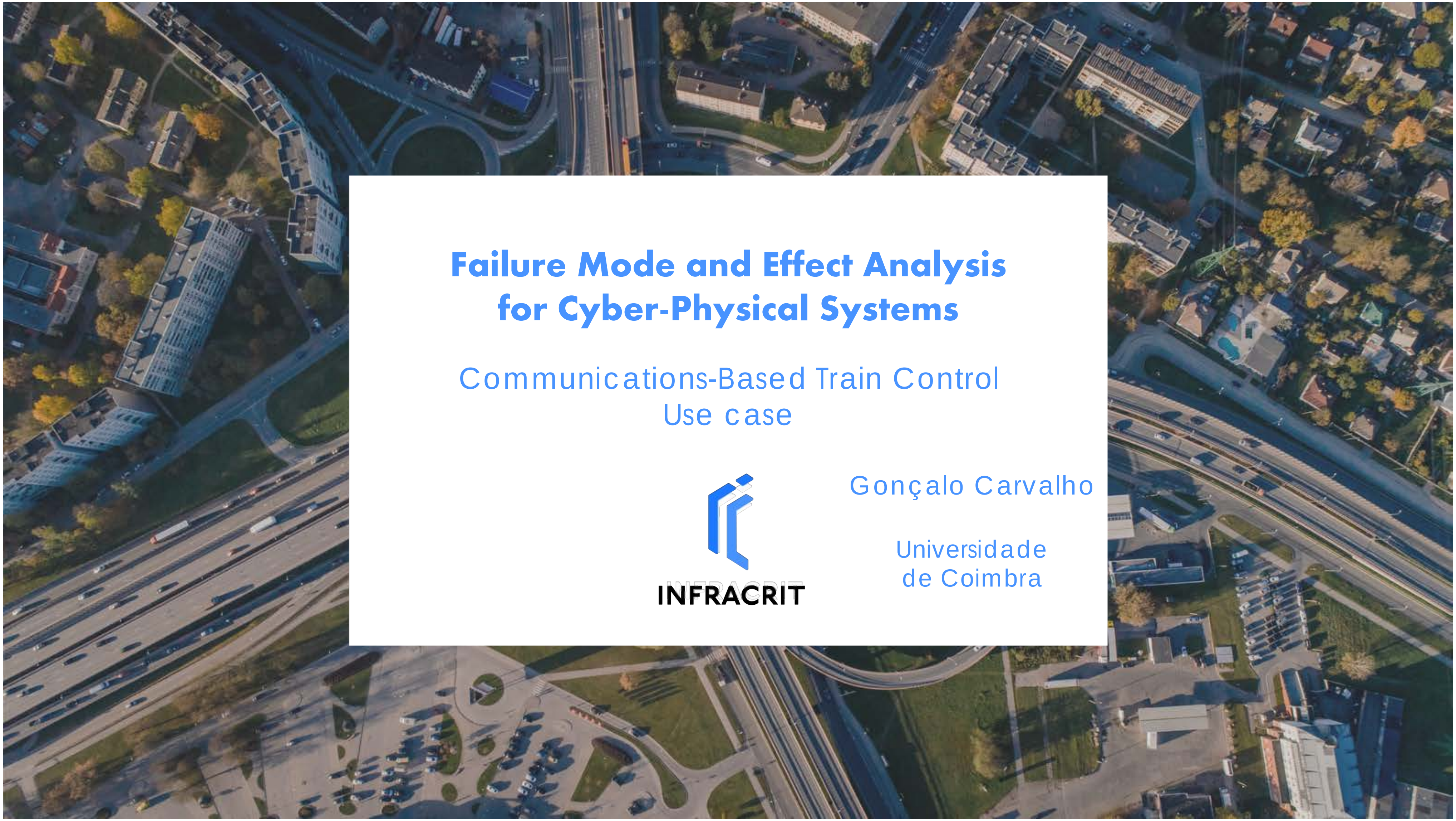


Failure Mode and Effect Analysis for Cyber-Physical Systems

Communications-Based Train Control Use case

INFRACRIT

Gonçalo Carvalho

Universidade de Coimbra

Agenda

01. Failure Mode and Effect Analysis (FMEA)

02. FMEA Drawbacks

03. New Risk Priority Number criteria and formula

04. Communications-Based Train Control (CBTC)

05. FMEA applied to CBTC

06. Conclusions and Future Work

01.

Failure Mode and Effect Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA)

- Engineering method designed to define, identify, and present solutions for system failures, problems, or errors.
- FMEA has five fundamental steps:
  - system subdivision
  - failure modes identification
  - RPN calculation
  - prevention actions recording
  - analysis reporting
- Identifies necessary decisions to prevent individual system failures and establish the risk priorities of failure modes through the Risk Priority Number (RPN).

FMEA – 5 steps

- System subdivision
- Failure modes identification
- RPN calculation
- Prevention actions recording
- Analysis reporting

FMEA – 5 steps

- System subdivision
- Failure modes identification
- RPN calculation
- Prevention actions recording
- Analysis reporting

FMEA – 5 steps

- System subdivision
- Failure modes identification
- RPN calculation
- Prevention actions recording
- Analysis reporting

RPN = Severity * Occurrence * Detectability

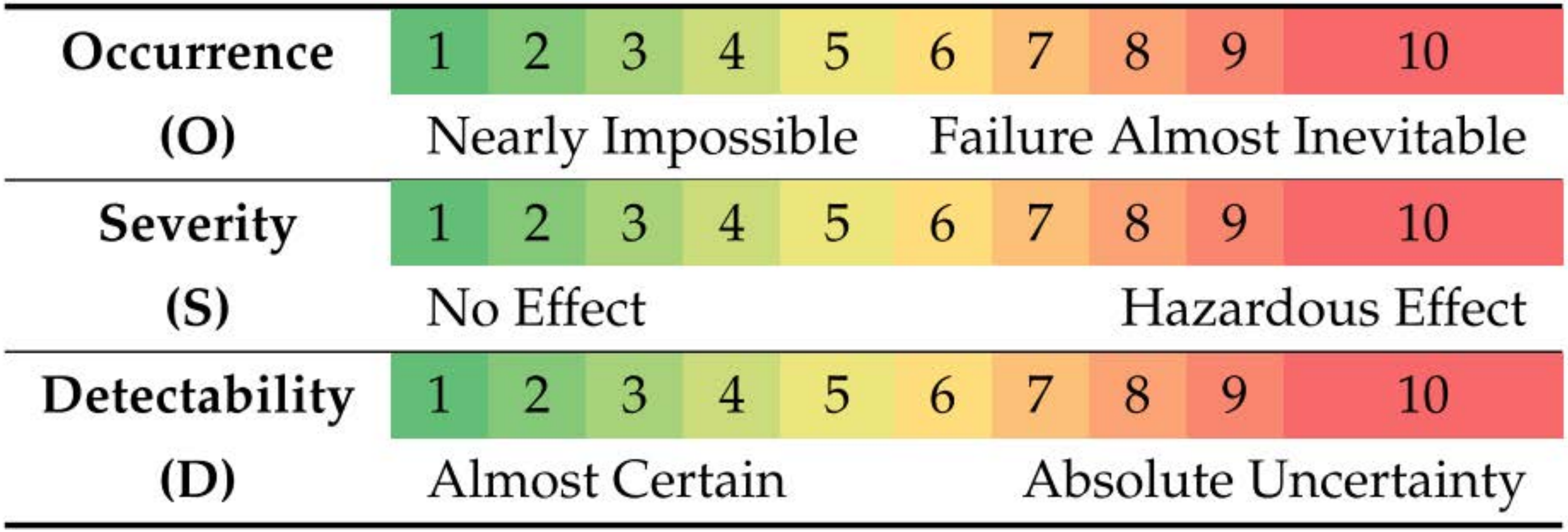
FMEA – 5 steps

- System subdivision
- Failure modes identification
- RPN calculation
- Prevention actions recording
- Analysis reporting

FMEA – 5 steps

- System subdivision
- Failure modes identification
- RPN calculation
- Prevention actions recording
- Analysis reporting

FMEA RPN calculation variables



Occurrence	1	2	3	4	5	6	7	8	9	10
(O)	Nearly Impossible					Failure Almost Inevitable				
Severity	1	2	3	4	5	6	7	8	9	10
(S)	No Effect									Hazardous Effect
Detectability	1	2	3	4	5	6	7	8	9	10
(D)	Almost Certain									Absolute Uncertainty

FMEA Drawbacks

- Bounded to the design limitations, such as the granularity
- Only considers failure modes regardless of its origin and the associated mechanisms
- Subjective, depending on the study team's experience

FMEA Drawbacks

- RPN has enormous gaps in ranges, it generates as just 120 of 1000 numbers
- Equal values of RPN are obtained from several combinations of diverse factors
- Does not have associated cost in the analysis
- Does not consider environmental or external damages to the system

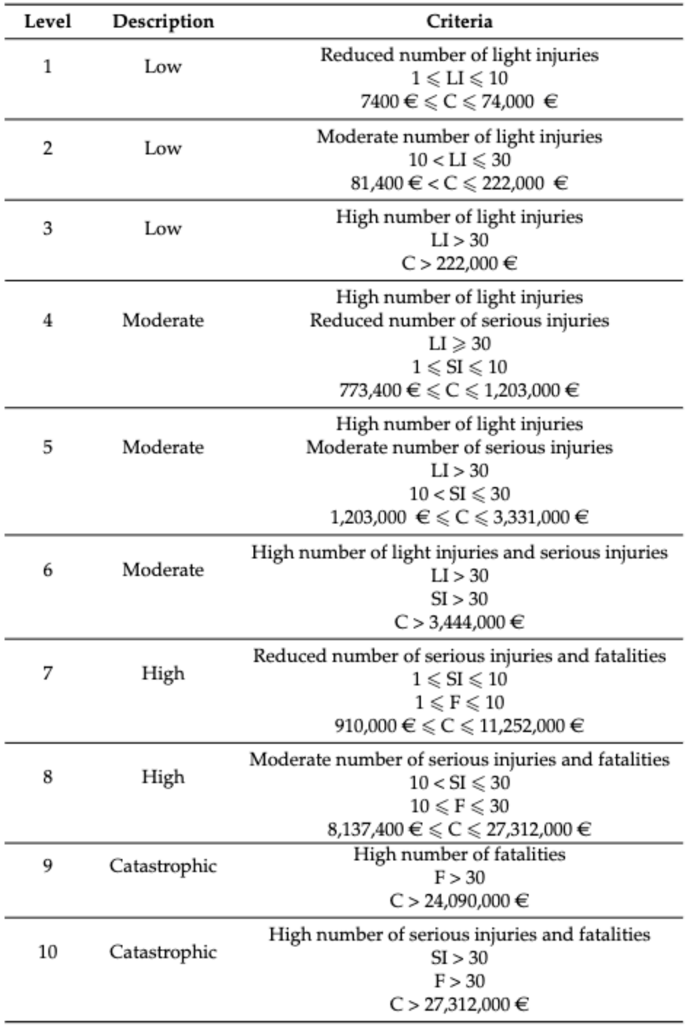
03.

New Risk Priority Number criteria and formula

New RPN Criteria and Formula

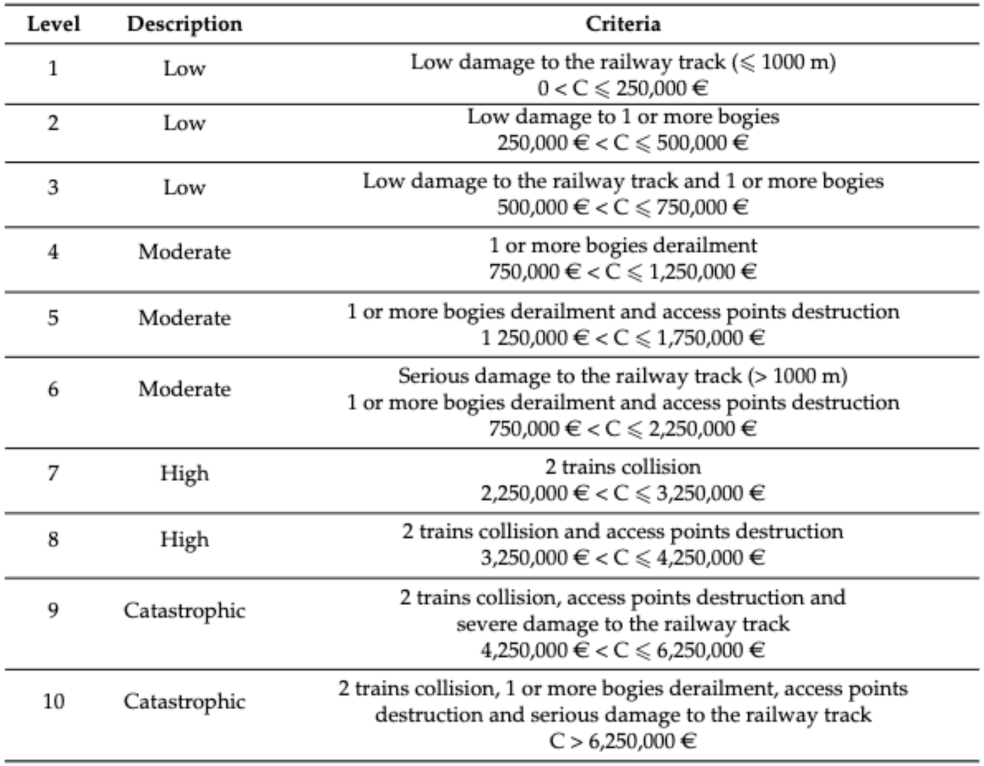
- Our goal is to assess the risk of different system failure modes based on the economic impact they represent.
    - Social
    - Infrastructural
    - Environmental
    - Delay

New RPN Criteria and Formula – Social Factor



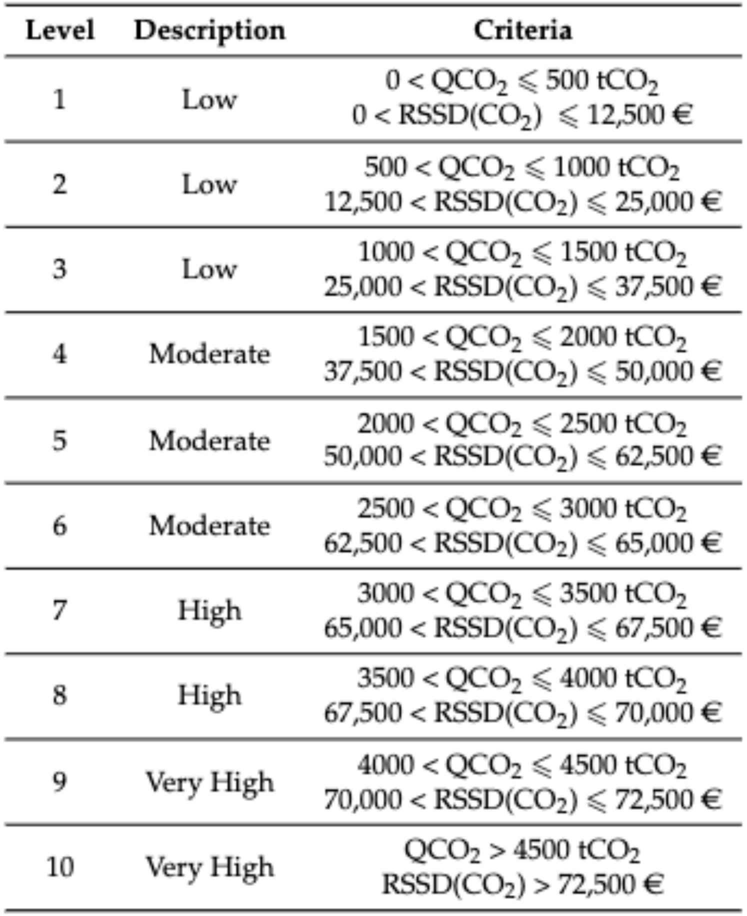
Level	Description	Criteria
1	Low	Reduced number of light injuries $1 \leqslant LI \leqslant 10$ $7400\text{ €} \leqslant C \leqslant 74{,}000\text{ €}$
2	Low	Moderate number of light injuries $10 < LI \leqslant 30$ $81{,}400\text{ €} < C \leqslant 222{,}000\text{ €}$
3	Low	High number of light injuries $LI > 30$ $C > 222{,}000\text{ €}$
4	Moderate	High number of light injuries Reduced number of serious injuries $LI \geqslant 30$ $1 \leqslant SI \leqslant 10$ $773{,}400\text{ €} \leqslant C \leqslant 1{,}203{,}000\text{ €}$
5	Moderate	High number of light injuries Moderate number of serious injuries $LI > 30$ $10 < SI \leqslant 30$ $1{,}203{,}000\text{ €} \leqslant C \leqslant 3{,}331{,}000\text{ €}$
6	Moderate	High number of light injuries and serious injuries $LI > 30$ $SI > 30$ $C > 3{,}444{,}000\text{ €}$
7	High	Reduced number of serious injuries and fatalities $1 \leqslant SI \leqslant 10$ $1 \leqslant F \leqslant 10$ $910{,}000\text{ €} \leqslant C \leqslant 11{,}252{,}000\text{ €}$
8	High	Moderate number of serious injuries and fatalities $10 < SI \leqslant 30$ $10 \leqslant F \leqslant 30$ $8{,}137{,}400\text{ €} \leqslant C \leqslant 27{,}312{,}000\text{ €}$
9	Catastrophic	High number of fatalities $F > 30$ $C > 24{,}090{,}000\text{ €}$
10	Catastrophic	High number of serious injuries and fatalities $SI > 30$ $F > 30$ $C > 27{,}312{,}000\text{ €}$

New RPN Criteria and Formula – Infrastructural Factor



Level	Description	Criteria
1	Low	Low damage to the railway track (⩽ 1000 m) $0 < C \leqslant 250{,}000$ €
2	Low	Low damage to 1 or more bogies $250{,}000$ € $< C \leqslant 500{,}000$ €
3	Low	Low damage to the railway track and 1 or more bogies $500{,}000$ € $< C \leqslant 750{,}000$ €
4	Moderate	1 or more bogies derailment $750{,}000$ € $< C \leqslant 1{,}250{,}000$ €
5	Moderate	1 or more bogies derailment and access points destruction 1 250,000 € $< C \leqslant 1{,}750{,}000$ €
6	Moderate	Serious damage to the railway track (> 1000 m) 1 or more bogies derailment and access points destruction $750{,}000$ € $< C \leqslant 2{,}250{,}000$ €
7	High	2 trains collision $2{,}250{,}000$ € $< C \leqslant 3{,}250{,}000$ €
8	High	2 trains collision and access points destruction $3{,}250{,}000$ € $< C \leqslant 4{,}250{,}000$ €
9	Catastrophic	2 trains collision, access points destruction and severe damage to the railway track $4{,}250{,}000$ € $< C \leqslant 6{,}250{,}000$ €
10	Catastrophic	2 trains collision, 1 or more bogies derailment, access points destruction and serious damage to the railway track $C > 6{,}250{,}000$ €

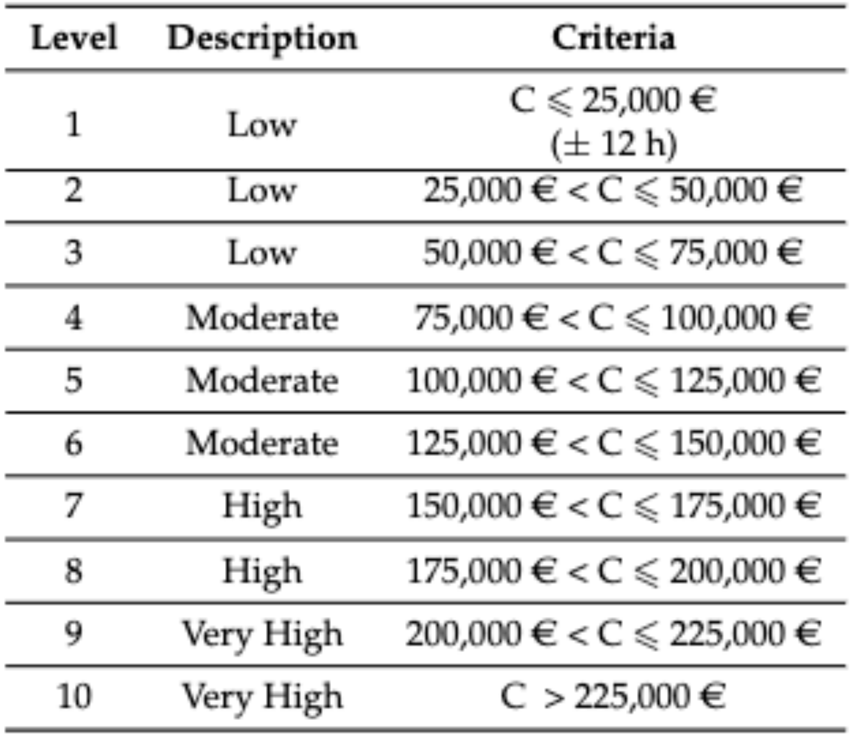
New RPN Criteria and Formula – Environmental Factor



Level	Description	Criteria
1	Low	$0 < QCO_2 \leqslant 500\ tCO_2$ $0 < RSSD(CO_2) \leqslant 12{,}500$ €
2	Low	$500 < QCO_2 \leqslant 1000\ tCO_2$ $12{,}500 < RSSD(CO_2) \leqslant 25{,}000$ €
3	Low	$1000 < QCO_2 \leqslant 1500\ tCO_2$ $25{,}000 < RSSD(CO_2) \leqslant 37{,}500$ €
4	Moderate	$1500 < QCO_2 \leqslant 2000\ tCO_2$ $37{,}500 < RSSD(CO_2) \leqslant 50{,}000$ €
5	Moderate	$2000 < QCO_2 \leqslant 2500\ tCO_2$ $50{,}000 < RSSD(CO_2) \leqslant 62{,}500$ €
6	Moderate	$2500 < QCO_2 \leqslant 3000\ tCO_2$ $62{,}500 < RSSD(CO_2) \leqslant 65{,}000$ €
7	High	$3000 < QCO_2 \leqslant 3500\ tCO_2$ $65{,}000 < RSSD(CO_2) \leqslant 67{,}500$ €
8	High	$3500 < QCO_2 \leqslant 4000\ tCO_2$ $67{,}500 < RSSD(CO_2) \leqslant 70{,}000$ €
9	Very High	$4000 < QCO_2 \leqslant 4500\ tCO_2$ $70{,}000 < RSSD(CO_2) \leqslant 72{,}500$ €
10	Very High	$QCO_2 > 4500\ tCO_2$ $RSSD(CO_2) > 72{,}500$ €

03. New Risk Priority Number criteria and formula

New RPN Criteria and Formula – Delay Factor

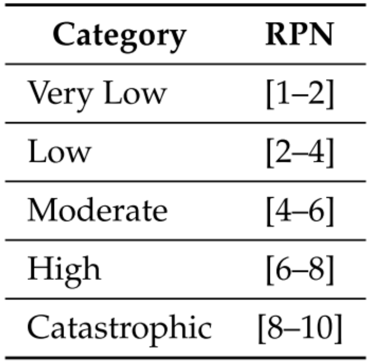


Level	Description	Criteria
1	Low	$C \leqslant 25,000$ € (± 12 h)
2	Low	25,000 € $< C \leqslant$ 50,000 €
3	Low	50,000 € $< C \leqslant$ 75,000 €
4	Moderate	75,000 € $< C \leqslant$ 100,000 €
5	Moderate	100,000 € $< C \leqslant$ 125,000 €
6	Moderate	125,000 € $< C \leqslant$ 150,000 €
7	High	150,000 € $< C \leqslant$ 175,000 €
8	High	175,000 € $< C \leqslant$ 200,000 €
9	Very High	200,000 € $< C \leqslant$ 225,000 €
10	Very High	$C >$ 225,000 €

New RPN Criteria and Formula

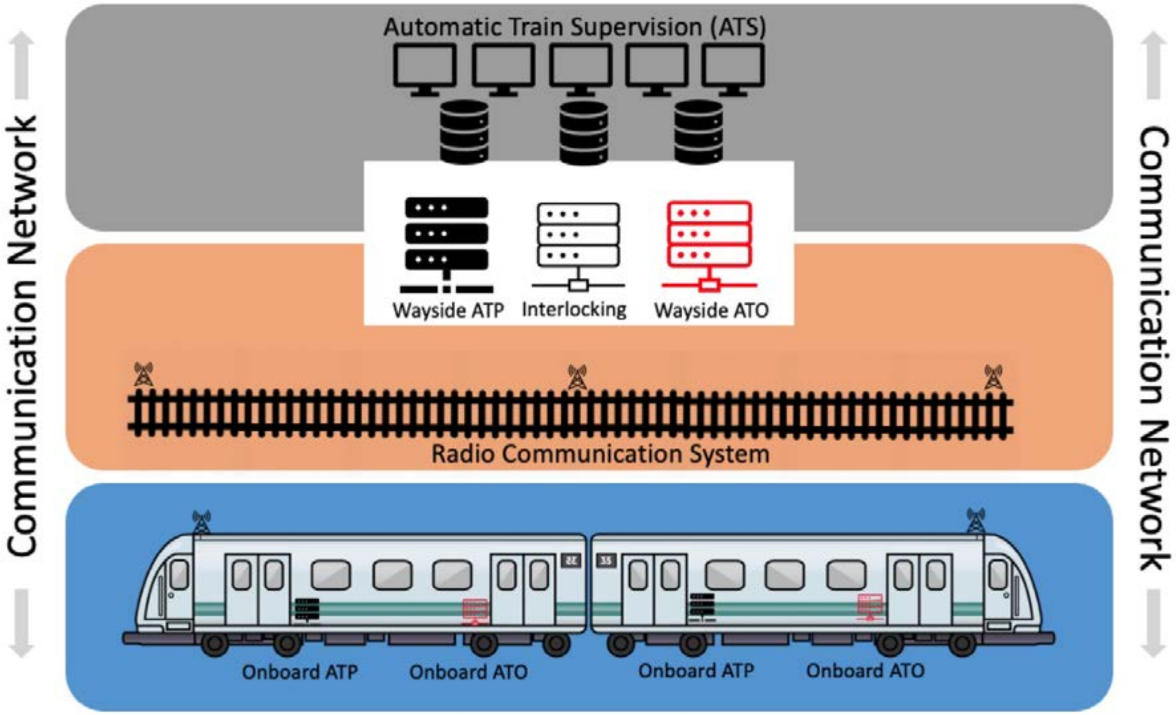
- To a final risk estimation, we propose five different categories: Very low, low, moderate, high, and catastrophic.
- RPN = SF * SFw + IF * Ifw + EF * Efw + DF * DFw
- Social Factor (SF), Infrastructure Factor (IF), Environmental Factor (EF), Delay Factor (DF), weight (w)

SF = 0.5
IF = 0.35
EF = 0.05
DF = 0.1



Category	RPN
Very Low	[1–2]
Low	[2–4]
Moderate	[4–6]
High	[6–8]
Catastrophic	[8–10]

Communications-Based Train Control (CBTC)



Communications-Based Train Control (CBTC)

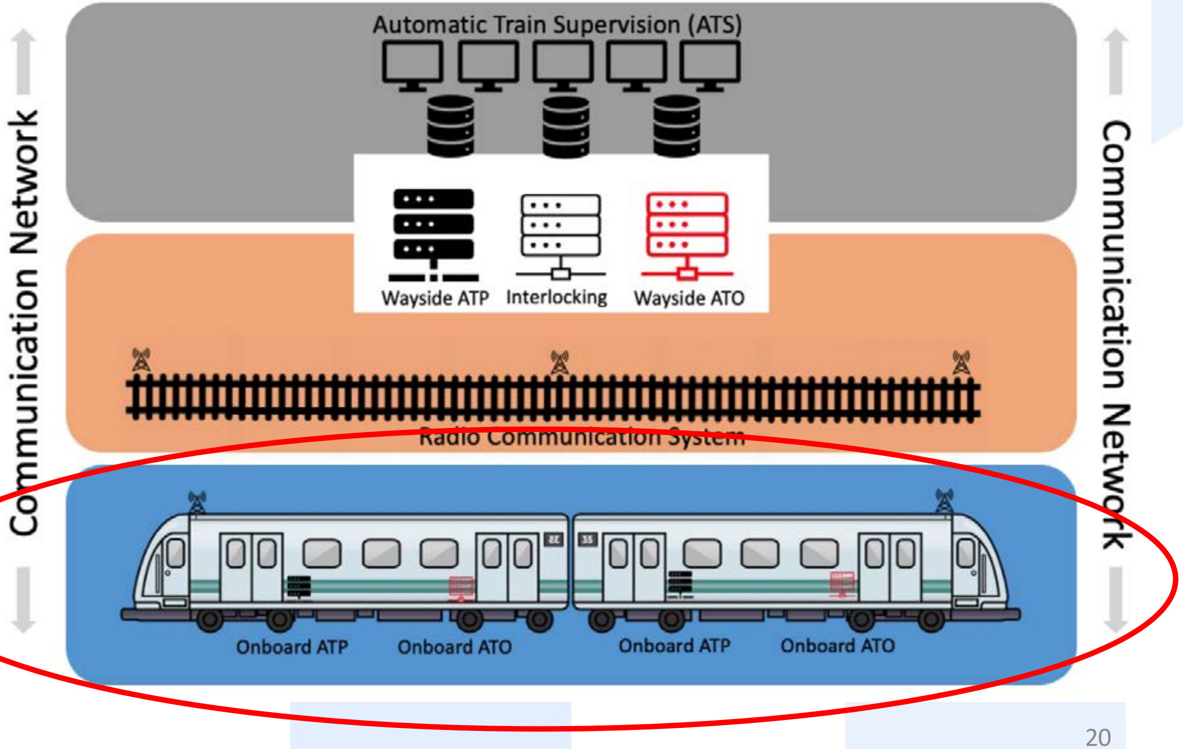
Several Cyber-Physical Systems

Is a safety and time-critical system

Dependent on data transfer

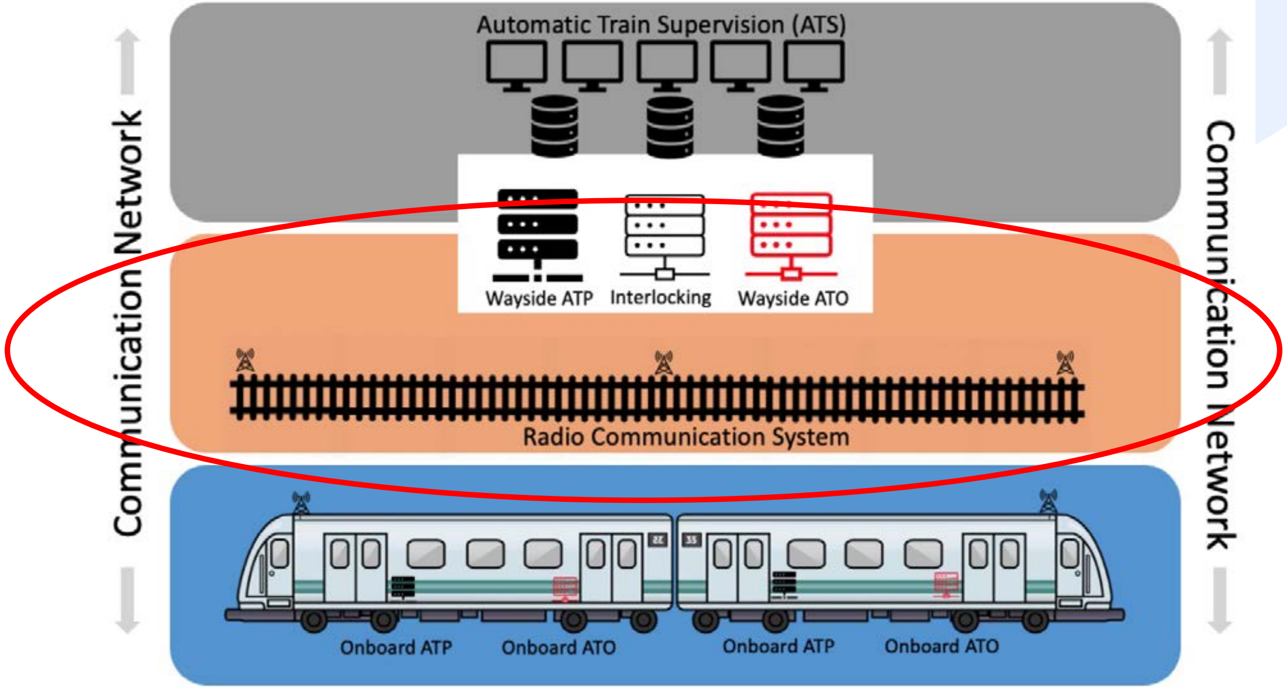
CBTC – onboard components

- Vehicle Onboard Computer (VOBC)
- Onboard Automatic Train Control (ATC):
  - Automatic Train Protection (ATP)
  - Automatic Train Operation (ATO)
- Radio Communication System (RCS)



CBTC – wayside components

- Zone Controller (ZC)
- Wayside ATP and ATO subsystems
- Computer-based Interlocking (CI)



CBTC – Cyber-security attacks

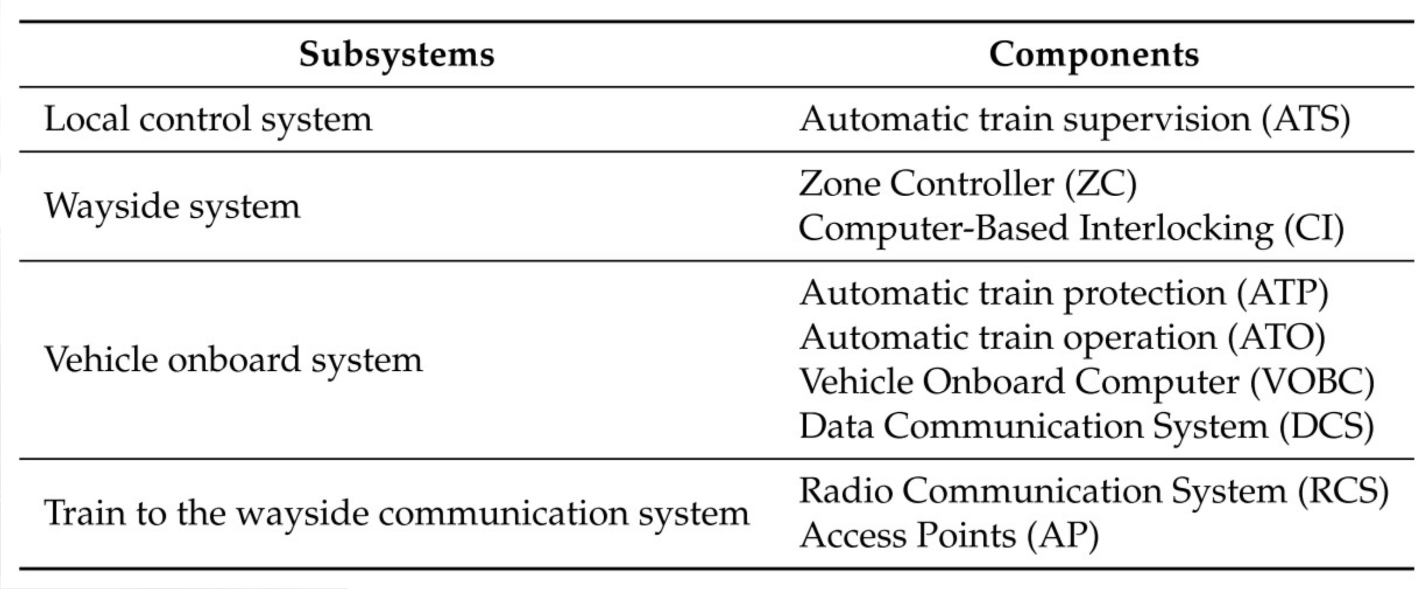
- Jamming attacks
- Man-in-the-Middle (MitM)
  - Message spoofing
  - Replay attacks

CBTC – Cyber-security defences

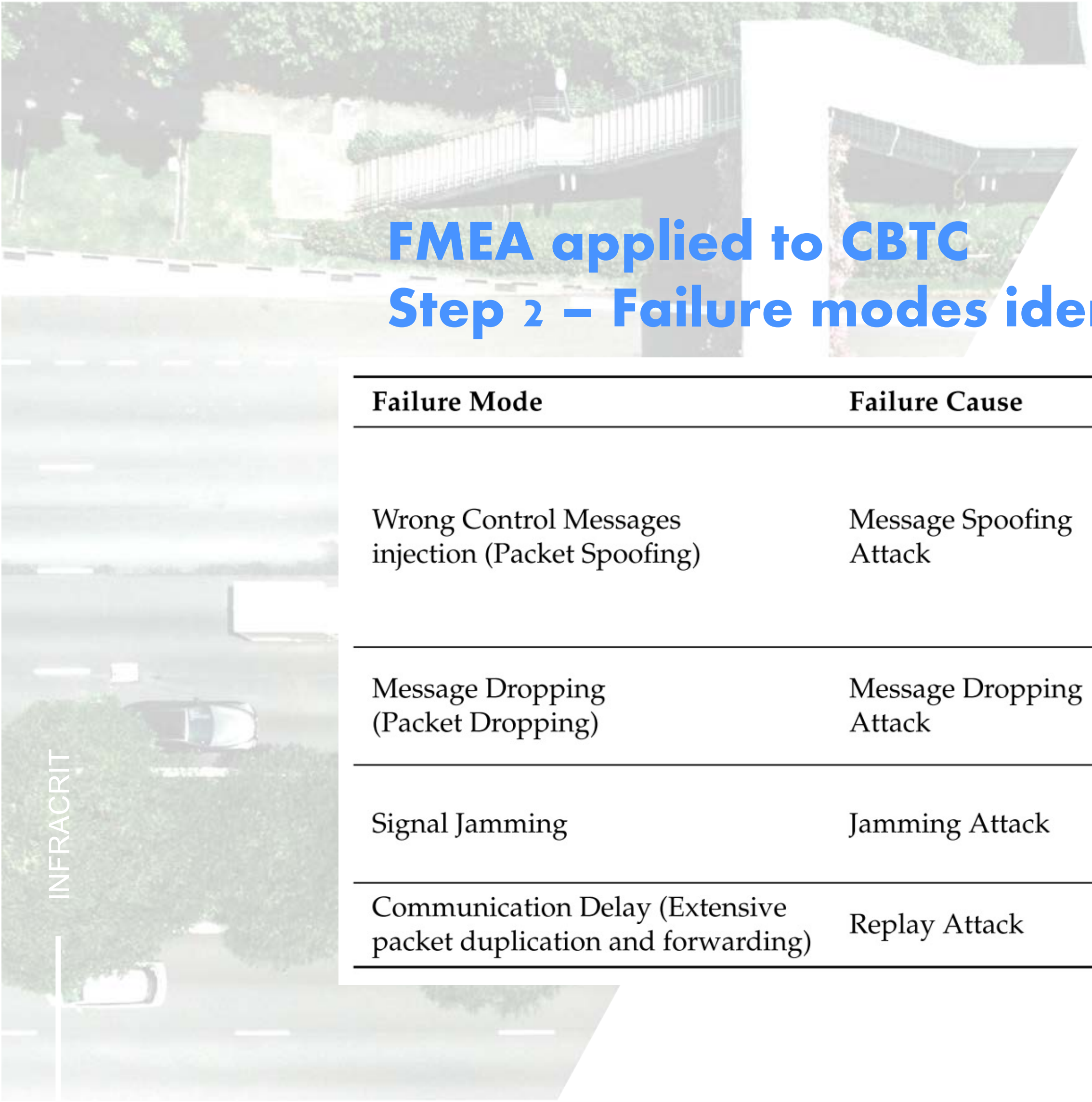
- End-to-end data encryption
- Authentication methods

- Examples:
  - Rail Radio Intrusion Detection System (RRIDS)
  - µTesla
  - Address Resolution Protocol poisoning prevention
    - MitM-Resistant ARP
  - Authenticated Acknowledgement

FMEA applied to CBTC
Step 1 – System subdivision



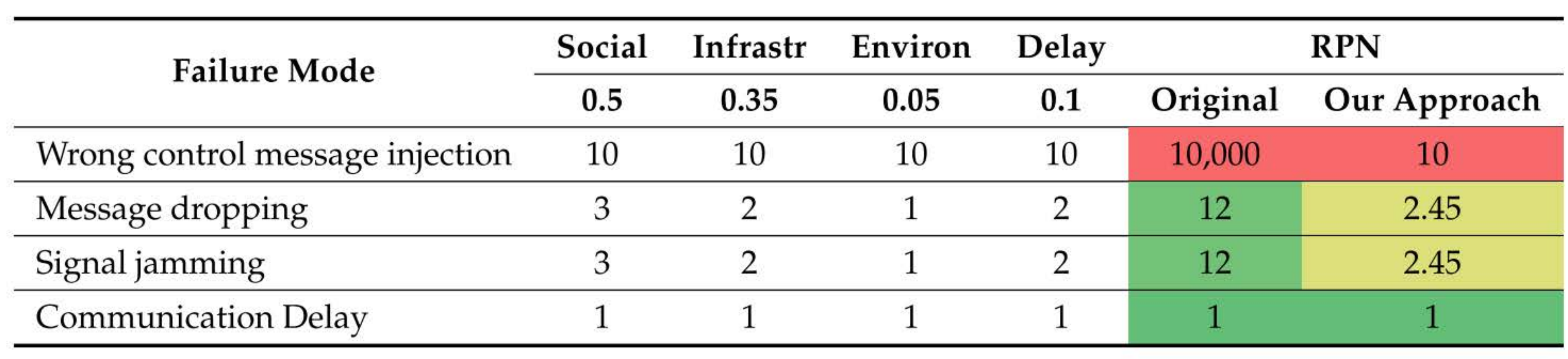
Subsystems	Components
Local control system	Automatic train supervision (ATS)
Wayside system	Zone Controller (ZC) Computer-Based Interlocking (CI)
Vehicle onboard system	Automatic train protection (ATP) Automatic train operation (ATO) Vehicle Onboard Computer (VOBC) Data Communication System (DCS)
Train to the wayside communication system	Radio Communication System (RCS) Access Points (AP)



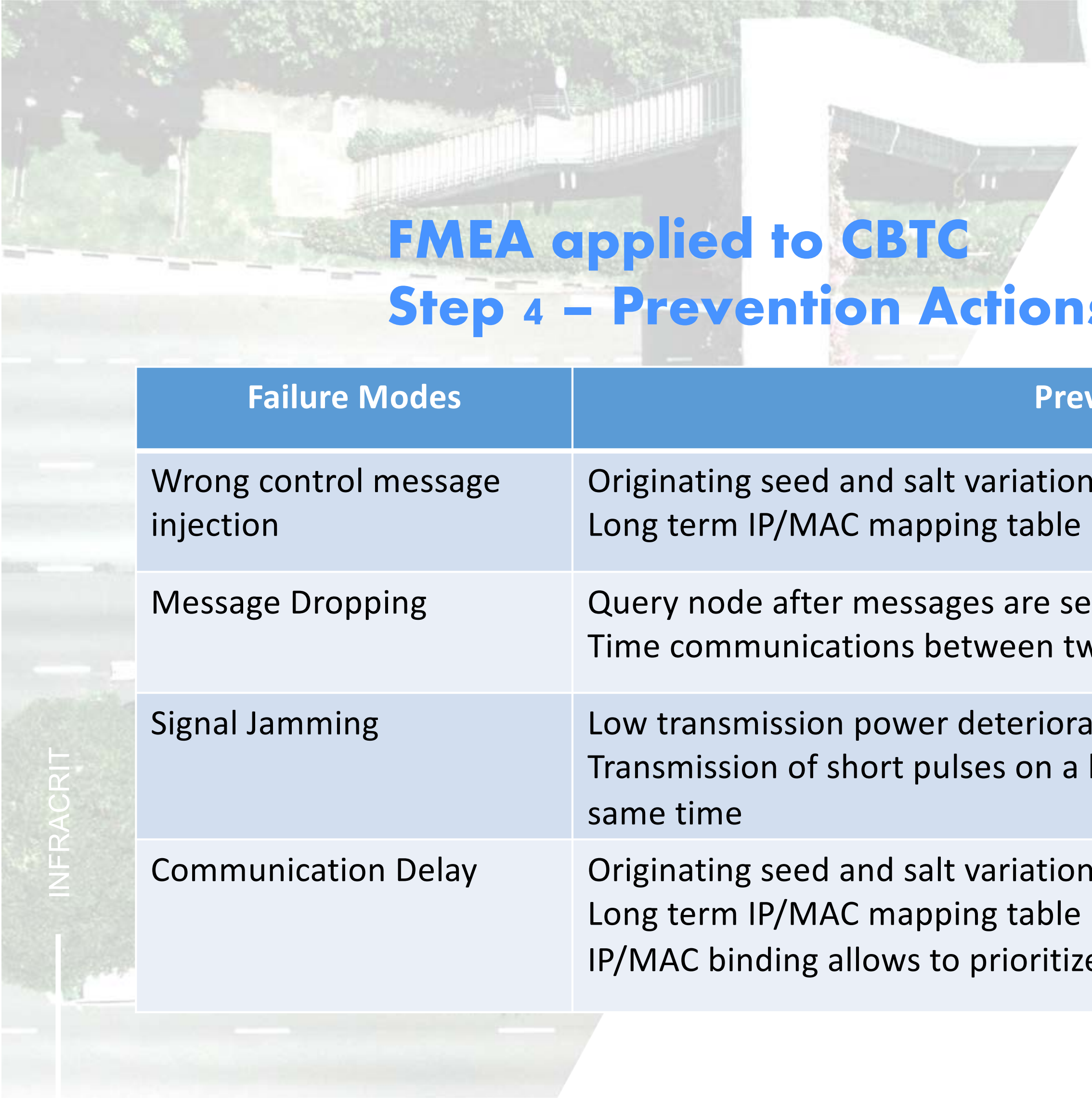
FMEA applied to CBTC
Step 2 – Failure modes identification

Failure Mode	Failure Cause	Failure Effect
Wrong Control Messages injection (Packet Spoofing)	Message Spoofing Attack	Unexpected abrupt braking Train location loss Train speed control loss Train full stop Train collision Train derailment
Message Dropping (Packet Dropping)	Message Dropping Attack	Train full stop Emergency braking; Change to conventional operation
Signal Jamming	Jamming Attack	Train full stop Emergency braking; Change to conventional operation
Communication Delay (Extensive packet duplication and forwarding)	Replay Attack	Train control performance breakdown Change to conventional operation

FMEA applied to CBTC
Step 3 – RPN calculation



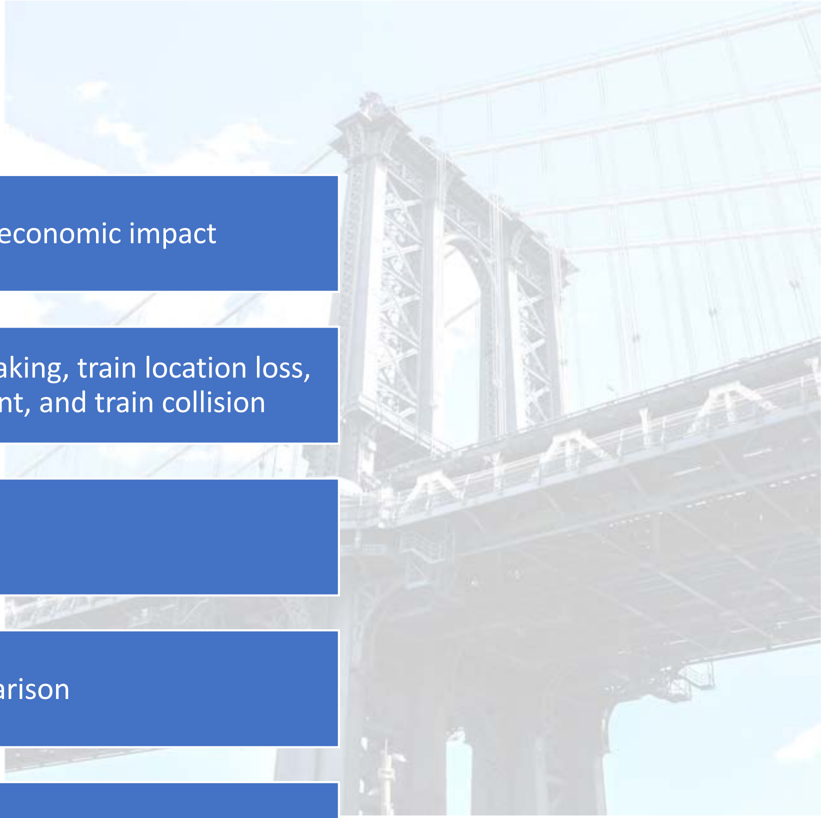
Failure Mode	Social	Infrastr	Environ	Delay	RPN	
	0.5	0.35	0.05	0.1	Original	Our Approach
Wrong control message injection	10	10	10	10	10,000	10
Message dropping	3	2	1	2	12	2.45
Signal jamming	3	2	1	2	12	2.45
Communication Delay	1	1	1	1	1	1



FMEA applied to CBTC
Step 4 – Prevention Actions

Failure Modes	Prevention actions
Wrong control message injection	Originating seed and salt variation method for authentication. Long term IP/MAC mapping table
Message Dropping	Query node after messages are sent Time communications between two nodes with a limit waitable timer
Signal Jamming	Low transmission power deteriorates chances for attacker signal location Transmission of short pulses on a broad spectrum of a frequency band at the same time
Communication Delay	Originating seed and salt variation method for authentication Long term IP/MAC mapping table IP/MAC binding allows to prioritize traffic with static IP assignment reservation

Conclusions and Future Work



- The factors’ weight according to the parameter’s economic impact
- The attacks consequences may be unexpected abrupt braking, train location loss, train speed control loss, train full stop, train derailment, and train collision
- Associated Cost with the Risk
- RPN scale from 1 to 10 for easy comparison
- Apply this RPN formula to other CBTC subsystems and infrastructures

QUESTIONS ?

THANK YOU

INFRACRIT