threat with the worst consequences, and for this reason the real risk to avoid; while other top events such as *wrong routing* would only led to delays and complaints by the customers.

Second, we pointed out a few communication (GSM-R system) failures, in order to give an idea to the reader of where the GSM-R system really step in the process and what are the most common issues that can arise from a malfunction. We indicated all of these failures with a yellow diamond and we did not develop any of them beyond.

Ultimately, since it can be useful when reading the tree, we remind the difference between the emergency braking system, that acts **automatically** in full supervision mode when target speeds are not respected, and the traditional braking system, activated **manually** by the train driver both in full supervision and partial supervision mode.

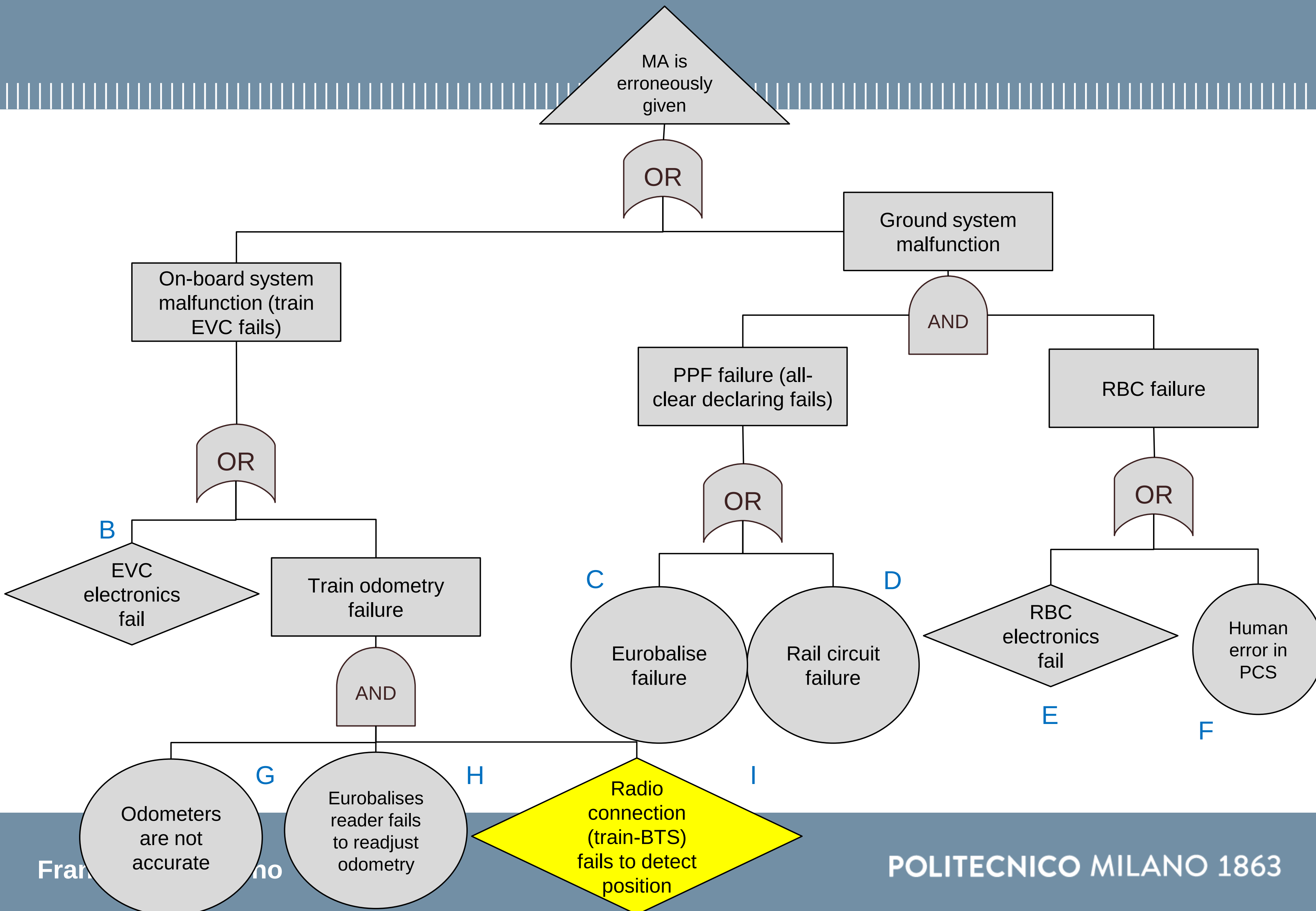
Note: probability values are mainly *reasonably imagined*, while some of them are directly provided in the papers. All of them refers to a 10 years interval.

FTA (I)

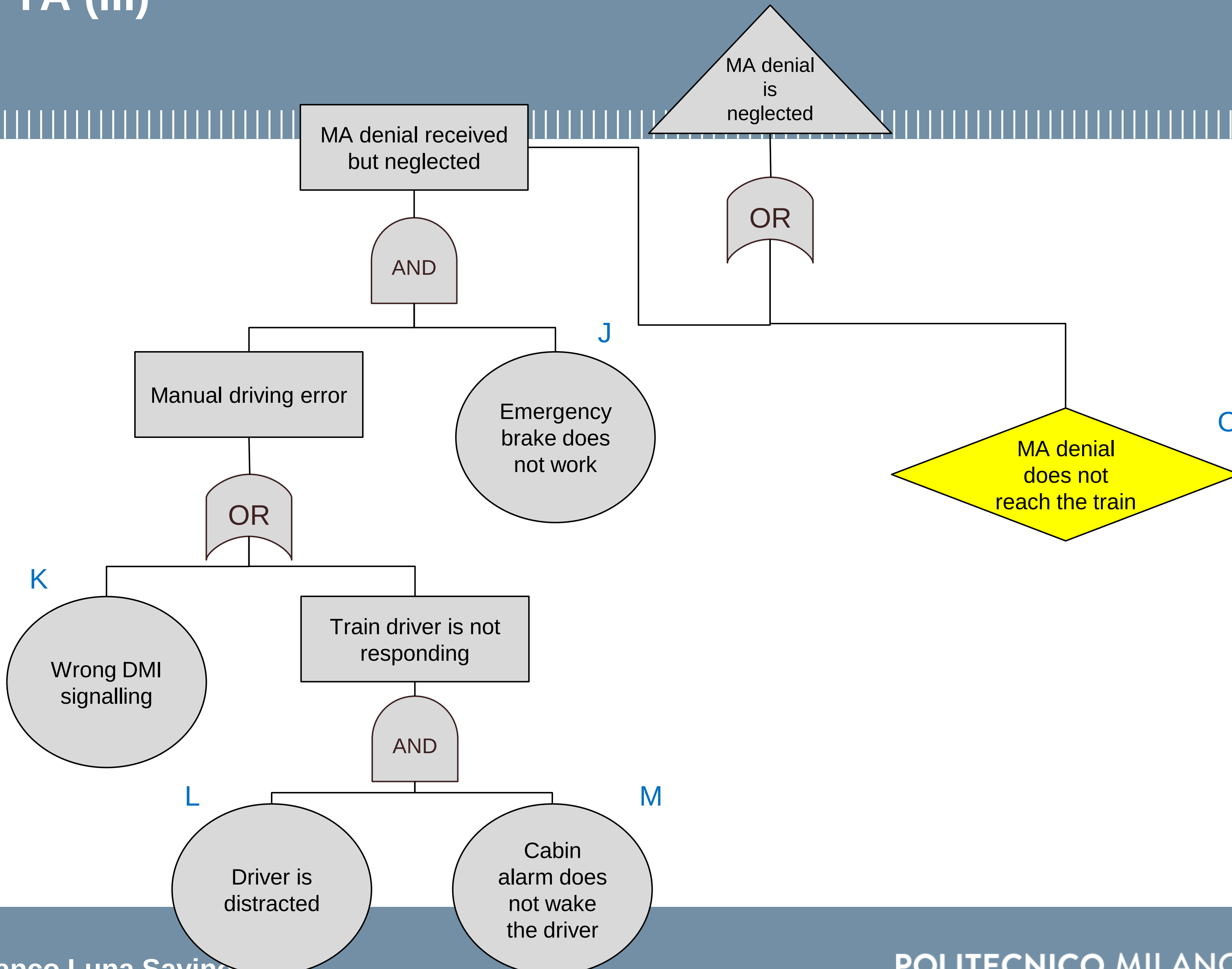


Train crash
OR
Collision in Full Supervision Mode
Collision in Partial Supervision Mode
Derailment
AND
AND
MA logic fails
Full supervision mode
Train does not stop when it needs to
Partial supervision mode
OR
AND
MA is erroneously given
MA denial is neglected
Manual driving error
A
Braking system failure

FTA (II)

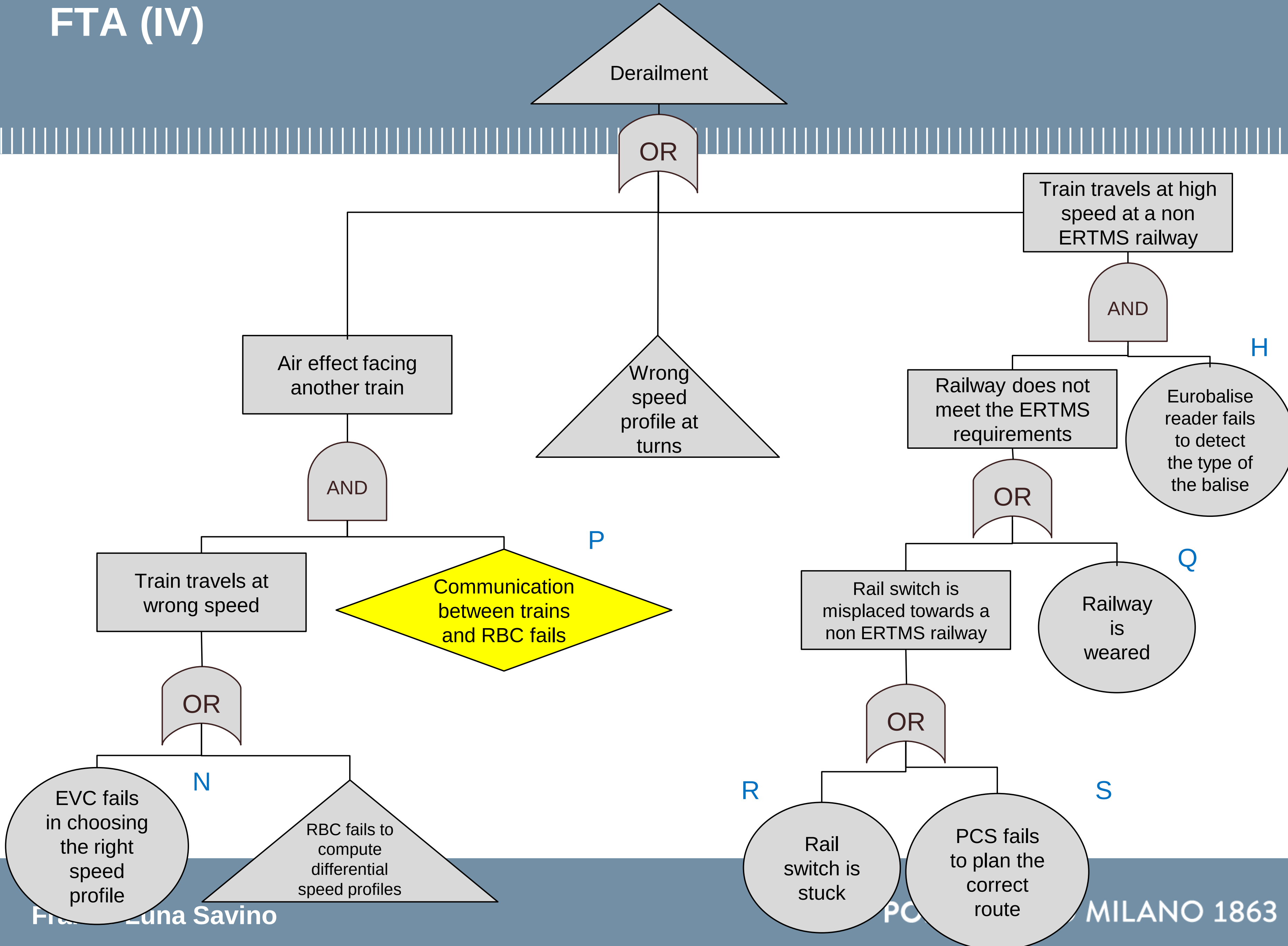

MA is erroneously given
OR
Ground system malfunction
On-board system malfunction (train EVC fails)
AND
PPF failure (all-clear declaring fails)
RBC failure
OR
OR
OR
B
EVC electronics fail
Train odometry failure
C
D
Eurobalise failure
Rail circuit failure
RBC electronics fail
Human error in PCS
E
F
AND
G
H
I
Odometers are not accurate
Eurobalises reader fails to readjust odometry
Radio connection (train-BTS) fails to detect position

FTA (III)

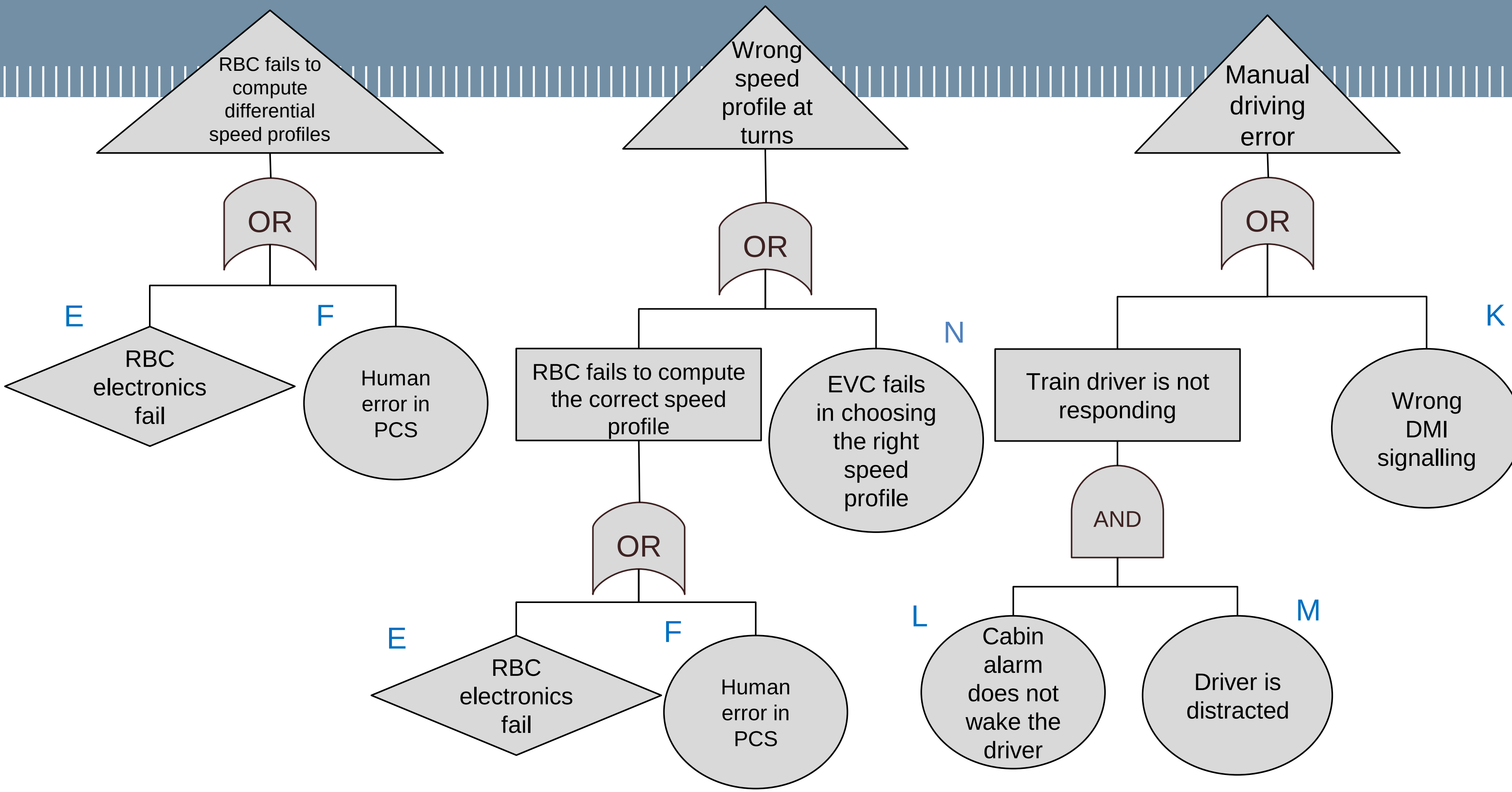


MA denial
is
neglected
OR
MA denial received
but neglected
AND
Manual driving error
J
Emergency
brake does
not work
O
MA denial
does not
reach the train
OR
K
Wrong DMI
signalling
Train driver is not
responding
AND
L
Driver is
distracted
M
Cabin
alarm does
not wake
the driver

FTA (IV)


Derailment
OR
Train travels at high speed at a non ERTMS railway
AND
H
Air effect facing another train
Wrong speed profile at turns
Railway does not meet the ERTMS requirements
Eurobalise reader fails to detect the type of the balise
AND
OR
P
Q
Train travels at wrong speed
Communication between trains and RBC fails
Rail switch is misplaced towards a non ERTMS railway
Railway is weared
OR
OR
N
R
S
EVC fails in choosing the right speed profile
RBC fails to compute differential speed profiles
Rail switch is stuck
PCS fails to plan the correct route

FTA (V)


RBC fails to compute differential speed profiles
OR
E
RBC electronics fail
F
Human error in PCS
Wrong speed profile at turns
OR
RBC fails to compute the correct speed profile
OR
E
RBC electronics fail
F
Human error in PCS
N
EVC fails in choosing the right speed profile
Manual driving error
OR
Train driver is not responding
AND
L
Cabin alarm does not wake the driver
M
Driver is distracted
K
Wrong DMI signalling

FTA: Probability (I)

Independent Events:

Event, i	Event Name, i	Probability, P(i)
A	Braking system failure	0.00005
B	EVC electronics fail	0.0000001
C	Eurobalise failure	0.00005
D	Rail circuit failure	0.00005
E	RBC electronic fail	0.0000008
F	Human error in PCS	0.0000009
G	Odometers are not accurate	0.00009
H	Eurobalise reader failure	0.000001
I	Radio connection (train-BTS) fails to detect position	0.00002
J	Emergency brake does not work	0.00008
K	Wrong DMI signalling	0.000003
L	Cabin alarm does not wake the driver	0.00003
M	Driver is distracted	0.00005
N	EVC fails in choosing the right speed profile	0.0000009
O	MA denial does not reach the train	0.0000004
P	Communication between trains and rbc fails	0.000006
Q	Railway is weared	0.00009
R	Rail switch is stuck	0.00006
S	PCS fails to plan the correct route	0.00004

FTA: Probability (II)

Top Event (T):

P(T)= P[(LM+K)A] + P[(LM+K)J+O+(GHI)+B+(C+D)(E+F)] + P[(R+S+Q)H +(E+F+N)P+(E+F+N)]

Minimal cut sets:

1(Partial supervision) - LMA+KA

2(Full supervision) - LMJ+KJ+O+GHI+B+CE+CF+DE+DF

3(Derailment) - RH+SH+QH+EP+PF+PN+N+E+F

FTA: Probability (III)

P(LMA) = $7.5 * 10^{-14}$
P(KA) = $1.5 * 10^{-10}$

P(LMA+KA) = 0.00000000015

P(LMJ) = $2.4 * 10^{-9}$
P(KJ) = $2.4 * 10^{-10}$
P(O) = 0.0000004
P(GHI) = $1.8 * 10^{-15}$
P(B) = 0.0000001
P(CE) = $4 * 10^{-11}$
P(DE) = $4 * 10^{-11}$
P(EF) = $7.2 * 10^{-13}$
P(CF) = $4.5 * 10^{-11}$

P(LMJ+KJ+O+GHI+B+CE+CF+DE+DF) = 0.000000503

P(RH) = $6 * 10^{-11}$
P(SH) = $4 * 10^{-11}$
P(QH) = $9 * 10^{-11}$
P(EP) = $4.8 * 10^{-12}$
P(PF) = $5.4 * 10^{-12}$
P(PN) = $5.37 * 10^{-12}$
P(N) = 0.0000009
P(E) = 0.0000008
P(F) = 0.0000009

P(RH+SH+QH+EP+PF+PN+N+E+F) = 0.0000026

P(T) = 0.00000310312
= 0.00031%

FTA: Probability (IV)
Importance ranking

Method 1: $\delta P_i(T) = P_{if}(T) - P_{is}(T)$

Event i	δP_i	$\frac{\delta P_i}{\Sigma} \cdot 100$	Ranking
A	0.00000300	0.000060%	8
B	1.00000000	19.997788%	4
C	0.00000170	0.000034%	11
D	0.00000170	0.000034%	12
E	1.00010600	19.999908%	1
F	1.00010600	19.999908%	2
G	0.00000000	0.000000%	19
H	0.00019000	0.003800%	6
I	0.00000000	0.000000%	18
J	0.00000300	0.000060%	9
K	0.00013000	0.002600%	7
L	0.00000001	0.000000%	16
M	0.00000000	0.000000%	17
N	1.00000600	19.997908%	3
O	1.00000000	19.997788%	5
P	0.00000260	0.000052%	10
Q	0.00000100	0.000020%	14
R	0.00000100	0.000020%	13
S	0.00000100	0.000020%	15

The results show that the most critical events are related to the RBC and the EVC respectively, these two components fulfill the most important roles in the control system, since the RBC is in charge of sending commands while the EVC collects the information and execute the commands received. The design of those components have a lot of considerations on robustness and redundancy that are not discussed due to the level of analysis that is considered for this project. However, in accordance to the standards used in the ERTMS there is a special consideration towards the power supply units and the reliability of the information.

POLITECNICO MILANO 1863

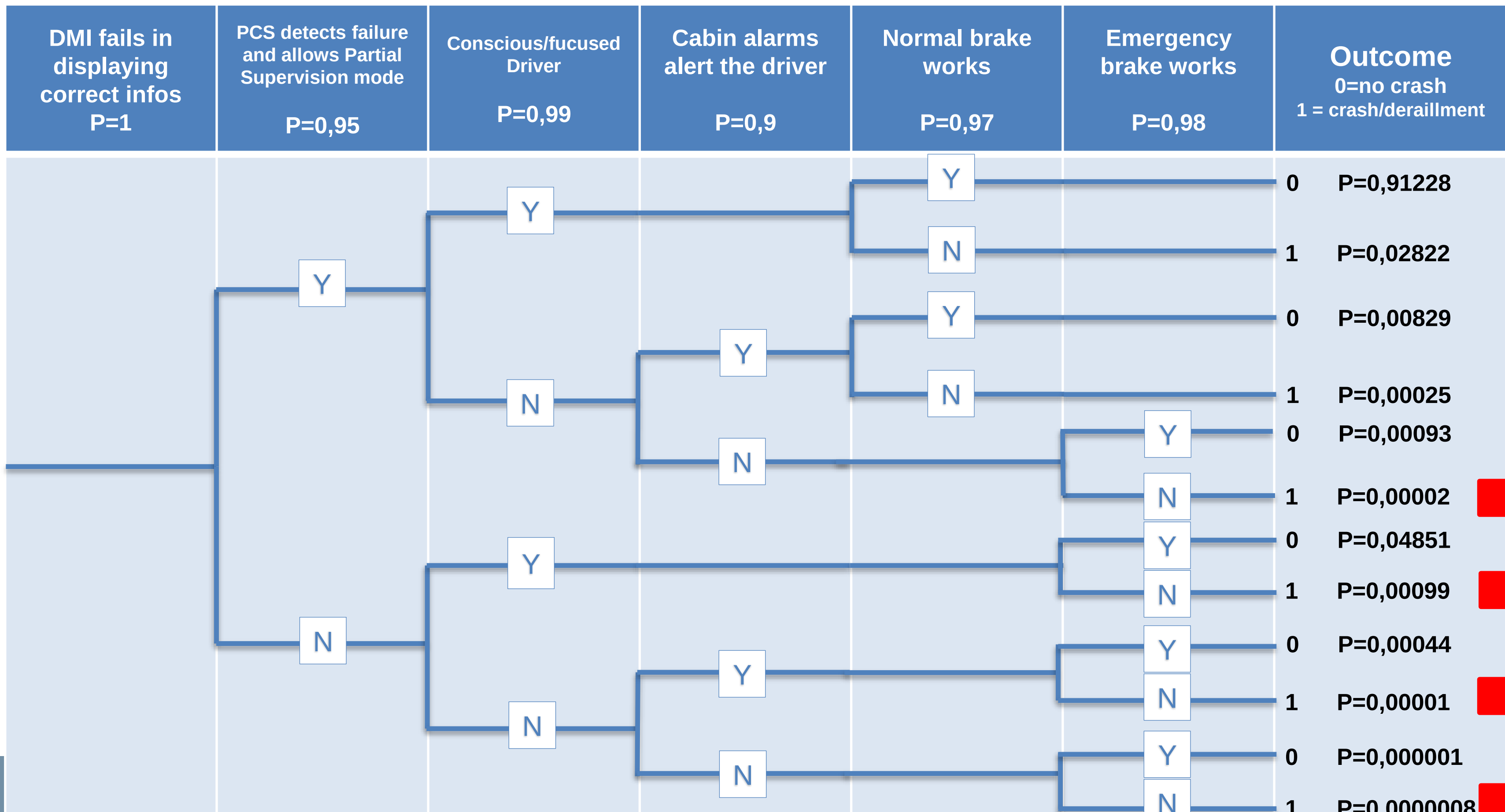
System hazard analysis of a high speed/high capacity railway

EVENT TREE ANALYSIS

ET (I)
Initiating event: DMI malfunction

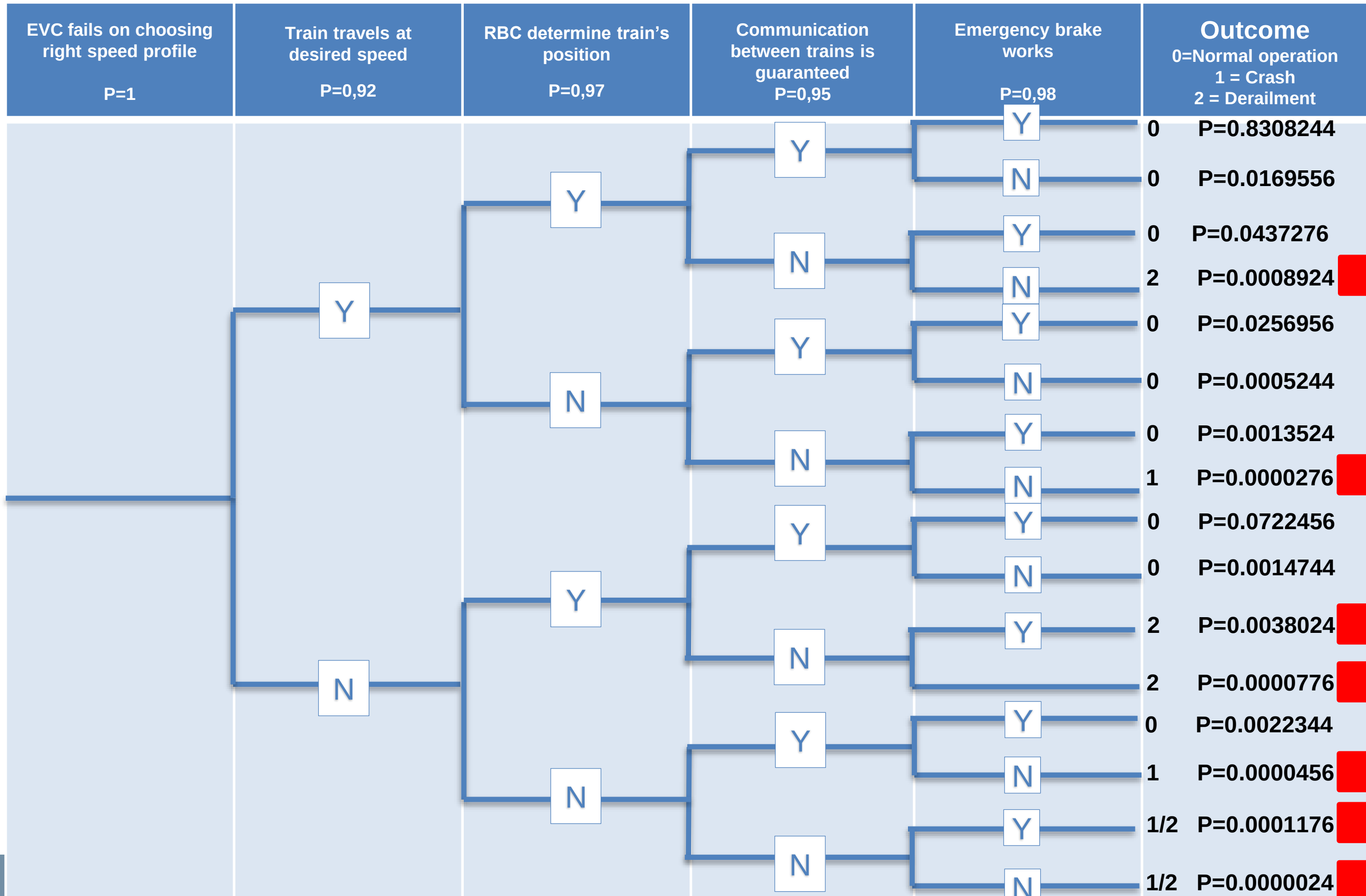
Note: In Partial Supervision mode speed is limited to 30/50 km/h so an eventual crash will not have severe consequences apart from the deriving delays on the line. The crashes at full speed are marked with a red square.

When operating at full speed, the driver is assisted by the DMI in order to maintain the train at the right speed at any time so that, if obstacles are detected outside his field of view, he is warn to brake *before* the *emergency braking point* in order to stop the train gently. Assuming the communication infrastructure works properly, a series of malfunctions can lead to risky situations if the driver is not assisted by the DMI. (Note that in Part. Sup. (authorized by the PCS and activated by the driver) the emergency brake is deactivated, while in Full Sup. the driver is not invited to brake through the traditional system because of the DMI failure)



ET (II)
Initiating event: EVC Error

The EVC (Euro Vital Computer) is the most important part for the ETCS onboard system since this computer is the one that manage all the information received by the different sources such as sensors, DMI and the data from the GSM-R communication tunnel in order to have a layer of logic that controls and protect the train system. This device is critical for the right operation on full-supervision mode, since a malfunction on this device will lead to an uncontrolled movement of the train. As previously stated, the level of analysis of this project does not allow to describe all the considerations related to safety on this device. This event tree analysis just consider the full supervision mode since the partial supervision mode analysis leads to a similar tree that was previously discussed.



POLITECNICO
MILANO 1863

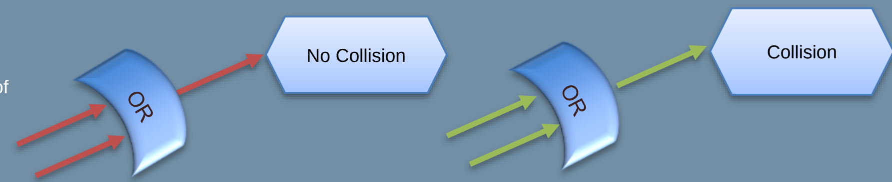
System hazard analysis of a high speed/high capacity railway

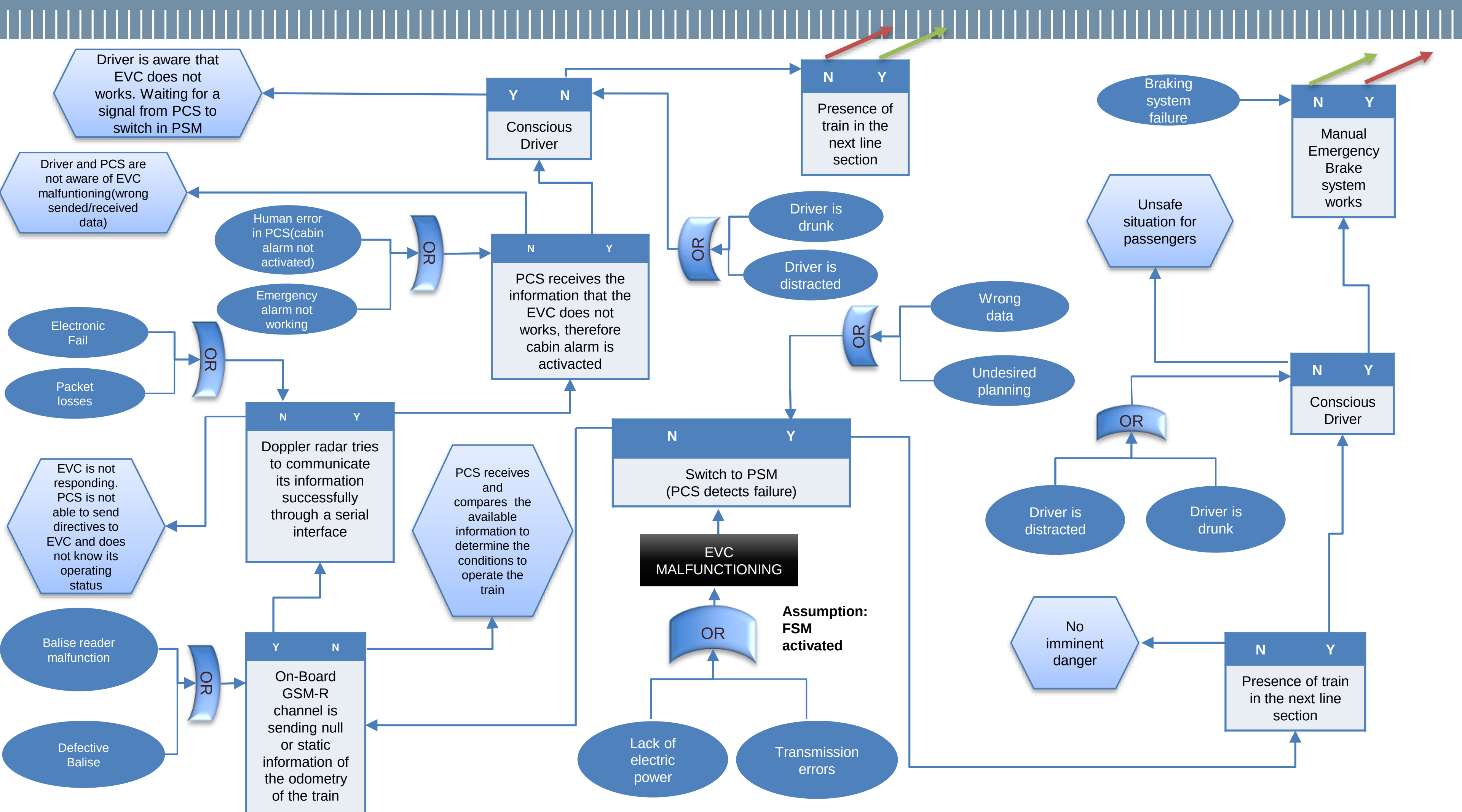
CAUSE CONSEQUENCE ANALYSIS

CCA(I)

Assumptions:
- GSM-R communication always working
- Doppler radar sensor is a redundant speed sensor that communicate its info on the serial interface for a high level of security(it does not depend on EVC)

Initiating event: EVC MALFUNCTION





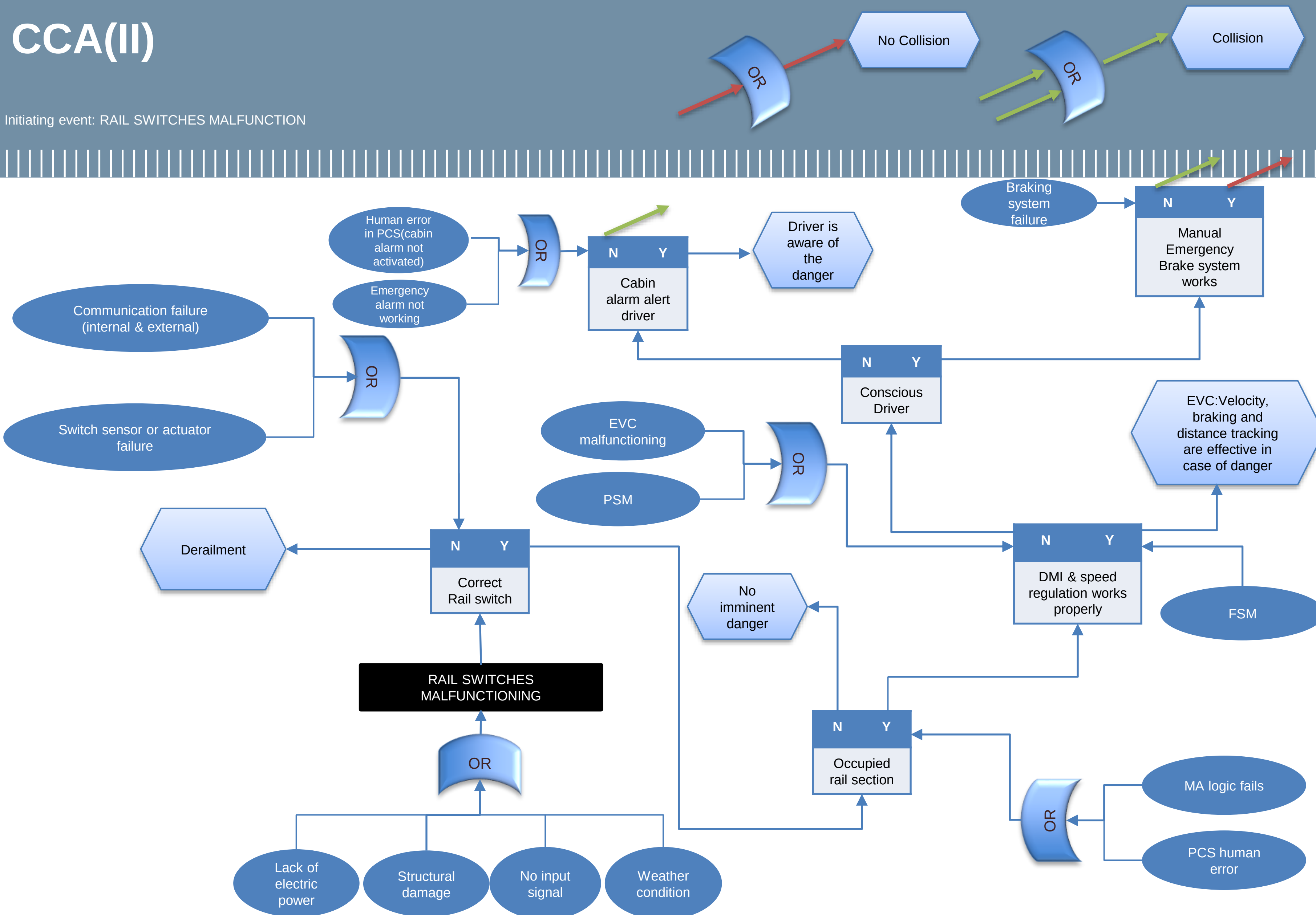
Franco Luna Savino

Notice: EVC malfunction implies:
- DMI malfunction
- Erroneous MA received
- Odometry subsystem cannot be read

POLITECNICO MILANO 1863

CCA(II)

Initiating event: RAIL SWITCHES MALFUNCTION



POLITECNICO
MILANO 1863

System hazard analysis of a high speed/high capacity railway

CONCLUSIONS

Conclusions (I)

First of all, we stress that we are dealing with a system with very dangerous operational speeds to be respected that each day is employed by a very large number of users, so the development of the ETCS and ERTMS standards has been yet studied and designed with very high safety standards and robustness, which are also precisely described in the papers, explicitly following the statement «every new system must at least guarantee the same safety level of the previous one operating at present time.»

From all the analysis we have made, we found out that an eventual EVC failure is potentially the most critical issue that can lead to a series of miscomunications between train and driver and train and ground-system that in the end, following a inaccurate path of actions regarding the railway management, will conduce to catastrophic crashes.

According to the present standards, the safety measures that are considered are mainly regarding the communication between the different modules of the EVC and its power supply, in fact reduntant buses and emergency power suppliers are currently used (like they are used in the general power supply system along all the line).

Conclusions (II)

In order to sensibily reduce the risks connected to this main problem, a possible solution could be decentralize the on-board system (even though maintaining all the function on-board) so that not all the functionalities of the train sensoring and controlling remain related to the EVC. By this way, redundancies and avoidance of eventual on-board system failures would be easier to implement. A drawback would surely be that the system complexity would increase and become more difficult to design and maintain.

An increase in the overall safety levels can lead to a more comfortable experience for the passengers and to a general reduction of travel times with the increase of the average reliable speed, since with more solid safety standards the conditions which require the Partial Supervision Mode will substantially decrease.

POLITECNICO MILANO 1863

System hazard analysis of a high speed/high capacity railway

REFERENCES and SOURCES

References: Bibliography and Videography

Bibliography:

- Course material, prof. Riccardo Scattolini;
- Transportation Systems Reliability and Safety, B.S. Dhillon. (14/02/2011)
- Specifica Requisiti Funzionali del Sistema di “Controllo Automatico della Marcia del Treno” per la Linea AV RM-NA. (28/02/2001);
- Linea AV Roma-Napoli – Modalità funzionale per l’attivazione dell’ERTMS/ETCS L2. (17-11-2004) ;
- Linea AV Roma-Napoli – Sistema di Comando/Controllo della Marcia dei Treni ERTMS/ETCS L2. (21/03/2002);
- Linea AV Roma-Napoli – Sistema di Comando/Controllo della Marcia dei Treni ERTMS/ETCS L2 – Appendice A – Architettura GSM-R di fase 1. (21/03/2002);
- «European Train Control System». Wikipedia, The free encyclopedia. https://en.wikipedia.org/wiki/European_Train_Control_System (05/11/2019);
- «ERMTS». Wikipedia, L’enciclopedia libera. https://it.wikipedia.org/wiki/ERTMS (30/08/2019).

Videography:

- «Il sistema AV/AC e lo sviluppo dell'ERTMS/ETCS in Italia [ITA]», Francesco Fumarola, https://www.youtube.com/watch?v=xCS9D1C7DXo;
- «Introducción a ERTMS... en 6 minutos | Exceltic», Exceltic, https://www.youtube.com/watch?v=Imi60yo6k7A;

Sources: figures

- Fig. 1 – Screenshot from «Introducción a ERTMS... en 6 minutos | Exceltic», Exceltic, https://www.youtube.com/watch?v=Imi60yo6k7A;

- Fig. 2 – «Illustration of the functioning of ETCS Level 1», François Melchior, «ERMTS». Wikipedia, L'enciclopedia libera. https://it.wikipedia.org/wiki/ERTMS (30/08/2019).

- Fig. 3 – «Illustration of the functioning of ETCS Level 2», François Melchior, «ERMTS». Wikipedia, L'enciclopedia libera. https://it.wikipedia.org/wiki/ERTMS (30/08/2019).

- Fig. 4 – Screenshot from «Il sistema AV/AC e lo sviluppo dell'ERTMS/ETCS in Italia [ITA]», Francesco Fumarola, https://www.youtube.com/watch?v=xCS9D1C7DXo;

- Fig. 6 – Adapted from «Segnali Ferroviari», Martino Antonio, «ERMTS». Wikipedia, L'enciclopedia libera. https://it.wikipedia.org/wiki/ERTMS (30/08/2019).